UNIVERSITÉ PIERRE ET MARIE CURIE - PARIS 6
UNIVERSITAS
U.F.R. INFORMATIQUE

THÈSE DE DOCTORAT

Pour obtenir le grade de
DOCTEUR DE L'UNIVERSITÉ PIERRE ET MARIE CURIE

Discipline : RÉSEAUX INFORMATIQUES

Présentée par
Mlle. Michele NOGUEIRA LIMA

Titre :

UNE ARCHITECTURE POUR LA SURVIVABILITÉ AUX ATTAQUES DANS LES RÉSEAUX AUTO-ORGANISÉS

Soutenance publique : le 6 octobre 2009

Directeur de Thèse:
M. Guy PUJOLLE

JURY

Rapporteur	M. Khaldoun AL AGHA	Professeur à l'Université Paris-Sud11
Rapporteur	M. José M. NOGUEIRA	Professeur à l'Université de Minas Gerais
Examinateur	M. David POWELL	Directeur de Recherche CNRS au LAAS
Examinateur	M. Serge FDIDA	Professeur à l'Université Pierre et Marie Curie
Examinateur	M. Pascal URIEN	Professeur à Telecom ParisTech
Directeur de thèse	M. Guy PUJOLLE	Professeur à l'Université Pierre et Marie Curie

Résumé

Cette thèse est originalement écrite en anglais sur le titre : *SAMNAR: A SURVIVABLE ARCHITECTURE FOR WIRELESS SELF-ORGANIZED NETWORKS*. Pour être en conformité avec les demandes de l'école doctorale d'informatique, télécommunications et électronique de Paris (EDITE de Paris), ce résumé en français présente de façon succincte le contenu de chaque chapitre.

Résumé du chapitre 1 : Introduction

Le développement des réseaux sans fil a renforcé l'importance des systèmes répartis dans notre quotidien. Ces réseaux sont de plus en plus disposés partout motivant ainsi la création de nouvelles applications et, par conséquent, l'augmentation dans le nombre d'usagés. Les personnes sont de plus en plus dépendantes de ces réseaux pour réaliser différentes activités comme par exemple accéder à ses comptes bancaires, acheter sur l'Internet et exécuter des analyses médicales. Ces caractéristiques induisent la nécessité d'un haut niveau de fiabilité, de sécurité et de disponibilité pour ces réseaux et ses applications.

Les réseaux sans fil auto-organisés comme les réseaux ad hoc mobiles, les réseaux mesh et les réseaux de capteurs, sont des exemples de systèmes répartis omniprésents. Ces réseaux sont hétérogènes et composés de dispositifs portables, appelés noeuds, qui communique entre eux par multi-sauts. En raison de l'auto-organisation, ces réseaux peuvent s'adapter aux changements dans leur environnement, comme, par exemple, la position géographique des noeuds, le modèle de trafic et les interférences. Chaque appareil peut se reconfigurer en fonction des changements dans la topologie du réseau, son rayon de couverture et la chaîne de communication allouée. Néanmoins, aucune entité de contrôle centralisée n'existe pour ces réseaux, nécessitant une approche décentralisée pour la gestion du réseau.

La sécurité est essentielle dans les réseaux sans fil auto-organisés, en particulier pour les applications sensibles à la sécurité notamment dans les domaines militaire, de la santé et des finances. Ces réseaux présentent des faiblesses liées aux fautes dans les protocoles des réseaux, aux vulnérabilités dans les systèmes d'exploitation et aux caractéristiques du réseau. Ces réseaux ont des défis non triviaux pour la sécurité en raison de leurs caractéristiques, telles que l'utilisation partagée du medium de communication sans fil, le dynamisme de la topologie du réseau, la communication multi-sauts et la faible protection physique des dispositifs portables. De plus, l'absence d'entité centralisée augmente la complexité des opérations de gestion de la sécurité, en particulier, le contrôle d'accès, l'authentification des noeuds et la distribution de clefs cryptographiques.

Plusieurs solutions de sécurité ont été proposées pour les réseaux sans fil auto-organisés. Ces solutions ont utilisé deux lignes de défense : la prévention ou la réaction. La première essaie de contrecarrer les attaques par la cryptographie, l'authentification et les mécanismes de contrôle d'accès, tandis que la deuxième cherche à détecter des intrusions et à réagir en conséquence. Cependant, chaque mécanisme de sécurité traite des questions spécifiques ayant des limitations face à différents types d'attaques et d'intrusions. Des défenses préventives, par exemple, sont vulnérables à la malveillance des noeuds qui participent déjà aux opérations du réseau et des défenses réactives ne travaillent de manière efficace que contre des attaques ou des intrusions connues.

En raison des limitations des mécanismes de défense préventifs et réactifs, les chercheurs sont en train d'appliquer une autre ligne de défense appelée tolérance aux intrusions. Cette ligne de défense vise à améliorer la résistance du réseau en présence d'attaques et d'intrusions en utilisant les techniques de tolérance aux pannes comme la redondance et des mécanismes de recouvrement. Toutefois, les solutions de sécurité restent toujours centrées sur un problème spécifique ou sur une couche de la pile protocolaire, étant ainsi inefficaces pour assurer les services essentiels des réseaux sans fil auto-organisés.

Les caractéristiques du réseau ainsi que des contraintes sur les lignes de défense renforcent le fait qu'il n'existe pas de réseau totalement protégé contre les attaques et les intrusions. Pour cette raison, de nouvelles approches sont nécessaires pour garantir l'intégrité, la confidentialité, l'authentification et, en particulier, la

disponibilité des services du réseau. Ces exigences motivent la création de services survivants aux attaques et aux intrusions dans le réseau sans fil auto-organisé.

Le concept de la survivabilité consiste en la capacité d'un réseau à soutenir des services essentiels même face à des attaques et à des intrusions. Dans ce travail, nous devons souligner la transmission de bits de données à partir d'un noeud à l'autre comme la fonctionnalité fondamentale du réseau et nous nous concentrons sur trois services essentiels: la connectivité dans la couche de liaison, le routage et la communication de bout-en-bout. Nous argumentons que la survivabilité des réseaux est obtenue quand une solution multicouche intègre les trois lignes de défenses, c'est-à-dire la prévention, la réaction et la tolérance, d'une manière auto-adaptative et coordonnée.

La définition du problème et des objectifs

Le problème abordé dans ce travail consiste à fournir une architecture de gestion de la sécurité afin de rendre les réseaux sans fil auto-organisés survivant aux attaques et aux intrusions. Même s'il existe de nombreuses solutions de sécurité pour ces réseaux, ils utilisent séparément différents mécanismes de sécurité sans assurer l'intégration et la coopération entre eux. De plus, ces solutions ne prennent pas en compte les particularités du réseau, telles que ses besoins et ses caractéristiques.

Ce travail présente une discussion générale sur la survivabilité dans les réseaux sans fil auto-organisés. Cette discussion nous permet d'identifier les questions ouvertes en relation à la survivabilité et à ses implications en ce qui concerne notamment les caractéristiques du réseau. Cette discussion a pour résultat l'état de l'art des travaux qui appliquent le concept de survivabilité dans les réseaux sans fil auto-organisés. Basée sur cet état de l'art, nous concevons l'architecture SAMNAR dont le but est de soutenir le fonctionnement des services essentiels, même en présence d'attaques et d'intrusions. Ensuite, nous employons l'architecture SAMNAR sur le service de routage et sur le service de gestion des clefs cryptographiques résultant, respectivement, en un mécanisme pour la sélection de routes survivantes et en un système survivant de gestion de clefs cryptographiques. Enfin, nous proposons un framework basé sur SAMNAR qui utilise la technologie

de la radio cognitive pour concevoir des connectivités adaptables dans la couche de liaison de la pile protocolaire.

Les contributions

Nous résumons les contributions de cette thèse par:

- **L'état de l'art des initiatives de survivabilité pour les réseaux sans fil auto-organisés.** L'état de l'art est utile pour comprendre la situation actuelle en relation au sujet de survivabilité et pour accentuer la pertinence des contributions. L'état de l'art présente une vue générale du concept de survivabilité dans le domaine des réseaux sans fil auto-organisés. Les initiatives de survivabilité et des architectures sont présentées et conceptualisées. Par conséquent, l'état de l'art nous permet d'identifier les questions ouvertes et les possibilités d'utiliser les concepts de survivabilité dans ces réseaux.

- **SAMNAR: l'architecture de survivabilité pour les réseaux sans fil auto-organisés.** Basé sur l'évaluation des initiatives de survivabilité, des solutions, des architectures et des protocoles existants, nous concevons une architecture de survivabilité pour les réseaux auto-organisés appelée SAMNAR. Cette architecture est inspirée du système immunitaire du corps humain et propose une approche adaptative de gestion de la sécurité afin d'aboutir à la survivabilité aux attaques et aux intrusions. L'architecture SAMNAR permet l'utilisation coordonnée des trois lignes de défense, la prévention, la réaction et la tolérance, d'une manière adaptative.

- **Le schéma pour la sélection de route survivante.** L'architecture SAMNAR a été employée pour le service de routage résultant en un schéma de sélection de routes survivantes. La solution proposée est indépendante de tout protocole de routage. Elle consiste à établir les routes les plus survivantes. Le schéma de sélection prend en compte plusieurs critères tels que les conditions du réseau en corrélation avec les trois lignes de défense. Les résultats de simulation montrent l'atténuation de l'impact des différentes attaques de routage avec une faible perte de performances pour le réseau.

- **La gestion survivante de clefs cryptographiques.** Cette contribution consiste en une infrastructure de clefs publiques, de l'anglais, Public Key Infrastructure (PKI), qui vise à gérer et à distribuer des clefs cryptographiques efficacement, même face à des attaques ou à des intrusions. Le PKI est basé sur l'architecture SAMNAR, sur les relations sociales des utilisateurs et sur la corrélation des différents types d'éléments de preuve pour certifier la responsabilité des utilisateurs sur leurs clefs publiques. Les résultats de simulation montrent une amélioration de survivabilité réussite par le PKI en termes d'efficacité et de survivabilité aux attaques.

- **Des directions pour la survivabilité des connectivités.** Cette contribution offre un ensemble de directions pour parvenir à la survivabilité dans les connectivités de la couche de liaison de la pile protocolaire. Un framework est proposé en considérant des connectivités reconfigurables. En particulier, la technologie de la radio cognitive est prévue pour être utilisée. Le framework est fondé sur l'architecture SAMNAR et il considère les caractéristiques et les opérations de gestion du spectre.

L'organisation de la thèse

La thèse est structurée en sept chapitres et deux annexes. Le chapitre 2 présente les concepts de la gestion et de la survivabilité de réseau ainsi que les besoins et les propriétés de survivabilité. Le chapitre 3 décrit l'architecture proposée, appelée SAMNAR, en mettant l'accent sur ses modules de gestion de la sécurité et sur l'approche basée sur l'adaptation de la coordination de des trois lignes de défense, la prévention, la réaction et la tolérance. Un schéma de sélection de routes survivantes est présenté dans le chapitre 4. Ce schéma est fondé sur l'architecture SAMNAR. Il utilise la logique floue pour corréler des critères classiques et des critères de sécurité afin de choisir les routes les plus survivantes. Les critères classiques sont ceux qui caractérisent l'environnement du réseau et son état, ainsi que les critères de sécurité qui résultent en des mécanismes de sécurité de prévention, de réaction et de tolérance. Le chapitre 5 présente le système survivant de gestion de clefs cryptographiques dans lequel les différents types d'éléments de preuve sont appliqués pour certifier la responsabilité des usagers pour leurs clefs publiques. Le

chapitre 6 propose un framework pour aboutir à la survivabilité des connectivités de la couche de liaison en prenant en compte plus particulièrement la technologie de la radio cognitive. Le chapitre 7 qui conclut la thèse présente des limites de l'architecture de survivabilité et fournit des orientations pour les travaux futurs. Enfin, l'annexe A décrit les initiatives de survivabilité existantes dans les protocoles de routage de réseaux sans fil auto-organisés et l'annexe B présente l'ensemble des règles floues utilisées pour l'évaluation des routes survivantes par le schéma de sélection de route proposé dans le chapitre 4.

Résumé du chapitre 2 : La gestion de la sécurité et les concepts de survivabilité

L'importance de la gestion dans les réseaux sans fil auto-organisés croît chaque jour. Ces réseaux sont des systèmes distribués hétérogènes composés de matériel, de logiciels et de protocoles de diverses organisations et fournisseurs. Assurer une intégration réussie entre ces différents éléments est essentiel pour maintenir le fonctionnement de services essentiels du réseau tels que la connectivité de la couche de liaison, le routage et la communication de bout-en-bout. La gestion du réseau est utilisée pour contrôler et pour surveiller cette intégration, ses composants et le fonctionnement des services essentiels. De plus, elle permet aux concepteurs du réseau de traiter les défauts, de réduire les coûts et de faire face aux situations inattendues pour le réseau tel que la présence d'attaques ou d'intrusions.

La gestion de la sécurité est l'un des principaux défis de la recherche dans les réseaux sans fil auto-organisés. Il s'agit d'une fonctionnalité du domaine de la gestion de réseau, composé par opérations qui contrôlent les mécanismes de la sécurité et les services et, donc, déjouent les attaques et les intrusions. En raison des caractéristiques des réseaux sans fil auto-organisés et de l'inefficacité des mécanismes classiques de sécurité pour bloquer toutes les attaques et les intrusions, de nouvelles approches de gestion de la sécurité sont nécessaires. De plus, l'accroissement de la dépendance des personnes aux ordinateurs et aux réseaux résulte en un grand besoin de fiabilité et de robustesse pour les réseaux auto-organisés. Par conséquent, les chercheurs et les industriels s'orientent vers

une perspective de survivabilité pour la gestion de la sécurité, s'intégrant ainsi entre les domaines de la sécurité et la fiabilité.

Le chapitre 2 fournit une vue globale de la gestion de la sécurité et des concepts liés à la survivabilité ainsi que des menaces relatives à la sécurité et à la survivabilité des réseaux sans fil auto-organisés. Le chapitre est organisé en cinq sections, comme suit. La section 2.1 analyse les menaces relatives à la sécurité dans ces réseaux. La section 2.2 présente les concepts de la gestion de la sécurité. Elle est suivie par les concepts liés à la survivabilité dans la section 2.3 et par les besoins de la survivabilité présentés dans la section 2.4. Enfin, la section 2.5 conclut le chapitre.

Les menaces dans les réseaux auto-organisés

Les réseaux sans fil auto-organisés sont vulnérables à de nombreuses menaces. Les caractéristiques du réseau telles que la topologie dynamique, son architecture décentralisée, le medium de communication sans fil, la faible sécurité physique des noeuds et la communication multi-sauts résultent en différentes vulnérabilités et rendent difficile la maintenance des services essentiels du réseau. L'architecture décentralisée, par exemple, exige la coopération entre les noeuds avec de connectivité d'un ou de plusieurs sauts sans avoir la garantie que tous les noeuds vont coopérer comme prévu. L'autonomie du réseau, le fort dynamisme de la topologie et l'absence de contrôle d'accès facilitent la participation des noeuds malicieux ou égoïstes à l'exploitation du réseau. De plus, la communication sans fil est vulnérable aux interférences et aux interceptions et la faible sécurité physique des noeuds augmente leurs possibilités d'être altérés.

Ce travail traite deux menaces spécifiques, les attaques et les intrusions. Une attaque est une action qui exploite une faiblesse du réseau de manière à compromettre l'intégrité, la confidentialité, la disponibilité et la non-répudiation de l'information ou des services du réseau. Une intrusion exploite également les faiblesses du réseau, elle résulte d'une attaque réussie. Les attaques et les intrusions sont produites par des attaquants, c'est-à-dire des entités malveillantes (comme des humains, des noeuds, des services ou des logiciels). Les attaquants

tentent de surpasser toute autorité qu'ils pourraient avoir en cherchant à atteindre leurs objectifs malveillants. Ils profitent des failles de sécurité créées par les caractéristiques du réseau, ou des faiblesses dans les protocoles de réseau ou de logiciel. Les pirates sont des exemples d'attaquants, les vandales, les logiciels malveillants et des noeuds malveillants ou égoïstes.

Il existe différentes classifications pour les attaques et les intrusions. La classification plus commune est celle qui regroupe les menaces par couche de la pile protocolaire. Cette classification est adaptée dans la thèse et nous avons comme exemple d'attaques selon cette classification: les attaques jamming dans la couche physique; les attaques d'exhaustion et de collisions dans la couche de liaison; les attaques blackhole, grayhole, wormhole, sybil et autres dans la couche de routage; et les attaques SYN flooding dans la couche de transport.

La gestion de la sécurité

La gestion de la sécurité est définie comme un ensemble de services pour protéger les réseaux et les noeuds attaqués et pour répondre à l'évolution des besoins de sécurité de l'utilisateur ou des conditions du réseau. Les fonctions principales de la gestion de la sécurité sont : le contrôle et le monitoring des services de sécurité et des mécanismes; la distribution des informations de sécurité; des rapports relatifs aux événements du réseau; le contrôle de la distribution du matériel de chiffrement; le contrôle d'accès, les droits et les privilèges.

Un service de sécurité est un ensemble d'opérations prévues par un protocole pour assurer une protection adéquate des ressources du réseau, des applications ou des transferts de données. Ces services sont destinés à contrer les attaques en utilisant un ou plusieurs mécanismes de sécurité. Les principaux services de sécurité sont les suivants: l'authentification, le contrôle d'accès, la non-répudiation et la confidentialité et l'intégrité des données.

Un mécanisme de sécurité est un processus conçu pour détecter, prévenir ou réparer le réseau suite à des attaques ou des intrusions. Il peut être indépendant de tout protocole ou être mis en oeuvre de façon spécifique. Dans les réseaux sans fil auto-organisés, les mécanismes de sécurité suivent deux lignes de défense : la prévention et la réaction. La première prévoit des mécanismes pour éviter

les agressions, tels que le pare-feu et la cryptographie. La deuxième consiste à prendre des actions pour détecter des dysfonctionnements et à réagir contre les intrusions, comme par exemple les systèmes de détection d'intrusion (IDS) ou les systèmes de réputation.

Malgré les efforts visant à améliorer les défenses préventives ou réactives, ces deux défenses ne sont pas suffisantes pour bloquer toutes les attaques et les intrusions. De cette façon, des chercheurs sont en train de travailler sur une autre ligne de défense, appelée tolérance aux intrusions. Cette ligne de défense complète les autres. Son but est d'atténuer les effets des actions égoïstes ou malveillantes par l'utilisation de techniques de tolérance aux pannes comme la redondance et la réplication des données.

Ce travaille vise à utiliser les trois lignes de défense de façon coordonnée et adaptative aux conditions du réseau afin d'aboutir à la survivabilité du réseau même en présence d'attaques et d'intrusions. Pour arriver à la survivabilité, ses propriétés doivent être réunies telles que la résistance, la recognition, la réparation et l'adaptation. De la même façon, ses besoins doivent être satisfaits comme la décentralisation du système de survivabilité, l'auto-organisation, le passage à l'échelle et d'autres.

Résumé du chapitre 3 : L'architecture de survivabilité SAMNAR

Le chapitre 3 décrit l'architecture de survivabilité, appelée SAMNAR, pour les réseaux sans fil l'auto-organisés. Les architectures incluent des concepts, des règles et des modèles. Les règles décrivent comment utiliser les concepts et les modèles montrent l'application des règles et des concepts. L'architecture SAMNAR discute des fonctions de la gestion de sécurité et guide le développement de protocoles et de services survivants. La gestion de la sécurité est composée de fonctions de contrôle et de surveillance des services et des mécanismes de sécurité, la distribution des informations, la génération d'établissement de rapports relatifs à la sûreté des événements, de la distribution du matériel de chiffrement et le contrôle de l'accès, les droits et privilèges.

Le chapitre 3 est organisé en cinq sections, comme suit. La section 3.1 présente les travaux précédants qui ont proposé des architectures en direction à la survivabilité. La section 3.2 donne un aperçu du système immunitaire humain et la section 3.3 décrit la corrélation de ce système avec notre architecture. La section 3.4 détail l'architecture SAMNAR. Enfin, la section 3.5 conclut le chapitre.

L'architecture SAMNAR présente une nouvelle approche pour la gestion de la sécurité afin de rendre les réseaux sans fil auto-organisés survivants aux attaques et aux intrusions. SAMNAR est inspiré du système immunitaire du corps humain dans lequel les différents types de défenses coopèrent de façon adaptative. L'architecture offre la prévention, la réaction et l'atténuation des préjudices causés par des attaques ou des intrusions, ainsi que la récupération de services en temps opportun après des intrusions. SAMNAR vise à augmenter la capacité du réseau à soutenir des services essentiels, comme la connectivité de la couche de liaison, le routage et la communication de bout-en-bout, même face aux attaques et aux intrusions. De plus, il propose une approche cross-layer pour la gestion de la sécurité.

Comme le système immunitaire du corps humain, SAMNAR est basé sur la coopération entre les trois lignes de défense : la prévention, la réaction et la tolérance. La prévention est vue comme le premier obstacle, elle est composée des mécanismes de sécurité préventifs visant à éviter tout type d'attaque. Des exemples de ces mécanismes sont les pare-feux et la cryptographie. Ils bloquent certaines attaques, mais, bien évidemment, sera incapable d'empêcher quelques autres attaques en raison de leurs limitations. La cryptographie et le pare-feu, par exemple, sont vulnérables aux attaques produites par des noeuds qui participent déjà légalement dans le réseau.

Pour certaines attaques qui arrivent à s'infiltrer dans un noeud ou un réseau, la défense réactive essaie de les détecter et de réagir. Des mécanismes, tels que les systèmes de détection d'intrusion ou la réputation, cherchent à évaluer le comportement des noeuds dans le réseau. Toutefois, les défenses réactives travaillent efficacement contre les intrusions qu'elle connaît bien, mais elles sont vulnérables aux intrusions inconnues. Les systèmes de détection d'intrusion, par exemple, nécessitent un ensemble de preuves et d'analyses pour détecter les intrusions basées sur des anomalies ou des schémas préétablis d'intrusion. Par conséquent,

les défenses réactives ont également des limites car des intrus peuvent réussir à compromettre le réseau. Afin de garantir le fonctionnement des services essentiels, même en présence d'intrusions, les techniques de tolérance aux intrusions sont appliquées. Ces techniques visent à atténuer les effets de l'intrusion et à stimuler les défenses préventives et réactives à s'adapter et à tenter de bloquer les attaques et les intrusions.

SAMNAR est une architecture de gestion de la sécurité pour les réseaux sans fil auto-organisés. Les caractéristiques de SAMNAR résultent en des exigences et des propriétés de la survivabilité. Chaque noeud est responsable de sa survivabilité réussite par la gestion des mécanismes de sécurité et par notre approche de survivabilité. Chaque noeud du réseau est également auto-géré, sans l'existence d'entité centrale dans le réseau pour offrir des fonctionnalités de gestion. L'architecture SAMNAR est composée de trois grands modules : la survivabilité, la communication et la collecte. Le principal module concerne la survivabilité en employant notre approche de survivabilité. Les modules de communication et de collecte appuient le premier module. Le module de survivabilité possède cinq composants indépendants, quatre sont liés aux propriétés de survivabilité, de résistance, de récupération, de reconnaissance et d'adaptabilité et le composant de contrôle. Les propriétés représentent respectivement la capacité du réseau à repousser les attaques; à détecter des attaques et à évaluer les préjudices; à restaurer des informations ou des fonctionnalités ; et à rapidement intégrer les enseignements tirés des échecs et l'adaptation aux nouvelles menaces.

Le composant de contrôle gère et coordonne tous les modules dans l'architecture. Il reçoit des informations de communication et des informations recueillis par des modules ainsi que de la résistance, la reconnaissance et de la récupération des composants. Le composante de contrôle corrèle et analyse toutes les informations afin de faire des inférences et de prendre des décisions. Toutes les décisions sont envoyées au composant d'adaptation qui définit et envoie des valeurs de paramètre satisfaisant à d'autres modules ou composants. Le composant d'adaptation apprend à effectuer des mesures et, plus tard, il peut prendre les mêmes mesures dans le noeud de réseau ou une condition connue.

Le module de communication est chargé de la communication cross-layer et inter-noeuds. La communication inter-couche propose l'échange d'informations

entre les couches. Il fournit des informations provenant de différentes couches du réseau en permettant au composant de contrôle de prendre des décisions fondées sur toutes les couches du réseau et d'assurer la survivabilité pour chacune d'elles. La communication inter-noeuds vise l'échange et la synchronisation de l'information entre les noeuds afin de garantir la survivabilité de l'ensemble du réseau. Un exemple de cette information est la configuration du noeud ou la détection d'intrusions dans le réseau. Les techniques de communication inter-noeuds doivent considérer les limitations des noeuds et l'hétérogénéité des capacités de ressources dans le réseau, telles que la mémoire, le processeur et la bande passante et doit être efficace dans l'utilisation de ces ressources.

Le module de la collecte contient des mécanismes visant à rassembler toutes les données requises par le module de survivabilité. Le module est composé de deux composants : le composant de prétraitement et le composant d'information de l'environnement. Le premier est exploité lorsque les données doivent être traitées avant de les envoyer au module de survivabilité. Des normalisations et des calculs précédents sont des exemples de prétraitement utilisés pour faciliter les analyses et les conclusions du module de survivabilité. Le deuxième maintient à jour des informations collectées périodiquement sur les conditions du réseau et il les envoie au module de survivabilité en cas de besoin.

Résumé du chapitre 4 : La survivabilité du routage dans les réseaux ad hoc et les réseaux mesh

Le routage est une fonctionnalité essentielle dans les réseaux sans fil auto-organisés. Sa fonction principale est de soutenir la transmission de données d'un utilisateur à d'un noeud à un autre. Le service de routage est composé de quatre phases : la découverte de route, la maintenance de la route, la sélection du chemin et la distribution du trafic. Le chapitre 4 démontre l'application de l'architecture SAMNAR dans la phase de sélection de route. Un schèma de sélection de route survivant est proposé pour les deux types de réseaux sans fil auto-organisés : les réseaux ad hoc (MANETs) et les réseaux mesh (WMNs).

Cette étude de cas traite le problème de sélection des routes les plus survivantes, c'est-à-dire les routes qui arrivent à maintenir le service de routage

même en présence d'attaques, d'intrusions ou d'actions égoïstes. Le schèma proposé combine différents critères de séléction représentant les conditions du réseau et les trois lignes de défense: la prévention, la réaction et la tolérante. Nous évaluons la survivabilité du schéma de sélection sur différents scénarios de mobilité urbaine avec différents modèles de propagation et sur le modèle de mobilité random waypoint avec le modèle de propagation two-ray ground. Les résultats de simulation démontrent l'amélioration de la survivabilité avec un faible impact sur la performance du réseau.

Le chapitre 4 est organisé en cinq sections, comme suit. La section 4.1 présente les travaux précédants en corrélation avec la problématique de sélection de routes. La section 4.2 décrit les modèles des attaques et du réseau pris en considération dans l'étude de cas. La section 4.3 détaille le schèma proposé en suivant ces trois phases: la collecte de données, la logique floue et la sélection de la route. La section 4.4 présente la méthodologie d'évaluation, l'environnement de simulation et les résultats. Enfin, la section 4.5 conclut le chapitre.

Le schèma de sélection de route proposé est basé sur l'architecture SAMNAR présentée dans le chapitre 3. Il utilise à la fois des critères classiques et des critères de sécurité pour choisir des routes plus survivantes. Des critères conventionnels (ou classiques) permettent la gestion des ressources et de la performance. Nous avons choisi le niveau de l'énergie restante (le taux de l'énergie) et la longueur du chemin comme des informations du réseau (environnement d'informations). Toutefois, d'autres critères pourraient être ajoutés ou remplacés, tels que le débit atteint par le chemin, la stabilité du lien et d'autres.

Conformément avec l'approche de survivabilité proposée, les critères de sécurité comprennent des éléments résultants des trois lignes de défense. Cette étude de cas utilise le temps d'expiration du certificat et la longueur de clef de cryptage pour représenter les critères de défenses préventives, la réputation du noeud comme critère de la défense réactive et le degré du chemin comme critère de tolérance en raison de la possibilité de fournir des routes redondantes. D'autres critères de sécurité peuvent également être ajoutés ou remplacés, comme par exemple le type de cryptographie utilisée et le pourcentage de faux positifs ou de faux négatifs.

Comme la corrélation de plusieurs critères et la sélection d'un chemin optimal est un problème NP-complet, des heuristiques, des méthodes d'optimisation et des distributions de probabilité ont été utilisées pour prendre de meilleures décisions. Certaines d'entre elle sont basées sur des limites dont les valeurs sont difficiles à déterminer en raison du fort dynamisme et des états incertains dans les réseaux MANETs et WMNs. De plus, le manque de ressources limite l'utilisation de méthodes qui demandent beaucoup de ressource pour les calculs, ou des solutions complexes.

Le schèma de sélection proposé emploie la logique floue (FL) car elle s'est révélée être un outil puissant pour prendre des décisions. FL permet la définition de valeurs intermédiaires entre 0 (faux) et 1 (vrai) et elle accepte des règles exprimées en langage naturel, les modèles et les problèmes d'une manière plus facile. De plus, FL gère de données imprécises.

Notre schèma de sélection de chemin est indépendant du protocole de routage. Cependant, le protocole doit être capable de trouver plusieurs routes noeud-disjointes de la source à la destination. Les chemins noeud-disjoints sont préférables par rapport aux chemins non-disjoints ou link-disjoints car ils n'ont pas de noeuds ou de liens partagés entre les routes.

Les phases de notre schèma de sélection de chemin sont : la collecte de données, l'inférence par la logique floue et la sélection adaptative des routes. La phase de collecte de données obtient les valeurs des critères par des processus de polling et en utilisant des paquets de contrôle appelés CPACKs. Le processus de collecte consiste à envoyer périodiquement des CPACKs à tous les chemins connus par un noeud. Les CPACKs ont deux fonctions: la vérification de l'état de la route et la collecte des valeurs des critères.

L'inférence par la logique floue calcule le niveau de survivabilité de chaque route. Le niveau de survivabilité de la route, appelé PSL, est réalisé par les phases suivantes : la fuzzification, l'inférence et la défuzzification. Les chemins sont classés et la route la plus survivante est choisie dans la phase de sélection des routes à partir de la valeur du PSL. Toutefois, en raison de nouvelles collectes de données, la valeur du PSL d'un chemin peut changer avec des mises à jour des valeurs des critères. Ainsi, l'ensemble des routes peuvent également changer de

façon adaptative. De façon générale, la valeur du PSL est calculée par la formule: $PSL \propto E \bullet K \bullet R \bullet D \bullet \frac{1}{L} \bullet \frac{1}{T}$.

Où, les symboles E, K, R, D, L et T sont les critères utilisés pas dans les évaluations de survivabilité des routes et représentent, respectivement, la valeur minimum du taux d'énergie entre les noeuds d'un chemin, la valeur minimum trouvée dans le chemin de la taille de la clef cryptographique utilisée, la valeur minimum entre toutes les réputations des noeuds dans un chemin, la valeur minimum de dégré entre les noeuds du chemin, la taille du chemin en termes de nombre de sauts et la valeur minimum de temps qui manque pour l'expiration des certificats digitaux.

Nous avons évalué notre schèma de sélection de chemin avec des simulations en utilisant le simulateur de réseau NS-2, version 2.30. Des simulations ont été effectuées en considérant deux réseaux: un réseau ad hoc en utilisant le modèle de mobilité *two-way random*, appelé le CAS 1 et un réseau mesh urbain employant des modèles réalistes pour la mobilité et la propagation du signal, appelé CAS 2. Pour ces évaluations, le schèma de sélection de chemin est instancié sur le protocole de routage AOMDV (On-demand Multipath Distance Vector Routing in Ad Hoc Networks). Ce protocole a été modifié pour fournir les valeurs des critères de sécurité et pour exécuter les fonctionnalités définies par le schèma comme la collecte des données, l'inférence floue et la sélection du chemin. Les chemins noeud-disjoints ont été utilisés afin de fournir la redondance.

Nous avons examiné deux aspects principaux: l'amélioration de la survivabilité du réseau obtenue par le schèma de sélection du chemin et l'impact du schèma sur les performances du réseau. Pour cela, nous comparons les résultats produits par la modification du protocole AOMDV, appelé AOMDV-SL, avec ceux générés par AODV et AOMDV en présence d'attaques blackhole (BH) ou grayhole (GH) et avec les combinaisons des deux avec l'attaque sinkhole. Le protocole AOMDV-SL fournit les informations de sécurité préventive, réactive et tolérante indépendamment d'un protocole sécurisé, d'un système de réputation, d'un mécanisme cryptographique ou d'une infrastructure de distribution de clef spécifique. Le protocole AOMDV n'a pas de mécanisme de sécurité contre l'ensemble des attaques forte collusion, mais nous l'avons utilisé en raison de ses performances.

Nous avons utilisé les métriques suivantes pour évaluer l'amélioration de la survivabilité obtenue par notre schèma et son impact sur les performances du réseau. Pour toutes ces métriques, nous avons calculé un intervalle de confiance de 95%.

- Misbehavior drop ratio (MDR) - mesure la proportion des paquets de données jetés en raison des attaques sur le total des paquets de données supprimés. Pour les analyses, nous avons mis en place des mécanismes dans le simulateur NS-2 pour enregistrer de paquets de données jetés à cause d'attaques.

- Taux de livraison de Paquets (PDR) - calcule le pourcentage de paquets de données livrés à destination par rapport à la quantité total de paquets de données envoyés par la source.

- La latence bout-en-bout des paquets de données (délai E2E) - se compose des retards de propagation, des délais d'attente aux interfaces, des retards de retransmission à la couche MAC, ainsi que des retards en tampon de la mémoire lors de l'étape de découverte de route.

En général, les résultats de simulation ont montré pour les deux cas étudies une réduction du pourcentage de paquets perdus en raison d'attaques indépendamment de la dynamique du réseau causée par la vitesse des noeuds. L'utilisation du notre schèma a abouti à un taux de survivabilité mesurée par la livraison des paquets similaires à ceux produits par les autres protocoles évalués. De plus, dans certains scénarios, la latence du réseau en utilisant le mécanisme de survivabilité est plus faible que celle des réseaux en employant les autres protocoles d'évaluation.

Résumé du chapitre 5 : Un système survivant pour la gestion de clefs cryptographiques publiques

La cryptographie est utilisée pour garantir la sécurité dans les différents services d'auto organisation dans les réseaux sans fil. En particulier, elle est utilisée pour assurer l'intégrité, la confidentialité, l'authentification et la non-répudiation dans la connectivité de la couche de liaison, dans la couche de routage ou dans la communication de bout-en-bout. Les opérations cryptographiques, telles que le

cryptage ou le décryptage, dépendent d'un matériel cryptographique et d'un algorithme. Le matériel cryptographique comprend les paires de clefs publique/privée, les clefs secrètes, les paramètres d'initialisation et les paramètres non secrets. Il détermine la sortie fonctionnelle des algorithmes cryptographiques, le contrôle de la complexité de la rupture des messages cryptés, l'authentification des noeuds et des utilisateurs et la validation des messages.

Le matériel cryptographique doit être distribué et géré. Plus précisément, un système satisfaisant pour la gestion de clefs cryptographiques, aussi connu comme une infrastructure de clef publique (PKI), doit assurer la distribution de clefs publiques ainsi que la légitimité de noeuds, la génération de clefs, leur disponibilité, leur stockage et leur révocation. Cependant, la conception des systèmes de gestion de clefs pour les réseaux sans fil auto-organisés est une tâche difficile en raison de leur auto-organisation et l'absence d'entité centrale. De plus, les changements de paradigmes du réseau vers l'informatique omniprésente et la dépendance croissante dans la technologie des réseaux sans fil obligent la conception de systèmes de gestion des clefs plus fiables, survivants et évolutifs.

Ce chapitre présente un système PKI survivant qui vise à assurer les opérations de gestion des clefs, même en face d'attaques ou d'intrusions. Notre PKI est basé sur l'architecture SAMNAR et sur la corrélation des différents types de preuves afin de prouver la corrélation entre des utilisateurs et leurs clefs publiques. L'architecture SAMNAR propose la coopération entre les lignes de défense préventive, réactive et tolérante en vue d'aboutir à la survivabilité du réseau. De plus, les relations sociales entre les utilisateurs du réseau sont utilisées comme preuve pour soutenir les décisions relatives aux possibilités de survivabilité. Nous évaluons la survivabilité de notre PKI avec des simulations. Les résultats démontrent des améliorations en termes d'efficacité et de capacité de survivabilité aux attaques.

Le chapitre est organisé en cinq sections, comme suit. La section 5.1 présente les initiatives corrélées aux systèmes survivant de gestion de clefs. La section 5.2 décrit le réseau et les modèles d'attaque considérés dans l'étude de cas. La section 5.3 détaille le système survivant en soulignant ses principales opérations: la création de la clef publique et des certificats, les échanges, la révocation des certificats et l'authentification. La section 5.4 présente la méthodologie d'évaluation

utilisée, l'environnement de simulation et les résultats. Enfin, la section 5.5 conclut le chapitre.

Les modèles et les hypothèses

Le modèle du réseau : Nous considérons un réseau multi-sauts ad-hoc composé de n noeuds mobiles ou fixes identifiés par $X_1, X_2, X_3, ..., X_n$. Le réseau est auto-organisé et les noeuds sont distribués au hasard sur une surface géographique. Les noeuds se déplacent sur cette surface en suivant un modèle de mobilité. Aucune entité centrale n'existe pour soutenir les services du réseau, tels que le routage, le contrôle d'accès ou la gestion du réseau. Ainsi, les noeuds ont des fonctionnalités similaires et contribuent à la maintenance du réseau, au routage et au processus de gestion de clefs publiques. Cependant ils possèdent des ressources limitées comme la capacité de calcul, la mémoire et des capacités de stockage.

Deux noeuds donnés, X_i et X_j, ont un lien physique sans fil, si leur distance euclidienne n'est pas supérieure au rayon de communication (r), alors X_i et X_j sont appelés voisins à l'égard l'un de l'autre. Un chemin d'accès physique entre deux noeuds, par exemple, X_i et X_k, est un ensemble de liens physiques sans fil. Deux noeuds sont physiquement connectés, s'il y a un chemin d'accès physique à partir de l'un et se terminant à l'autre. Nous appelons réseau physique l'ensemble des liaisons physiques sans fil. Aucun noeud n'a une connaissance complète de la topologie physique du réseau nécessitant ainsi en routage pour communiquer avec les noeuds qui sont dehors de son rayon de communication.

Le modèle de confiance : la fiabilité parmi les noeuds dépend de l'amitié existante entre les utilisateurs qui participent au réseau. Si deux utilisateurs, par exemple, I et J sont des amis, ils se font mutuellement confiance et leurs dispositifs respectifs, X_i et X_j, peuvent échanger leurs clefs publiques. Un noeud donné fait confiance à l'autre si leurs utilisateurs ont échangé leurs clefs publiques à travers un canal parallèle (par exemple, sur un canal infrarouge) au moment d'une rencontre physique. Nous envisageons une fiabilité bidirectionnelle entre deux noeuds, cela veut dire que si X_i fait confiance à X_j, X_j va aussi croire X_i. Cette hypothèse est fondée sur l'analyse statistique du *Web of Trust* entre les

utilisateurs de PGP. Cette analyse montre que près de deux tiers des liens dans le grand réseau social sont étroitement liés de façon bidirectionnelle.

Nous supposons l'existence d'un système de réputation. Il permet à tous les noeuds de localement évaluer le comportement de ses voisins par l'observation et par des informations de seconde main. Chaque noeud dans le réseau physique maintient une table avec les valeurs de la réputation de tous les noeuds voisins. Les valeurs de réputation sont comprises dans l'intervalle [0.0,1.0] et représentent le comportement des noeuds par rapport au fonctionnement du réseau.

Chaque noeud possède également un niveau préventif qui est une valeur normalisée dans l'intervalle [0.0,1.0]. Il représente combien le noeud est protégé contre les attaques qui essaient de lui compromettre individuellement. Le niveau de prévention est automatiquement calculé à partir de l'existence de mécanismes de prévention, tels que des pare-feux individuels, des anti-virus, des spywares et d'autres. Les mécanismes de prévention permettent de compenser les gros dommages produits par les noeuds individuels. Nous considérons que le niveau de prévention est calculé et stocké de manière sécurisée et que sa manipulation par des utilisateurs malveillants est difficile. Des logiciels tamper-resistants peuvent être utilisés pour stocker de manière sécurisée les niveaux de prévention.

Le modèle des menaces : différents types d'attaques peuvent nuire les PKIs dans les réseaux sans fil auto-organisés. Nous nous concentrons sur les attaques qui peuvent compromettre les principes de disponibilité, confidentialité, intégrité, authenticité et non-répudiation dans le système de gestion de clef publique. Nous considérons un scénario d'attaque où l'adversaire est capable de compromettre un ou plusieurs noeuds et, par conséquent, de denier ou retarder les fonctions du système de gestion des clefs. Plus précisément, nous traitons les attaques suivantes: Sybil, mascarade et déni de service (DoS).

- L'attaque Sybil: les attaques Sybil se produisent lorsque les noeuds adversaires créent des identités multiples dans le PKI en vue de manipuler des clefs et des certificats à leur avantage. Les fausses identités des noeuds peuvent apparaitre comme des légitimes et, par conséquent, ces noeuds peuvent violer les principes de la confidentialité, de l'authentification et de la non-répudiation.

- L'attaque par mascarade: un noeud malveillant peut forger l'identité d'un noeud légitime et porter atteinte aux principes de la non-répudiation et de l'authentification. Des noeuds malicieux peuvent participer au système de gestion des clefs comme s'ils étaient des noeuds légitimes. De plus, par cette attaque, les noeuds peuvent compromettre les principes d'intégrité et de confidentialité des messages.

- Le déni de service (DoS): un noeud qui a une mauvaise conduite peut cesser de fournir le service d'authentification, ainsi que le service de stockage des clefs, ou la production, la distribution ou la révocation des certificats. Par conséquent, il diminue le bon fonctionnement des services de gestion des clefs. La motivation pour cette attaque peut être l'économie des ressources, comme le stockage ou le processeur, tandis que le noeud participe au système de gestion des clefs. Cependant, un noeud compromis peut participer au système de gestion de clefs pour l'endommager. Ces attaques sont également appelées manque de coopération dans notre cas d'étude.

Notre PKI suit le paradigme *WAN-en-LANS*. Ce paradigme propose la création de régions/groupes avec différents niveaux de fiabilité en vue de parvenir séparément à la capacité de survivabilité de chaque domaine, puis d'atteindre la survivabilité de tout le PKI. Le paradigme ne définit pas le niveau de granularité du groupe, qui peut être un seul noeud. Notre PKI définit trois principaux niveaux de fiabilité: le niveau du noeud, le niveau du groupe initiateur et le niveau du système. Ces trois niveaux visent à atteindre les exigences de survivabilité pour le système de gestion des clefs publiques, en particulier, la décentralisation, le passage à échèle et l'auto-organisation.

Chaque noeud est individuellement responsable pour parvenir à la survivabilité du PKI. Un noeud génère sa paire de clefs, privé et publique, et il a besoin de distribuer sa clef publique. Le noeud doit s'assurer que sa clef publique ne sera pas falsifiée ou mise à jour par des noeuds malveillants, mais aussi de que la disponibilité du matériel cryptographique. Par conséquent, il emploie des mécanismes de sécurité préventifs et réactifs pour se protéger contre les attaques

ou les intrusions. Des certificats numériques, par exemple, établissent la responsabilité des noeuds en relation avec leurs clefs publiques et les pare-feux personnels offrent une protection individuelle pour le noeud. De plus, le noeud possède des informations sur la réputation des noeuds prochains afin d'aider à choisir avec quels noeuds il échangera ses clefs publiques. La paire de clefs peut être stockée dans un firmware spécial ou dans un espace du disque dont l'accès est limité par un mot de passe.

Des groupes initiateurs assurent les propriétés de survivabilité dans notre PKI. Un groupe initiateur est composé de noeuds qui se font confiance entre eux en signifiant que chacun d'eux a mutuellement échangé ses clefs publiques par un canal secondaire suivant la relation d'amitié existante parmi leurs propriétaires. Les groupes initiateurs aident à la distribution des clefs publiques et assurent la conformité entre la clef publique et l'identité du noeud d'une manière décentralisée. Les groupes initiateurs favorisent également la redondance. Les membres d'un groupe agissent comme témoins lors de l'échange des clefs publiques entre une paire de noeuds. De plus, un noeud peut participer à différents groupes initiateurs en générant des noeuds en commun entre les groupes.

Notre PKI dépend des groupes initiateurs pour l'exécution de nombreuses opérations. Chaque groupe initiateur est propriétaire de sa paire de clefs. Sa clef privée est utilisée pour la signature numérique des certificats délivrés par les membres du groupe. Les certificats de clef publique sont utilisés pour lier une clef publique à une identité. C'est pourquoi dans notre PKI nous avons deux types de certificats de clefs publiques: les certificats de noeud et les certificats de groupe. Les certificats de noeud assurent que les clefs publiques sont liées aux identités des utilisateurs, alors que les certificats de groupe associent les clefs du groupe avec l'identification du groupe. Les certificats de noeuds sont signés avec la clef privée du groupe dans lequel le noeud participe. Les certificats de groupe sont signés par la clef privée d'un autre groupe.

Nous utilisons un modèle abstrait basé sur la théorie des graphes pour soutenir l'explication des opérations de PKI. Cette approche a été utilisée par Hubaux et. al et Maurer et. al. Toutefois, dans notre modèle, seuls les certificats publics de groupe et les clefs publiques des groupes sont représentés dans une graphie identifiée par G (V, E). Les clefs publiques de groupes composent l'ensemble des

sommets V et les certificats de groupe composent l'ensemble d'arêtes orientées E. Nous appelons G la graphie de certificat de groupe. Chaque sommet du graphe correspond à un ensemble de noeuds, à leurs clefs publiques respectives et aux certificats de noeud. Ainsi, nous supposons qu'en arrivant à un certificat de groupe, le système arrivera aussi à un certificat de noeud dans le groupe.

Les sommets et les arêtes d'un graphe G possèdent des coefficients de pondération. En sachant que chaque noeud est associé à un niveau préventif et à un niveau de réputation, le poids des sommets de G représente le niveau minimum de prévention entre le niveau de prévention de tous les noeuds du groupe initiateur. De la même façon, le poids des arêtes de G représente le minimum niveau de réputation entre les toutes les valeurs de réputation des noeuds dans un groupe initiateur. La valeur minimale de niveaux de prévention ou de la réputation démontre la faiblesse du groupe par rapport à des lignes de défense préventive et réactive. Dans notre système, lorsqu'un noeud a besoin d'authentifier une clef publique d'un autre noeud, il cherche au moins deux chaînes disjointes valides de certificats de groupe, à partir de son groupe jusqu'au groupe initiateur du deuxième noeud.

L'objectif principal de nos évaluations est d'analyser la faisabilité de nos hypothèses, de montrer la capacité de survivabilité de notre PKI contre les attaques et de quantifier son coût de communication et d'efficacité. Nous avons évalué la viabilité des groupes initiateurs et nous avons observé une plus forte probabilité de former des groupes de 4 ou 5 membres. Nous avons analysé le coût des communications pour l'accomplissement les opérations principales de notre PKI. Et nous avons évalué la capacité de survivabilité de notre PKI avec différents pourcentages d'attaques DoS (appelées aussi attaques par la manque de coopération) et d'attaques Sybil.

Pour l'évaluation de la survivabilité, nous avons défini un ensemble de mesures telles que la convergence dans l'échange de certificats de groupes, la taxe d'authentification des utilisateurs, la taxe des groupes parvenues, le pourcentage de groupes non-compromis et le pourcentage d'authentifications non-compromises. Les résultats de simulation ont démontré que notre PKI exige moins de secondes pour converger que d'autres PKIs. De plus, nous avons observé un pourcentage élevé de certificats de groupe parvenus ou d'authentification d'utilisateurs, même en

présence d'un pourcentage élevé d'attaques DoS. En ce qui concerne les attaques Sybil, même en présence d'un pourcentage élevé de noeuds faux dans le PKI, nous observons encore un pourcentage élevé de groupes ou d'authentifications qui n'ont pas été compromis par des noeuds faux. En ce qui concerne le meilleur nombre de membres dans un groupe initiateur, en général, les meilleurs résultats ont été obtenus lorsque les groupes possèdent 4 ou 5 membres.

Résumé du chapitre 6 : Des directions pour la survivabilité dans la couche de liaison

Le chapitre 6 fournit des orientations de recherche pour atteindre la survivabilité dans la couche de liaison, plus particulièrement dans la connectivité. Même si la connectivité sans fil dans la couche liaison peut être fournies par différents technologies de communication, nous prenons comme référence la technologie de la radio cognitive (CR) car elle présente naturellement l'une des propriétés de la survivabilité : l'adaptation. Cette technologie a été envisagé afin d'offrir une bande passante élevée pour les utilisateurs mobiles grâce à des techniques d'accès dynamique et à l'utilisation optimale des fréquences du spectre radioélectrique. La radio cognitive propose des concepts pour l'accès opportuniste au spectre et la capacité de partager les canaux sans fil avec les utilisateurs titulaires d'une licence (aussi connus comme les principaux utilisateurs). Nous présentons des directions pour arriver à la survivabilité en considérant la perspective des utilisateurs sans licence. Ces utilisateurs, également appelés utilisateurs secondaires ou cognitives, peuvent exploiter de manière adaptative le spectre sans compromettre les opérations de l'utilisateur principal.

La sécurité a reçu peu d'attention sur le lien sans fil, en particulier, la connectivité dans la couche de liaison, en particulier, dans la technologie de la radio cognitive. Des entreprises, des agences gouvernementales et les chercheurs ont mis l'accent sur le développement de la gestion des fréquences du spectre radioélectrique sans traiter les questions de sécurité. Des protocoles, des architectures et les normes ont été créés, mais peu d'entre eux considèrent l'emploi des mécanismes de sécurité. De plus, les propositions se restreignent à l'application de techniques classiques de sécurité, telles que la cryptographie, les systèmes

de détection d'intrusion et l'authentification. Le standard IEEE 802.22, par exemple, fournit une sous-couche de sécurité conçue afin d'assurer la confidentialité, l'authentification et l'intégrité des données via des transformations cryptographiques dans les unités de données MAC.

Cependant, les mécanismes classiques de sécurité ne sont pas suffisants pour prévenir la connectivité sans fil de la couche de liaison contre les attaques et les intrusions. Les mécanismes de sécurité préventive, comme la cryptographie, la confidentialité, l'intégrité et l'authentification sont en général inefficaces contre les surcharges, l'interception ou la manipulation telles que les attaques DoS et le jamming. Les mécanismes de sécurité réactive, comme les systèmes de détection d'intrusion (IDS), sont basés sur l'analyse du comportement du réseau ou sur le comportement des attaques connues et les actions d'intrusion. Les nouvelles technologies de communication étant plus dynamiques et adaptables, les attaques sont contraintes d'être plus intelligent afin de facilement contourner ces mécanismes de sécurité.

Basées sur l'architecture SAMNAR, nous fournissons des directions pour un framework pour la survivabilité dans la couche de liaison en utilisant la technologie de radio cognitive. Le framework suit une approche multicouche afin d'analyser la situation du réseau et de prendre les décisions adéquates pour les paramètres de sécurité. Le framework a l'intention d'offrir l'auto-reconfiguration aux mécanismes de sécurité telles que leurs valeurs de paramètre, la taille de la clef cryptographique, l'algorithme de cryptographie, des règles et des politiques.

Nous avons pris comme référence le framework pour la gestion du spectre de la radio cognitive proposé par Akyildiz al. al et nous y avons ajouté des aspects de sécurité pour une connectivité survivante dans la couche de liaison. Dans notre framework, la survivabilité dans la couche de liaison est appuyée sur des informations et des décisions prises par différentes couches de la pile protocolaire. Cette caractéristique est attendue dans l'architecture SAMNAR. Dans ce framework, l'échange d'informations entre les couches est assuré par le module de communication inter-couche. Ce module est constitué de techniques pour enregistrer et recueillir des informations de différentes couches. L'information est, en général, liée à l'environnement réseau et, en particulier, elle peut concerner les besoins de QoS, le délai de transfert de paquets, la perte de paquets, le routage

de l'information et le délai dans la couche de liaison. Le module de communication inter-couche peut également prévoir des mécanismes pour prétraiter les informations. Il envoie ensuite des informations vers le module de contrôle. Le module inter-couche possède des fonctionnalités définies dans le module de collecte et dans la composante inter-couche du module de communication conçu dans l'architecture SAMNAR.

Un module de coopération est défini dans le framework. Ce module possède la totalité des fonctionnalités définies sur la composante de communication inter-noeud de l'architecture SAMNAR. Il est composé de techniques pour assurer la communication entre les noeuds. De plus, il a comme entrées des informations sur la disponibilité des bandes de fréquences identifiées par les techniques utilisées dans le module de détection du spectre. La coopération entre les noeuds apporte des entrées pour la caractérisation du spectre où le comportement du spectre est évalué ainsi que les activités des utilisateurs secondaires et principaux.

Le module de contrôle est le coeur du framework. Il est chargé d'analyser les informations reçues des autres modules, de faire des inférences et de prendre des décisions à propos de l'adaptation nécessaire. Le module de contrôle envoie des décisions prises pour le module de reconfiguration. Ce module définit les mieux mécanismes de sécurité à être utilisés dans les modules de la résistance, de la récupération et de la reconnaissance basée sur les analyses du module de contrôle. Les reconfigurations de sécurité sont également influencées par les besoins de QoS requis par les applications.

Résumé du chapitre 7 : Conclusions

Le chapitre 7 présente les conclusions de la thèse et les orientations futures. L'objectif est de renforcer nos contributions et de souligner certaines directions de travaux futurs. Par conséquent, nous soulignons d'abord les principales contributions de la thèse dans la section 7.1. Puis, nous présentons dans la section 7.2 les limitations et les orientations de recherche dans ce domaine. Enfin, dans la section 7.3, nous présentons la liste des publications résultant de cette thèse.

Certaines limites peuvent être identifiées dans l'état actuel de ce travail. De telles limitations conduisent aux orientations futures. Tout d'abord, SAMNAR

est une architecture conceptuelle et générique qui provient des directions pour parvenir à la survivabilité dans les réseaux sans fil auto-organisés. Comme l'objectif principal d'une recherche est de développer des solutions plus pratiques, SAMNAR doit être utilisée vers la définition d'un framework, ses fonctions et la mise en uvre d'une API (Application Program Interface) afin de permettre son use pratique. De plus, le cadre doit prendre en considération les différences dans les études de cas. Il faut également de la flexibilité pour permettre l'ajout de nouvelles fonctions lorsque nécessaire.

Une autre limitation dans cette thèse est liée à des paramètres pour l'évaluation de la survivabilité. En fait, la façon de mesurer la survivabilité est un sujet qui produit de nombreuses discussions dans ce domaine. Ainsi, la définition de paramètres spécifiques de cette proposition est une demande. Nous avons inclus dans cet ouvrage quelques mesures nouvelles avec cette proposition, cependant, de notre point de vue, ce n'est pas suffisant. Nous envisageons encore un long chemin avec des discussions sur ce sujet considérant les caractéristiques des réseaux sans fil auto-organisés.

Cette thèse présente aussi des limites en ce qui concerne le module de communication de l'architecture SAMNAR. Nous ne traitons pas par exemple les problèmes de communication liés à la diffusion de l'information. En raison de la décentralisation, caractéristique d'auto-organisation des réseaux sans fil, nous croyons que des solutions doivent être proposées afin de minimiser l'impact sur les performances et d'améliorer leur efficacité. De plus, les besoins de la survivabilité et la situation du réseau doivent être considérés. La création d'une stratégie de communication qui peut s'adapter ou modifier les techniques utilisées en fonction de la situation du réseau est une bonne direction de recherche. Le développement de solutions d'adaptation, d'algorithmes et deprotocoles en considérant des aspects de survivabilité du réseau.

UNIVERSITY OF PARIS 6
UNIVERSITAS

THESIS

Submitted for the degree of
Doctor of Philosophy

By
Michele Nogueira Lima

Title :

SAMNAR: A SURVIVABLE ARCHITECTURE FOR WIRELESS SELF-ORGANIZING NETWORKS

Defense: October, 6^{th} 2009

Advisor:
Guy PUJOLLE

Committee

Khaldoun AL AGHA	Professor at Paris-Sud11 University
M. José M. NOGUEIRA	Professor at University of Minas Gerais
M. David POWELL	CNRS researcher at LAAS
M. Serge FDIDA	Professor at UPMC
M. Pascal URIEN	Professor at Telecom ParisTech
M. Guy PUJOLLE	Professor at UPMC (Advisor)

To my beloved *family* and my beloved *friends*.
Each of you has a special place in my heart and memory forever.

Acknowledgements

I do not have words to say how much I am thankful for all people that directly or indirectly contributed and supported me along this thesis. First, I would like to thank my advisor, Prof. Guy Pujolle, that has believed in my abilities and my autonomy for developing this work. He always offered me the means and opportunities for professional progress. I am grateful for the members of my Thesis' committee. Thank you for accepting the invitation. I thank Prof. David Powell for my visit at LAAS/CNRS and for his comments to improve my research. I thank Prof. Khaldoun Al Agha for practical discussions and for encouraging my progress. I thank Prof. José Marcos Nogueira for following my advance since my master degree and for opening professional perspectives. I am grateful for all financial support from Brazilian Government by CAPES, Ministry of Education, and I thank Prof. Geraldo Robson, Prof. Placido Pinheiro and Prof. Dorgival Guedes for all assistance with recommendation letters.

I would like to thank my colleagues at LIP6 and Phare team. All discussions, issues, problems, and negative or positive critics had a great impact on my professional and personal life. All situations I have experienced persuaded me towards my advances, and I am very grateful for this. Particularly, I would like to thank people from the office 803, Sondes Khemiri, Nadjib Ait Saad, Zeinab Movahedi, Shahab Gashti and Mathieu Bouet, as well as Moez Esseghir, Meriem Kassar, Tara Ali Yahaita, Samir Ghamri Doudane and Badis Tebbani. I also thank Véronique Varenne, Raymonde Kurinckx, Clémentine Pellissier, Aziza Lounis, Konstantin Kabassanov and Laetitia Jacquey for all administrative support. I hope that our friendship can stay for long time.

I thank all Brazilian people at LIP6: Daniel Cunha, Daniel Macedo, Pedro Velloso and Marcelo Amorim. Thank you for all assistance and information about cultural differences.

I would like to thank Prof. Ian F. Akyildiz for the possibility of visiting the BWN lab/GeorgiaTech. I had learned very much with this experience and I had made friends for forever: Aravind Kailas, Maria Gregori, Kaushik Chowdhury, Josep Miquel Jornet, Massimiliano Pierobon, Pu Wang, Berk Canberk, Brandon Lo, Claudia Cormio, Won Yeol Lee and Lluis Giné. Special thanks to Angela Roggenhofer and Gregory Jennings for all your efforts to make unique my stay in Atlanta. Also, thank you for English improvements in my thesis.

Thank you so much, my dear friends, Anna, Dominique, Gaby, Philippe, Alzennyr, Juliana, Menotti, Simon, Ligia, Yosra, Mathias and Perrine. I know, I need to go out often, but I hope you know that your support and free time together gave me the force to overcome all the difficulties of this period. I never will forget inline skating time, or our trips as that one in New Orleans. My deepest thanks to my longtime friends: José Pinheiro, Viviane, Laura, Talita, Lilian, Rosanne, Claudio, Fabricio, Marcelo, Adriano, Yuri and Helio. Thank you for sentences like: "*fear does not match with you*", "*you can, girl!*", "*I am so proud of you*" or "*is it done?*". You cannot imagine how these sentences helped me.

Thank all people that worked closer to me, particularly, Eduardo Silva and Helber Silva. I know, it was time of deadlines and efforts. I am grateful of your courage. Observe how much we learned and improved.

I thank my family for all love, support and efforts. Thank my mother and my aunts who had a great role in this process.

Finally, I would like to express my deepest sense of gratitude for Aldri Luiz dos Santos. I do not know how things could have been otherwise. I just know that we *survived* two theses, and this represents many things to me. I really appreciate your love and support for making my dreams real.

Abstract

This work presents a survivable architecture for wireless self-organized networks. First, we survey the stat-of-the-art of survivability in these networks, allowing us to identify open issues and highlight their survivability requirements and properties. Assessing the existing initiatives of survivable protocols, architectures and models, we propose SAMNAR, a conceptual architecture inspired on the human body immune system. SAMNAR's goal lies in the maintenance of network essential services, as link-layer connectivity, routing and end-to-end communication, even in the presence of attacks or intrusion.

SAMNAR employs a new approach for security management. Since three defense lines are identified as preventive, reactive and tolerant, SAMNAR proposes that survivability can be achieved by the coordinated use of these three defenses in an adaptive way. Its approach consists in developing different levels of obstacles for attacks and intrusions. Preventive security mechanisms, such as cryptography, firewalls or access control, are the first protection of the network blocking attacks. Reactive security mechanisms, such as intrusion detection systems, are the second protection, detecting and reacting against intrusions, that is, successful attacks. Tolerant security mechanisms are the third protection, mitigating intrusion or attack effects until the network can adapt preventive or reactive defense lines in order to control attacks or intrusions.

We apply SAMNAR in two case studies. The first case study is performed taking into account the routing essential service. It proposes a survival path selection scheme in which criteria provided by three defense lines are correlated. Fuzzy logic is used to analyze these inputs,

make inferences and decide the most survivable path. We evaluate the survival path selection scheme by simulations and in the presence of different attacks. Results show that improvements can be reached in terms of packets dropped due to attacks or intrusions. Further, in terms of latency and packet delivery ratio, results show a similar behavior between protocols using our scheme and the original version of those protocols.

The second case study proposes a survivable public key management system (PKI). Since key management systems are necessary for enforcing integrity, confidentiality, authentication and non-repudiation in essential services, we develop a PKI aiming to manage and distribute cryptographic keying material in a survivable way. Our PKI is fully decentralized using different evidences to prove the liability of users for their public keys. These evidences resulted from the coordination among three defense lines, such as the use of personal firewalls as preventive security mechanism, reputation system as reactive security mechanism, and redundancy as tolerant security mechanism. Further, social relationships among users are also used as evidences supporting the generation of groups in the system, increasing the tolerance against attacks or intrusions. We use simulations to evaluate our survivable PKI under different attacks or intrusions, particularly, Sybil and lack of cooperation. Results present the practical viability of group formation and a high percentage of groups or node authentication non-compromised by attacks or intrusions even in the presence of high percentage of misbehavior nodes. Further, the survivable PKI achieves the maximum convergence of all certificates in the system.

Finally, we employ SAMNAR in the link-layer connectivity essential service. We provide directions for a survivable framework considering the use of cognitive radio technology due to their natural characteristic of adaptation, one of the survivability properties. The framework is composed of different functions and it extends the spectrum management framework existent in the literature.

Contents

List of Figures

Chapter 1

Introduction

Improvements on wireless networking have increased the importance of distributed systems in our everyday lives. Network access is becoming ubiquitous through portable devices and wireless communications, making people more and more dependent on them. This raising dependence claims for simultaneous high level of reliability, availability and security on commercial, financial, medical and social transactions supported by pervasive and wireless distributed systems.

Self-organizing wireless networks, ad hoc, mesh and sensor networks, are examples of pervasive distributed systems. These networks are composed of heterogeneous portable devices, called nodes, communicating among themselves in a wireless multi-hop manner [119]. Self-organizing wireless networks can autonomously adapt to changes in their environment such as device position, traffic pattern and interference. Each device can dynamically reconfigure its topology, coverage and channel allocation in accordance with changes. Further, no centralized entity controls the network, requiring a decentralized management approach.

Security is crucial to self-organizing wireless networks, particularly for security-sensitive applications on military, homeland security, financial and health care domains. Security threats take advantage of protocol faults and operating systems' vulnerabilities as well as network characteristics. These networks pose nontrivial challenges to security design due to their characteristics such as shared wireless medium, highly dynamic network topology, multi-hop communication and low physical protection of portable devices [86, 113]. Moreover, the absence of central

entities increases the complexity of security management operations, particularly access control, node authentication and cryptographic key distribution.

Several security solutions have been proposed [40, 60, 63, 73, 83, 115, 118]. These solutions have employed two defense lines, preventive or reactive, in which the former attempts to thwart attacks by cryptography, authentication and access control mechanisms, and the latter seeks to detect intrusions and react accordingly [5]. However, each security mechanism addresses specific issues having limitations to deal with different types of attacks and intrusions. Preventive defenses, for example, are vulnerable to malicious nodes that already participate in network operations, and reactive ones work efficiently only against well-known attacks or intrusions.

Due to the limitations of preventive and reactive defense lines, researchers have applied in the last few years another defense line called intrusion tolerance [113]. This defense line intends to improve the network resilience against attacks and intrusions using fault-tolerance techniques, typically redundancy and recovery mechanisms. However, security solutions remain still focused on one specific issue or layer of the protocol stack, being ineffective to ensure essential services of self-organizing wireless networks.

Network characteristics as well as constraints on defense lines reinforce the fact that no network is totally immune to attacks and intrusions. Therefore new approaches are required to guarantee integrity, confidentiality, authentication and, especially, availability of network services. Such requirements motivate the design of survivable network services for self-organizing wireless networks. Survivability is the capability of a network to support essential services even in face of attacks and intrusions [54]. In this work, we highlight the delivery of data bits from one node to another as fundamental network functionality and we focus on three essential services: *link-layer connectivity*, *routing* and *end-to-end communication*. We argue that survivability is achieved when a cross-layer solution integrates preventive, reactive and tolerant defense lines in a self-adaptive and coordinated way.

This chapter is organized as follows. First, we describe the problem addressed by this work and its objectives. Next, we present its contributions. Finally, we outline the organization of the remaining chapters.

1.1 Problem Description and Objectives

The problem tackled in this work consists in providing an architecture for security management in order to make self-organizing wireless networks survivable to attack and intrusion. Albeit there are many security solutions for those networks, they use different security mechanisms separately without providing the integration and cooperation among them. Moreover, those solutions do not take into account the particularities of the network such as its requirements and characteristics.

This work presents a general discussion about survivability in self-organizing wireless networks, allowing us to identify open issues, survivability requirements and its implications regarding particularly network characteristics. This discussion surveys related works applying survivability concepts on self-organizing wireless networks. Based on the survey, we design the SAMNAR architecture, whose goal is to support the operation of essential services even in the presence of attack and intrusion. As showcases, SAMNAR is employed on routing and cryptographic key management services resulting, respectively, in a survival path selection scheme and a survivable key management system. Lastly, we propose a framework based on SAMNAR that considers adaptable link layer connectivity using cognitive radio technology.

1.2 Contributions

We summarize the contributions of this thesis as:

- **A survey of survivable initiatives for self-organizing wireless networks.** The survey provides an overview of employing survivability concepts on the domain of self-organizing wireless networks. Survivable initiatives and architectures are presented and contextualized, emphasizing the relevance of our contributions. As a result, the survey allows us to identify open issues and opportunities to use survivability concepts in these networks.

- **SAMNAR: survivable architecture for self-organizing wireless network.** Assessing existing survivable initiatives, solutions, architectures and protocols, we design a survivable architecture for self-organizing wireless networks called SAMNAR. This architecture is inspired on the human body immune system and proposes an adaptive security management approach to achieve survivability in the presence of attack and intrusion. SAMNAR offers the coordinated and adaptive use of preventive, reactive and tolerant defense lines.

- **Survival path selection scheme.** SAMNAR has been employed on the routing service resulting in a survival path selection scheme. The proposed scheme is independent of any routing protocol and consists in identifying the most survivable paths. The selection scheme takes into account several criteria that correlate network conditions with three defense lines. Simulation results show the mitigation on the impact of different routing attacks with low performance loss for the investigated network.

- **Survivable key management.** This contribution consists in a survivable Public Key Infrastructure (PKI) aiming to efficiently manage and distribute cryptographic keys even in face of attacks or intrusions. The PKI is based on the SAMNAR architecture, on social relationships of users, and on the correlation of different types of evidences to prove the liability of users for their public keys. Simulation results and analytical models highlight the improvements reached by the survivable PKI in terms of effectiveness and survivability to attacks.

- **Directions for a survivable link-layer connectivity.** A framework is proposed considering a reconfigurable link layer connectivity, specifically, using cognitive radio technology. This framework based on SAMNAR considers the characteristics and the operations of spectrum management.

1.3 Thesis Organization

This thesis is structured into seven chapters and two appendixes. Chapter 2 presents an overview of secure management and survivability concepts, as well as the requirements and properties of survivability. Chapter 3 describes the proposed architecture, SAMNAR, emphasizing its modules and the security management approach based on the adaptive coordination of preventive, reactive and tolerant defense lines. A survival routing path selection scheme is presented in Chapter 4. This scheme based on SAMNAR uses Fuzzy logic to correlate conventional and security criteria in order to choose the most survivable routes. Conventional criteria are those characterizing the network environment and condition, whereas security criteria result from preventive, reactive and tolerant security mechanisms. Chapter 5 presents the survivable key management infrastructure in which different kinds of evidence are applied to prove the liability of users for their public keys. Chapter 6 proposes a framework to accomplish survivability on link-layer connectivity considering particularly cognitive radio technology. Chapter 7 concludes the thesis, presents the limitations of the survivable architecture and provides directions for future work. Finally, Appendix A describes initiatives on building survivable routing protocols for self-organizing wireless networks, and Appendix B presents the set of Fuzzy rules used for evaluating the survival path selection scheme proposed in Chapter 4.

Chapter 2

Security Management & Survivability Overview

Network management is indispensable for self-organizing wireless networks. These networks are distributed systems composed of heterogeneous hardware, software and protocols produced by various organizations and vendors. Providing a successful integration among these different components is crucial to maintain the operation of essential network services such as link-layer connectivity, routing and end-to-end communication [78]. Network management is employed to control and monitor such integration, individual components and the operation of essential services. Moreover, it helps network designers to handle faults, reduce costs and deal with unexpected network situations such as the presence of attacks or intrusions.

Security management is one of the key research challenges on self-organizing wireless networks [88]. It is a functional area of network management [94], consisting of facilities to control security mechanisms and services and, then, thwart attacks or intrusions. Due to network characteristics and the inefficiency of conventional security mechanisms to put all attacks and intrusions off [25, 103], new security management approaches are required. Moreover, the raising dependence of people on computers and networks results in a high expectation that self-organizing networks should be dependable and present robust performance. Hence, researchers and industry have employed a survivable perspective to secu-

rity management, supporting the integration between security and dependability domains.

This chapter provides an overview of security management and survivability concepts, as well as security threats and survivability requirements for self-organizing wireless networks. It is organized in five sections as follows. Section 2.1 analyzes the security threats in these networks. Section 2.2 presents the concepts of security management. It is followed by an overview of survivability concepts in Section 2.3 and by survivability requirements in Section 2.4. Finally, Section 2.5 concludes the chapter.

2.1 Security Threats

Self-organizing wireless networks are susceptible to many threats. Network characteristics such as dynamic topology, decentralized network architecture, shared wireless medium, low physical security of nodes and multi-hop communication result in different vulnerabilities and make difficult to maintain essential network services [4, 86, 108]. The decentralized architecture, for example, requires cooperation among nodes by one-hop or multiple hop connectivity without having guarantees that all nodes will cooperate as expected. The network autonomy, high dynamism of the topology and the lack of access control facilitate the participation of malicious or selfish nodes in network operations. Further, wireless communication is vulnerable to interference and interceptions, and the low physical security of nodes increases their possibilities of being tampered with.

This work addresses two specific threats, called attacks and intrusions. An **attack** is any action that explores a weakness of the network in order to compromise the integrity, confidentiality, availability and non-repudiation of information or network services. An **intrusion** also exploits weaknesses of the network, but it results from a successful attack. These two threats are classified as malicious faults in the dependability domain [54], consisting in malicious or selfish actions that intend to alter the functioning of a network or its nodes.

Malicious faults result in errors, meaning intentional deviations of the correct service operation in order to achieve malicious fault goals. Particularly, malicious fault goals are:

- to disrupt or halt services, causing the denial of services;
- to access or alter confidential information;
- to improperly modify the behavior of services and protocols.

Attackers are malicious entities (humans, nodes, services or software) that produce attacks or intrusions. Attackers attempt to exceed any authority they might have, seeking to achieve malicious fault goals. They take advantage of vulnerabilities produced by network characteristics, or weaknesses in network protocols, software or hardware. Examples of attackers include hackers, vandals, malicious software, and malicious or selfish nodes.

Three main classifications for attacks exist [108]. The first one is based on attack means being categorized as passive or active. Passive attacks intend to steal information and eavesdrop on the communication without provoking any disruption of data or services. Examples of passive attacks are eavesdropping, traffic analysis and traffic monitoring. Active attacks on the other hand involve service interruption, data modification or fabrication causing errors, network overload, or blocking nodes of effectively using network services. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

Attacks can also be classified as external and internal according to the participation of the attacker in the network. External ones are produced by attackers that are not legally part of the network, whereas internal attacks are generated by nodes participating the network operations. An attacker is not legally part of the network if it does not have the cryptographic material necessary to be authenticated or to participate of specific services such as routing.

Finally, attacks can be categorized based on which layers of the network protocol stack will be affected. Table 2.1 summarizes the main attacks on self-organizing wireless networks according to network layers. However, we emphasize that some of them are considered multi-layer such as DoS and Sybil ones, acting on more than one layer.

Some of these attacks are also classified as Byzantine or misbehaviors. In these attacks, attackers have full control of a number of authenticated nodes and

Layer	Attack	Description
Physical	Jamming	attackers generate deliberate interference to deny the target's use of a communication channel.
Link	Exhaustion	attacker induces repeated retransmission attempts aiming to exhaust target's resources.
	Collision	malicious nodes produce deliberate collisions or corruption in order to prevent the use of a link.
Network	Wormhole	pairs of malicious nodes cooperate to provide a low-latency side-channel for communication by means of a second radio with higher-power and long-range link. They intend to attract data traffic for this side-channel being easy to control the traffic or perform other attacks.
	Blackhole	malicious nodes manipulate routing packets in order to participate in routes and then drop data packets.
	Sinkhole	an attempt is made to lure traffic from the network to pass through an adversary in order to facilitate other attacks.
	Flooding	adversary nodes overload victim's limited resources: memory, processing or bandwidth.
	Selective forward or Glayhole	malicious nodes behave like normal nodes most of the time, but selectively drop sensitive packets for the application. This selective dropping is hard to detect.
	Sybil	multiple fake identities are created for adversary nodes, meaning that an attacker can appear to be in multiple places at the same time.
	Rushing	adversaries quickly forward their route request (RREQ) messages when a route discovery is initiated, in order to participate in any route. This attack can be carried out against on-demand routing protocols, as AODV [77], DSR [46] and others.
Transport	SYN Flooding	an adversary sends many requests of TCP connection establishment for a target node, overloading its resources.

Table 2.1: Attacks by network layers

behave arbitrarily to disrupt the network [10]. Blackhole, wormhole and rushing attacks are examples of Byzantine ones. Further, nodes can also present a selfish

behavior in which they take advantage of their participation in the network, but refuses to expend their own resources for cooperating with network operations [9].

2.2 Security Management

Security management is a set of facilities to protect networks and individual nodes from attacks, and to respond to changing user security requirements or network conditions. It owns as functions:

- controlling and monitoring security services and mechanisms;
- distributing security-relevant information;
- reporting security-relevant events;
- controlling the distribution of cryptographic keying material;
- authorizing subscriber access, rights, and privileges.

A security service is a set of operations provided by a protocol layer or communication system which ensures adequate protection to network resources, applications or data transfers [95]. These services are intended to counter attacks making use of one or more security mechanisms. The main security services are:

- **authentication** - the assurance that the communicating node or user is the one that it claims to be;
- **access control** - the prevention of unauthorized use of a network resource;
- **data confidentiality** - the protection of data from unauthorized disclosure;
- **data integrity** - the assurance that received data are exactly as sent by an authorized node or user;
- **non-repudiation** - the protection against denial by a node or user of having participated in all or part of the communication.

Security mechanism is a process designed to detect, prevent or recover the network from attacks or intrusions [95]. It can be independent of any particular protocol layer or be implemented in a specific one. In self-organizing wireless networks, security mechanisms follow two defense lines: preventive and reactive [108]. The former provides mechanisms to avoid attacks, such as firewalls and cryptography. The latter consists in taking actions on demand to detect misbehaviors and react against intrusions, such as intrusion detection systems (IDS) [43] or reputation systems [18]. The last ones address malicious and selfish issues by using nodes that track their neighbor's behavior and exchange this information with others in order to compute a reputation value about their neighbors. Reputation values are then used by nodes to decide with whom to cooperate and which nodes to avoid. Nodes with a good reputation are favored.

Albeit the efforts to improve preventive and reactive defense lines, these two defenses are not sufficient to put all attacks and intrusions off [25, 103]. Preventive defenses are vulnerable to internal attacks. Nodes participating legally in the network can perform network operations, as well as encryption and decryption, allowing malicious nodes to harm the integrity, confidentiality, availability and non-repudiation of data and services.

Reactive defenses work efficiently only against well-known intrusions. Intrusion detection systems, for example, require extensive evidence gathering and comprehensive analysis in order to detect intrusions based on anomalies or predetermined intrusion patterns. Anomalies are deviations of the network operation in relation to a behavior considered normal. Such behaviors are defined by baselines, being difficult in practice to determine them due to the dynamically changing topology and volatile physical environment of self-organizing wireless networks. Predetermined patterns are characteristics of known attacks and intrusions used for their detection. These patterns must be constantly updated to assure the IDS efficiency. Moreover, unknown or new attacks and intrusions will not be detected.

Due to these limitations on both defense lines, research groups have built security mechanisms towards a third defense line called **intrusion tolerance** (IT) [25]. This defense line complements the other ones and its goal is to mitigate the effects of malicious or selfish actions by the use of fault tolerance mech-

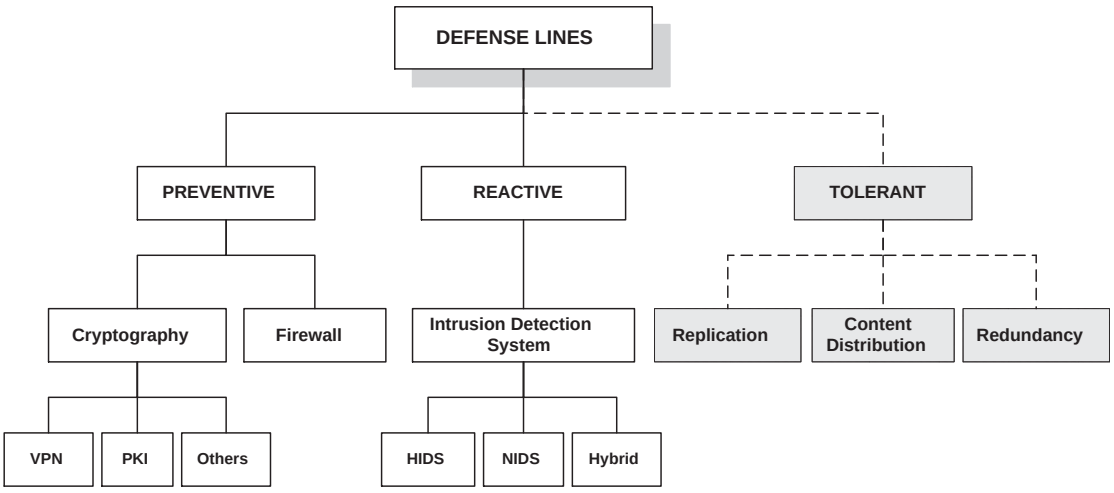


Figure 2.1: Classification of defense lines

anisms in the security domain [25, 97, 102, 104]. Intrusion tolerance emerged with Fraga and Powell's initiative [33], however, the development of such systems only had more attention in the last decade with the MAFTIA (*Malicious-and Accidental-Fault Tolerance will be Internet Applications*) [1] and OASIS (*Organically Assured and Survivable Information System*) [2] projects. Examples of fault tolerance mechanisms are data redundancy and replication. Figure 2.1 illustrates the organization of these three defense lines.

2.3 Survivability Concepts

Dependability is the ability of a system (node, network or service) to avoid failures that are more severe and frequent than it is acceptable. A failure is an event that occurs as consequence of errors - deviations of the correct service operation. Dependability is an integrating concept that encompasses as main attributes: availability, reliability, safety, integrity and maintainability. These attributes represent, respectively, the system's readiness for correct service, the continuity of correct service, the absence of severe consequences on the user and the environment, the nonexistence of improper system alteration and the ability to undergo modifications and repairs.

Security is a domain well developed with its own terms and concepts. Differently of dependability, it is a combination of the following attributes: confidentiality, integrity, availability, nonrepudiability, auditability and authenticity. These attributes represent the prevention of the unauthorized disclosure, deletion, withholding or amendment of data and information. Laprie *et. al* have analyzed the relationship among the attributes of both domains, supporting the integration between dependability and security [54].

In this work, survivability represents the new field of study resulted from the integration of security and dependability. Survivability allows systems to survive, limit damage, recover and operate robustly, particularly, in face of attacks and intrusions [29]. It is a system capability of providing essential services in the presence of malicious threats, and to recover compromised services in a timely manner after the occurrence of intrusions.

Survivability is important due to the characteristics of attacks and intrusions. These threats present different conditions and features in comparison with failures and accidents since they have intentional human causes. They are controlled by an intelligent adversary's mind, being hard to forecast when they will happen, as well as their effects. New attacks and intrusions have a high probability to occur exploiting different vulnerabilities of the system. Hence, attacks and intrusions can only be efficiently treated when analyzed separately, requiring attributes, such as those proposed by survivability, to address known forms of malicious faults and create defenses against new ones.

Requirements and key properties have been defined for survivability. Requirements are detailed in Section 2.4, whereas survivability properties are summarized as resistance, recognition, recovery and adaptability [97]. **Resistance** is the capability of a system to repel attacks. Firewalls and cryptography are examples of mechanisms used to reach it. **Recognition** is the system's capability of detecting attacks and evaluating the extent of damage. Examples of recognition mechanisms are intrusion detection systems using techniques such as pattern matching and internal system integrity verification. **Recovery** is the capability of restoring disrupted information or functionality within time constraints, limiting the damage and maintaining essential services. Conventional strategies applied for achieving recovery are data replication and redundancy.

Finally, **adaptability** is the system's capability of adapting to emerging threats and quickly incorporating lessons learned from failures [29, 97]. Examples of adaptation techniques are topology control by radio power management, active networking and cognitive radio technology. The application of active networking technology intends to allow the dynamic selection of MAC or network layer parameters, and the dynamic negotiation of algorithms and entire protocols based on application requirements or the communication environment [97]. Figure 2.2 illustrates the interaction among these key properties.

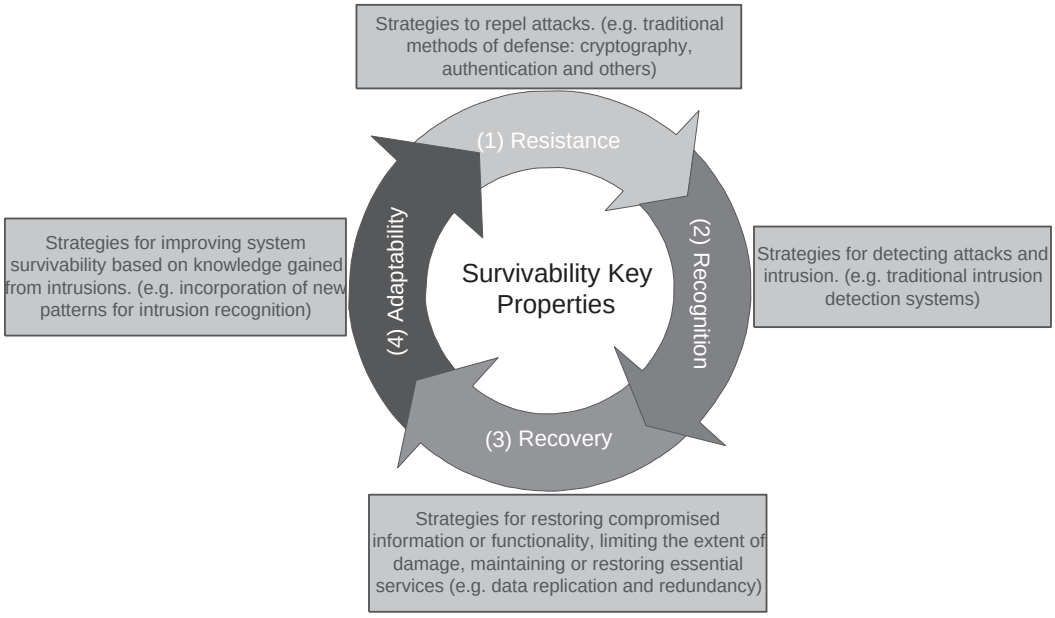


Figure 2.2: Survivability key properties

2.4 Survivability Requirements

Survivability requirements can vary substantially depending on system scope, criticality, and the consequences of failure and service interruption [29, 58]. Self-organizing wireless networks introduce diverse functions, operations and services influenced by the context and applications. In a critical situation where parts of the system are compromised by attacks or intrusions, priority is given to maintain

network connectivity in three levels: link-layer, routing and end-to-end communication. Hence, to reach network survivability some requirements must be provided. Requirements mean the functions or features required to improve network capability of delivering essential services in face of attacks or intrusions, and to recover services.

Survivability requirements for self-organizing wireless networks are categorized in two groups: those requirements related to *essential services* and those requirements related to *network characteristics*. The first group is composed of requirements resulted from essential service characteristics. These requirements are summarized as:

- **heterogeneity** - an approach of survivability must consider the heterogeneity of nodes, communication technology and capacity of node's resources.
- **self-configuration** - the network must be able to change dynamically the parameter values of the connections, nodes and protocols, as well as of security mechanisms, such as cryptographic key length, firewall rules and reputation system thresholds;
- **self-adaptation** - capability of the network to adjust itself in response to mobility, environment and the requirements of activities as Quality of Service (QoS) level;
- **efficiency** - survivable approach should support the efficient use of node and network resources, such as node energy and network bandwidth when a malicious fault is suspected or happening;
- **access control** - mechanisms must control the access of nodes in the network, as well as monitor their activities;
- **protection** - security mechanisms need to be managed and combined in order to protect the communication at all layers of the protocol stack;
- **integrity**, **confidentiality**, **authentication** and **non-repudiation** - security principles must be assured for communication;

- **redundancy** - the network must tolerate and mitigate attacks by means of intrusion tolerance techniques, such as double protocols or cryptography operations, simultaneous use of multiple routes and others;

- **robustness** - the network must proceed services during eventual disconnection and along with partial segments of paths.

Table 2.2 summarizes these requirements taking into account the three essential services.

Essential services	Survivable requirements
Connectivity	applicable to heterogeneous networks
	self-configuring (mainly, for naming and service discovery)
	self-adaptation of node transmit powers in response to mobility, activities, environments and attacks
	the efficient use of node's resources
Routing	node access control
	protection of wireless communication at physical, medium and data link layers
	integrity, confidentiality and authenticity principles
	efficiency and robustness
	the use of redundant approaches
Communication	working in different and variable conditions
	the use of asymmetric and unidirectional links
	the use of multiple communication channels
	should work even on eventual disconnections

Table 2.2: Survivability requirements

The second group includes certain survivability requirements resulted from network characteristics such as:

- **decentralization** - survivability must be provided by a decentralized approach in order to avoid central point of attacks;

- **self-organization** - mechanisms for supporting survivability must be self-organized without requiring human intervention in face of changes on network conditions;

- **scalability** - mechanisms to provide survivability must consider the variability on the total number of nodes and the dynamic topology;
- **self-management** - survivable mechanisms must guarantee network functionality and efficiency on all network conditions;
- **self-diagnosis** - the network must monitor itself and find faulty, unavailable, misbehaving or malicious nodes;
- **self-healing** - survivable approaches must prevent connectivity disruptions and recover the network from problems that might have happened. They must also find an alternative way of using resources and reconfiguring nodes, network or protocols for keeping them in normal operation;
- **self-optimization** - mechanisms must optimize the use of network resources, minimizing latency and maintaining the quality of service.

In Table 2.2, each essential service (link-layer connectivity, routing and communication) is associated to three different layers, respectively: link, network and application layers. Separately, they are not sufficient for achieving a complete survivable system due to the characteristics of attacks and intrusions. Hence, a cross-layer approach can make security mechanisms more robust, resistant and survivable. The routing layer, for example, can use energy or bandwidth information provided by the link layer in order to take better choices and to be more adaptive. The routing layer can inform others of detected attacks and then, those layers can start an alert procedure. In summary, the survivability existent on the layers must mutually support themselves.

Based on these previous considerations and on the survivability key properties presented in Section 2.3, we have identified three view planes for survivable systems, as illustrated in Figure 2.3. In the first one (key properties), we have the properties that must be achieved by the system. In the second one (requirements), we highlight the requirements that survivable systems need to reach. Finally, in the third one (protocol layers), we emphasize that all network layers need to be addressed by the system. We argue that a holistic survivable system must consider these three planes.

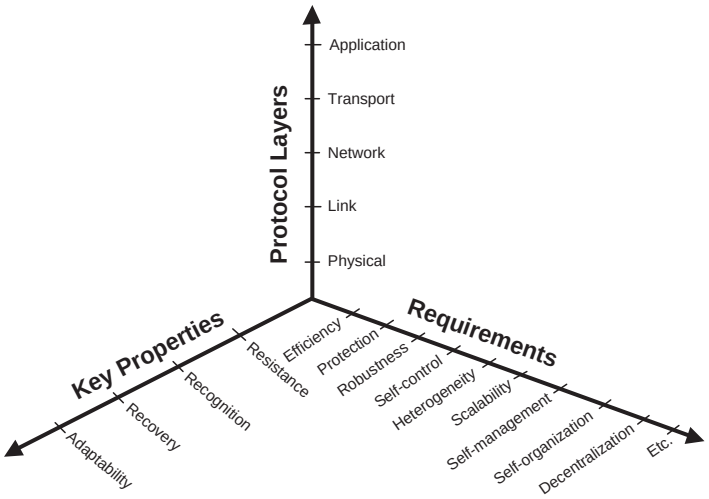


Figure 2.3: Planes of view for survivability

2.5 Conclusions

This chapter provided an overview of the main concepts required to provide survivable network management. First, the main security threats, attacks and intrusions were defined considering their correlation with malicious faults on the dependability domain. Three different classification for attacks and intrusions in self-organized wireless networks were presented. The first one categorizes attacks as passive or active, the second one as internal or external, and the third one follows the layers of the protocol stack. It was emphasized that some of the attacks and intrusions are multi-layers.

The characteristics and the importance of security management were highlighted. Security management intends to control and monitor security services and mechanisms in order to assure security in network services and data. Security services consist of authentication, access control, data confidentiality, data integrity and non-repudiation, whereas security mechanisms are categorized as preventive, reactive or tolerant ones. Hence, tolerant security mechanisms have been employed in the last few years aiming to mitigate the effects of attacks and intrusions that preventive or reactive mechanisms cannot handle.

Survivability is the capability of the network to offer essential services like

link-layer connectivity, routing and end-to-end communication, in face of attacks and intrusions, and recover compromised services after the occurrence of intrusions. Key properties of survivability are provided by the adaptive cooperation of the three types of security mechanisms. Survivability key properties are defined as resistance, recognition, recovery and adaptability. Different survivability requirements were identified, being categorized in those resulted from essential services and those resulted from network characteristics. Finally, it was emphasized that a holistic survivable network needs to consider the integration of three plans: survivability key properties, survivability requirements and the layers of the protocol stack.

Chapter 3

The SAMNAR Architecture

This chapter describes a survivable architecture for self-organizing wireless network called SAMNAR. Architectures include concepts, rules and models, in which rules describe how to use concepts, whereas models show the application of both rules and concepts. SAMNAR discusses security management functions and guides the design of survivable protocols and services. Security management functions consist of controlling and monitoring security services and mechanisms, distributing security-relevant information, reporting security-relevant events, controlling the distribution of cryptographic keying material, and authorizing subscriber access, rights, and privileges.

The main objective of SAMNAR is to present a new approach for security management in order to make viable survivable self-organizing wireless networks. SAMNAR is inspired on the human body immune system in which different types of defenses cooperate adaptively. The architecture intends to offer prevention, reaction and mitigation of damages, as well as recovering of compromised services in a timely manner after the occurrence of intrusions. SAMNAR focuses on increasing the network capability of supporting essential services, link-layer connectivity, routing and end-to-end communication, even in face of attacks and intrusions. Moreover, it proposes a cross-layer approach for network security management.

The chapter is organized in five sections as follows. Section 3.1 presents previous works that have proposed survivable architectures. Section 3.2 gives an

overview of the human body immune system and Section 3.3 describes its correlation with our architecture. Section 3.4 details the SAMNAR architecture. Finally, Section 3.5 concludes the chapter.

3.1 Related Works

In these last few years, research interests in survivability have increased. Initially addressed by military area, the first survivability architectures have been proposed in order to improve both security and dependability of information systems, distributed services and storage systems in the Internet domain [34, 45, 50, 53, 66, 85, 106, 111]. Although the importance of all architectures in the survivability development, we emphasize Willow [111], SITAR [106] and SABER [50] architectures due to their completeness in terms of survivability properties. Further, these architectures exemplify, respectively, the centralized, partially distributed and fully distributed architectures.

The Willow architecture [111] is designed to enhance the survivability of critical information systems. This architecture proposes the merging of different mechanisms aiming to avoid, eliminate and tolerate faults. All of these mechanisms are based on a reconfiguration approach in which nodes of the network can together monitor and respond to faults. Each node and network operations are monitored continuously. However, the analysis of their operation is performed by central nodes, called servers, restricting the efficiency of the architecture.

SITAR [106] is a survivable architecture for distributed services whose goal is to provide the minimal level of services despite the presence of active attacks. This architecture is composed of different components such as proxy servers, monitors, audit control module and adaptive regeneration module. These components are transparent for the clients and servers of the service and each component has a backup in order to guarantee its operation. The architecture controls all requests and responses, and can be centralized or partially distributed.

The SABER architecture [50] integrates also different mechanisms to improve the survivability of Internet services. SABER proposes a multi-layer approach in order to block, evade and react to a variety of attacks in an automated and

coordinated fashion. The SABER architecture is composed of DoS resistant module, IDS and anomaly detection, migration process and automated soft-patching system. All of these components are controlled by an infrastructure of coordination. This infrastructure provides the communication and correlation among the components in a decentralized fashion.

Albeit various survivable architectures exist, few of them were developed for self-organizing wireless networks. Aura and Maki [8], for example, proposed a distributed architecture towards a survivable access control in ad hoc networks. The survivability is achieved creating secure groups of nodes, managing their membership and proving group membership. Operations of security are based on public key certificates, being all the architecture based on cryptography. Groups are formed to grant access rights to nodes. Then, the survivability of this scheme is reached by the existence of multiple groups and by their independence. If a group does not exist anymore, another group can execute access control operations. Despite authors claim to propose an architecture, the solution is a specific survivable scheme for access control, not presenting a set of rules, concepts or models. Moreover, we identified that only resistance and recovery survivability properties are reached by this scheme.

A survivable architecture for wireless sensor networks (WSNs) was proposed by Tipper *et. al* [79]. The architecture aims to provide critical services in spite of physical and network based security attacks, accidents or failures. However, the architecture is limited to identify a set of requirements related to security and survivability, such as energy efficiency, reliability, availability, integrity, confidentiality, and authentication.

3.2 Bio-inspired Principles

The immune system provides defenses for human body to overcome all types of attacks. Human body environment is composed of millions of tiny attackers (bacteria, toxins, pathogens, viruses) and the human body is constantly under the attack of these tiny organisms. Immune system is composed of special cells, proteins, tissues and organs, aiming to defend human body against these microorganisms through a series of steps called the immune response.

The immune system presents three types of immunity as natural, active and passive. The natural immunity includes external barriers of the body, such as the skin and mucous membranes, working as the first line of defense. Usually, the skin **prevents** invasion by microorganisms unless it is damaged, for example, by an injury, insect bite, or burn.

Mucous membranes, such as the linings of the mouth and nose, are coated with secretions that overcome microorganisms. For example, the mucous membranes of the eyes produce tears, which contain an enzyme that tackles bacteria and helps to protect the eyes from infection. The airways filter out particles presented in the air and breathed in. The walls of the passages in the nose and airways are coated with mucus. Microorganisms in the air become stuck to the mucus, which is coughed up or blown out of the nose. Mucus removal is aided by the coordinated beating of tiny hairlike projections (cilia) that line the airways. The cilia sweep the mucus up the airways, away from the lungs. The digestive tract has a series of effective barriers, including stomach acid, pancreatic enzymes, bile, and intestinal secretions. The contractions of the intestine (peristalsis) and the normal shedding of cells lining the intestine help to **remove** harmful microorganisms.

If the first defense is broken, the body **reacts** with the active immunity represented particularly by white blood cells, or leukocytes. Two types of leukocytes exist, phagocytes and lymphocytes. Together, they **seek out** and **destroy** the microorganisms and substances that cause diseases. Phagocytes are cells that chew up invading organisms whereas lymphocytes allow the body to **remember**, **recognize** and **adapt** to previous invaders and help the body destroy them.

Passive immunity is in general provided by another source and it lasts for a short time until the body can make stronger their own defenses. This immunity provide **tolerance** for the body against microorganisms. For example, antibodies in a mother's breast milk provide an infant with temporary immunity to diseases that the mother has been exposed to. This can help to protect the infant against infection during the early years of childhood.

These defenses work cooperatively to maintain the human body alive. The immune system controls and manages the three defense lines stimulating each one when necessary. This perfect combination among defenses keeps the body

protected against all threats, guaranteeing the individual survivability. An example is observed when a person dies and its immune system stops. Quickly, the body is attacked and damaged by microorganisms resulting in its deterioration.

3.3 Correlating Bio-inspired Principles and The Proposed Approach

Inspired by the immune system of the human body, we argue that survivability can be reached by the cooperative and adaptive use of preventive, reactive and tolerant defense lines. Figure 3.1 illustrates our survivable approach. It consists of different levels of obstacles against attacks and intrusions that must work together in an adaptive way.

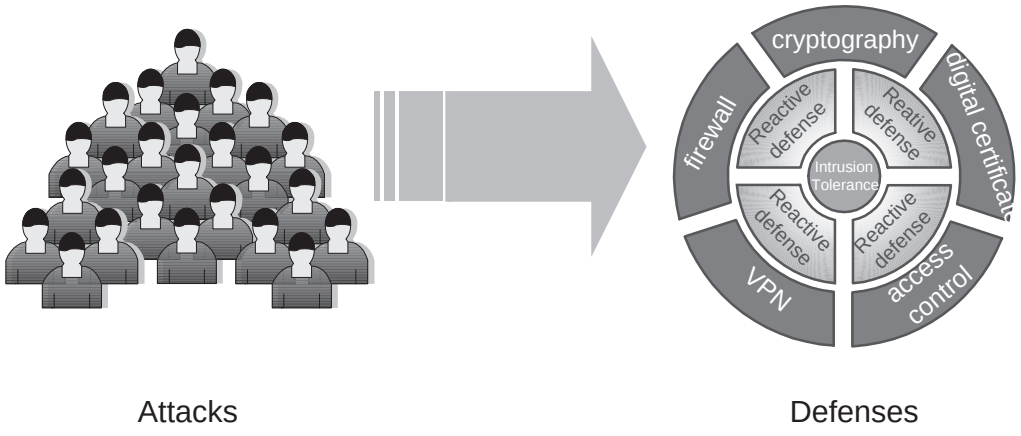


Figure 3.1: All defenses working together

The first obstacle is generated by preventive security mechanisms aiming to avoid any type of attack. Examples of these mechanisms are firewalls and cryptography. They block certain attacks, but naturally will be incapable of preventing others due to their limitations. Cryptography and firewall, for example, are vulnerable to attacks produced by nodes already legally participating in the network.

For some attacks succeeding to intrude into a node or network, reactive defenses will try to detect and react against them. Mechanisms such as intrusion

detection systems or reputation systems try to evaluate the behavior of nodes in the network. However, reactive defenses work efficiently against well-know intrusions, being vulnerable to unknown intrusions. Intrusion detection systems, for example, require extensive evidence gathering and comprehensive analysis in order to detect intrusions based on anomalies or predetermined intrusion patterns.

Therefore, reactive defenses have also limitations. Some intruders can be successful in compromising the network. In order to guarantee the operation of essential services even in the presence of intrusions, intrusion tolerance techniques are applied. These techniques aim to mitigate intrusion effects, and stimulate preventive and reactive defenses to adapt and attempt to block attacks or intrusions. Next section details the SAMNAR architecture that was designed using this approach.

3.4 Survival Architecture

SAMNAR is an architecture for security management in self-organized wireless networks. SAMNAR characteristics result from the requirements and properties of survivability. Each node is responsible for reaching its survivability by the management of security mechanisms and following our approach of survivability presented in Section 3.3. Each node in the network is also self-managed meaning that no central entity in the network provides management functionalities.

The SAMNAR architecture is illustrated in Figure 3.2. It is composed of three major modules named **survival**, **communication** and **collect**. The main module is the survival one employing our survivability approach, whereas communication and collect modules provide support for the first one. These modules are respectively detailed in Subsections 3.4.1, 3.4.2 and 3.4.3.

3.4.1 The survival module

The **survival module** holds five independent components, being four ones related to the survivability properties, resistance, recovery, recognition and adaptability, and the control component. The properties represent respectively the

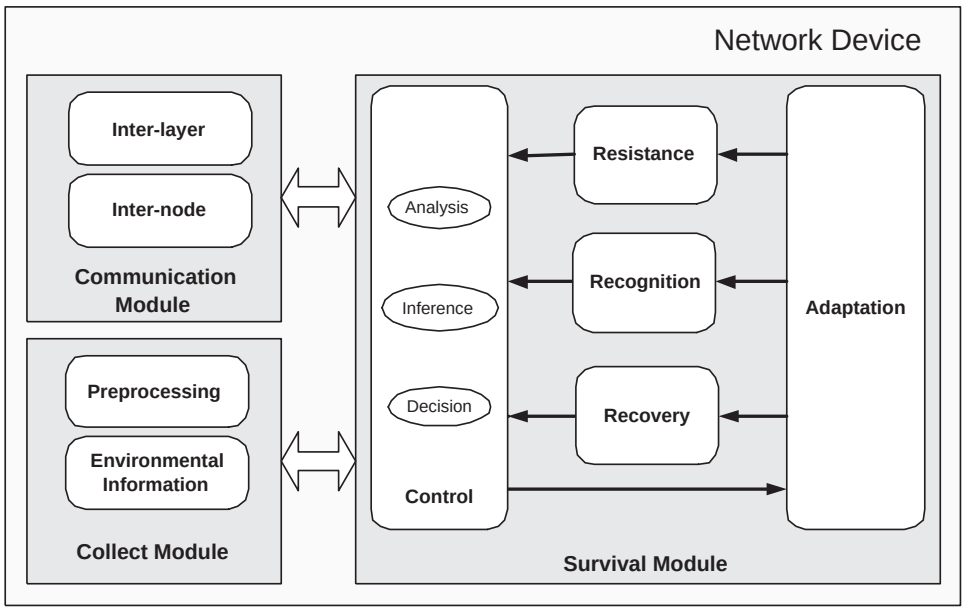


Figure 3.2: SAMNAR architecture

network capability of repelling attacks; detecting attacks and evaluating the extent of damage; restoring disrupted information or functionalities; and quickly incorporating lessons learned from failures and adapting to emerging threats.

The *resistance component* consists of preventive mechanisms such as firewall, access control, authentication and cryptography. This component works in a self-protection and self-adjusting fashion where preventive mechanisms and their configuration will be changed depending on the network or environmental conditions. The rule of a distributed firewall, for instance, can be more rigorous in certain environments, while simpler rules can be applied in more secure environments. Another example is the cryptographic key size that can be larger depending on the environment.

The *recognition component* is composed of reactive mechanisms to identify malicious behaviors, such as IDSs, reputation systems, anti-malwares and anti-spammers. Recognition mechanisms can also have the capability of reacting and stopping intrusions. All the mechanisms will be reconfigured if necessary by the adaptation component. New configurations as IDS rules will depend on the network and environmental conditions. This component provides to the control com-

ponent information about detections, trustworthiness of neighbor devices among others.

The *recovery component* consists of mechanisms to enhance the attack tolerance of network essential services. Mechanisms to restore disrupted information or functionality, such as replication or redundancy, have been employed as tolerant mechanisms. The application of two cryptography algorithms successively and the replication of message pieces are examples of redundancy. Sending redundant message pieces by different routes increases the probability of the message to be received by the destination node and the possibility of message recovery in case of piece losses. However, redundant strategies should consider resource limitations, as well as service and application requirements.

The *adaptation component* complements the previous ones. It is responsible for adapting preventive, reactive and tolerant mechanisms, as well as local or network configurations. It can replace a given protocol or a defense mechanism, such as changing a weaker cryptographic algorithm for a stronger one, depending on the necessities and requirements on time. Further, the adaptation component can change the key size of a cryptographic algorithm, the rules into an IDS or a firewall, the used route and others in accordance with the network condition or decisions taken by the control component.

The *control component* manages and coordinates all modules in the architecture. It receives information from communication and collect modules as well as from the resistance, recognition and recovery components. The control component correlates and analyzes all information in order to make inferences and take decisions. All decisions are sent to the adaptation component that define and send satisfactory parameter values to other modules or components. Adaptation component learns with taken actions and later, it can take the same action if the node or network present a similar condition.

3.4.2 The communication module

The **communication module** is responsible by cross-layer and inter-node communications. The *inter-layer component* offers the exchange of information inter-layers. It supplies information from different network layers to control component

so that it takes decisions based on all network layers and achieves the survivability for all of them.

The *inter-node component* provides communication, exchange and synchronization of information among the nodes aiming to guarantee the survivability of the whole network. Example of this information is the node configuration or network intrusion detections. Techniques for inter-node communication must consider the limitations and heterogeneity of the network resource capacities, such as memory, bandwidth and processing, and must be efficient in using these resources.

3.4.3 The collect module

The **collect module** holds mechanisms to gather all data required by the survival module. The collect module is composed of the *preprocessing component* and the *environmental information component*. The first one is exploited when gathered data need to be treated before sending to the survival module. Normalizations, previous calculations and others are examples of preprocessing used for facilitating analyses and inferences of the survival module. The second component stores information gathered periodically about the network conditions, sending it to the survival module when required.

3.5 Conclusions

This chapter presented SAMNAR, an architecture for providing survivability in self-organizing wireless networks. SAMNAR is inspired by the human body immune system in which different types of defense are aggregated and coordinated to guarantee the survivability of an individual. SAMNAR combines preventive, reactive and tolerant defense lines in an adaptive way. The goal is that preventive defenses will be the first obstacle against attacks, reactive defenses will be the second obstacle trying to detect and react against intrusions, and tolerant defenses will be the third obstacle working in a proactive way in order to mitigate intrusions or attacks effects. All these defenses are adapted to the network

situation or condition making the protection stronger or weaker depending on the goals and priorities of the network in a given moment.

The SAMNAR architecture is composed of three main modules: survival, communication and collect. Survival module employs the three defense types. This module consists of resistance, recognition, recover, adaptation and control components. The first three components own security mechanisms related to the three defense lines, such as cryptography algorithms, intrusion detection systems and recovery techniques. These components are managed by the control component, which is responsible for making inferences, analyzing and taking decisions based on the network conditions or on the feedbacks from security mechanisms.

In our architecture, each node is responsible for its survivability and for the network survivability at all. Hence, SAMNAR presents a communication module responsible for all techniques related to inter-layer communication or inter-node communication. Inter-layer or cross-layer component supports the exchange and the use of information provided by different layers of the protocol stack. The inter-node component defines the mechanism and configuration to be used in the communication among nodes. Finally, SAMNAR defines a collect module in which mechanisms will be defined for collecting information from the network or environment necessary for taking decisions and inferences by the control component.

Chapter 4

Routing Survivability in Mobile Ad Hoc and Mesh Networks

Routing is a fundamental network functionality for self-organizing wireless networks. Its main function is to support the correct delivery of user data from one node to another. Routing service is composed of four phases: route discovery, route maintenance, path selection and traffic allocation. This chapter demonstrates the application of the SAMNAR architecture proposing a survival path selection scheme for two specific types of self-organizing wireless networks: mobile ad hoc networks (MANETs) and wireless mesh networks (WMNs).

This case study handles the problem of selecting the most survivable routes meaning those ones able to maintain routing even in the presence of attacks, intrusions or selfish actions. The proposed scheme combines different criteria representing network conditions and the three defense lines: preventive, reactive and tolerant. We evaluate the survival path selection scheme on different scenarios using urban mesh network mobility and propagation models, and the random waypoint model with the two-ray ground propagation model. Simulation results demonstrate survivability improvements with low impact on network performance.

This chapter is organized in five sections as follows. Section 4.1 presents previous works correlated with the path selection problem. Section 4.2 describes the network and attack models considered in this case study. Section 4.3 details the proposed path selection scheme following its three phases: data collection, fuzzy

inference and path selection. Section 4.4 presents the evaluation methodology, simulation environment and results. Finally, Section 4.5 concludes the chapter.

4.1 Related Work

Researchers have proposed different path selection schemes for self-organizing wireless networks, particularly for mobile ad hoc and mesh networks. Path selection consists in deciding to use the best route for data packet transfer in order to, for example, achieve the best network performance, improve reliability or minimize latency. This section gives an overview of these schemes and we group them in two classes, single criterion based and multi-criteria based. Schemes from the first group utilize only one criterion to choose best routes, whereas schemes from the second group combine many criteria to decide and select the best route. Examples of criterion are packet loss rate in a path, route lifetime and path length – the number of hops between a source and a destination.

The majority of existing path selection schemes utilizes a single criterion to choose best routes [35, 42, 44, 49, 56, 74, 116]. In general, the criterion represents the route condition, such as throughput, route lifetime, packet loss or latency. The split multipath routing protocol (SMR) [56], for example, picks out as primary route the shortest routing path in terms of the number of hops between a source and a destination. Then, it computes the maximum disjoint path as a secondary route. The disjoint pathset selection protocol (DPSP) [74] chooses in linear time a set of highly reliable paths, being determined by path length. Hua and Zaas [42] have presented three path selection algorithms based on residual path lifetime, and Han *et. al* [35] have investigated path duration in order to maximize the expected duration of the chosen paths. Jiang *et. al* [44] have developed mechanisms to predict the link availability, and based on those predictions paths are selected. Yuan *et. al* [116] have proposed an opportunistic and credit-based routing in which high-throughput links are selected to greedy forward data in a multipath way and mitigate DoS attacks.

The use of a single selection criterion ignores many self-organizing wireless network characteristics. MANETs, for example, present dynamic topology determined by different factors, such as node mobility, signal strength, node battery

capacity, among others. These factors are correlated, being unsatisfactory to utilize just one or two criteria for choosing a set of paths. Moreover, the correlation among criteria is important to make choices more accurate. The Genetic Fuzzy Multi-path Routing Protocol (GFMRP) [59] is the most relevant protocol focusing on these issues. There, Liu *et. al* [59] apply fuzzy set theory and evolutionary computing to correlate criteria and select a set of paths. Fuzzy logic is applied to minimize correlation complexity. However, GFMRP's goal is to maximize network lifetime and reliability.

Despite of the improvements achieved separately by each single criterion or multi-criteria schemes, just a few of them consider security characteristics to select paths. Berman *et. al* [13], for example, proposed intelligent routing schemes to reduce message interception probability. This scheme uses directional antennas and controls the physical distance among the hops. Awerbuch *et. al* [11] proposed a new algorithm for adaptively selecting routing paths in a network with dynamic adversarial edge failures. Nevertheless, the path selection is made comparing accumulated packet loss on all paths.

Yi *et. al* proposed SAR (security-aware ad hoc routing) [115]. It classifies nodes based on their trust level. In the route discovery process, the source node can estimate the minimum security level required by the node in order to participate in the routing path. However, SAR is not a multipath routing protocol and does not correlate security criteria with others related to network characteristics. Nie *et. al* [71] proposed the fuzzy logic based security-level (FLSL) routing protocol. It selects the highest security-level routes, calculated by fuzzy logic through the correlation among path length and two security characteristics, cryptographic key length and frequency of key exchanges. However, the initial FLSL proposal defines a single path protocol and it does not address survivability issues.

4.2 Network and Attack Models

Network model: We focus on multi-hop wireless ad hoc networks consisting of n mobile or stationary nodes. The network is self-organized and nodes are randomly distributed in an area A with density d equals to n/A. Mobile nodes move following a mobility model. Neither routing support infrastructure exists

nor a central control entity to manage network resources. Hence, nodes have similar functionality, and cooperate with each other for network maintenance and routing.

Nodes need a multi-hop communication. No node has a complete knowledge of the network topology, requiring routing to communicate with nodes that are out of its radio range. Each node possesses a single channel with a common transmission range r and bandwidth w. All nodes can be data sources communicating via unicast transmissions. Nodes in the transmission range of a node x are called neighbors of x and the communication with them is single-hop.

We assume that a number of paths, NP, is available for the transmission of data packets from a source node to a destination node. Any multipath routing protocol can be employed. Multipath routing protocols are preferred in relation to single path routing protocols due to the redundancy offered, minimizing recovery time in case of failures, and allowing the parallel use of many routes for data transfer in order to increase throughput and reduce latency. All paths must be mutually disjoint, meaning that they have no nodes in common. Hence, they are independent in the sense that attackers in one path cannot cause the failure of another. However, as nodes own a single channel for transmission, it should be noted that node disjointness cannot guarantee the total independence of paths due to interference produced by other nodes transmitting at the radio range [99].

We consider the existence of a public key infrastructure (PKI) binding cryptographic public keys with their respective node identities. Each node possesses a security credential based on its public key certificate. Node credentials have an expiration time and should be renewed periodically. Security credentials are used for authenticating nodes and controlling their access into the network as in the credential system proposed by Luo *et. al* [61]. Messages must also be authenticated and those that cannot be authenticated are discarded. Nodes use public keys to encrypt and, hence, protect route discovery and data forward phases. Moreover, nodes use a reputation system in order to continuously evaluate the reputation of its vicinity. Example of reputation system is that one [83] proposed by Refaei *et. al.*

Attack model: This case study focuses on attacks that can compromise routing service, not addressing attacks that can degrade or disrupt MAC, or physical

layers. We concentrate our analysis on authorized nodes acting maliciously or selfishly, alone or in collusion since unauthorized nodes cannot join the network due to access control and authentication mechanisms; and also since some types of attacks can be prevented by traditional encryption, authentication and integrity mechanisms (such as eavesdropping and packet modification). Attacks yielded by adversarial nodes such as blackhole, grayhole, wormhole and sinkhole cannot be prevented only by authentication mechanisms or cryptographic techniques.

4.3 Path Selection Scheme

Based on the SAMNAR architecture presented in Chapter 3, we created a path selection scheme for MANETs and WMNs. This scheme utilizes both *conventional criteria* and *security criteria* for choosing more survivable paths. Conventional criteria allow resource and performance management, and we have chosen remaining energy (energy rate) and path length as network information (*environmental information*). However, other criteria could be added or replace those used in this case study, such as path throughput, link stability and others.

In accordance with the proposed survivability approach, security criteria comprise features yielded by the three defense lines. This case study considers **certificate expiration time** and **cryptographic key length**, as criteria from preventive defenses; **node reputation** as reactive defense criterion; and **path degree** as criterion of tolerance due to the possibility of providing path redundancy. Other security criteria could also be added or replace those employed, such as the type of used cryptography and the percentage of false positive or false negative.

As correlating several criteria and selecting an optimal path set is a NP-complete problem [74], heuristics, optimization methods and probability distributions have been used to make best decisions. Some of them are based on thresholds, whose values are difficult to determine due to the high dynamism and uncertain states of MANETs and WMNs. Moreover, resource constraints limit the use of computationally-intensive methods or complex solutions.

The proposed selection scheme employs *fuzzy logic* (FL) [117] since it has proved to be a powerful tool for making decisions [107, 117]. FL allows the defi-

nition of intermediate values between 0 (false) and 1 (true), and it accepts rules expressed in natural language, and models problems on an easier way. Further, FL manages imprecise and noisy data [107, 117].

Our path selection scheme is independent of a specific routing protocol. However, the protocol should be able to find node-disjoint multipath routes from source to destination. Node-disjoint paths are preferred than non-disjoint or link-disjoint ones due to the nonexistence of nodes or links shared among the routes.

The design of the path selection involves three phases: *data collection*, *fuzzy inference* and *adaptive path selection*. The data collection phase obtains criterion values by a polling process using special packets called check packets (CPACKs). This process consists in sending CPACKs periodically for all known paths of a given node. CPACKs have two functions: to verify the path status and to collect criterion values. This phase is described in Section 4.3.1.

The fuzzy inference phase calculates the survivability level of each path. The path survivability level (PSL) is achieved by the FL stages: input fuzzification, inference and defuzzification, detailed in Section 4.3.2. Based on PSL, the paths are ranked, being the most survival routes chosen in the path selection phase. However, due to new data collections the PSL value of a path can change with updates in criterion values. Thus, the set of selected routes can also change adaptively. Figure 4.1 illustrates the integration of these phases.

4.3.1 Data collection

Periodic data collections are executed by means of CPACKs. For each CPACK, it is assumed to be created a cryptographic message digest as that proposed in [49] aiming to prevent forgeries. After generating the message digest, nodes send CPACKs for all previously discovered paths. The route discovery process follows the specification of the routing protocol.

CPACKs are forwarded hop by hop to the destination and, in every intermediate node, criterion values are gathered and stored on specific fields. Arriving at the destination node, it changes the value of the *way* field and sends the packet back. The packet can use any route to return to the source.

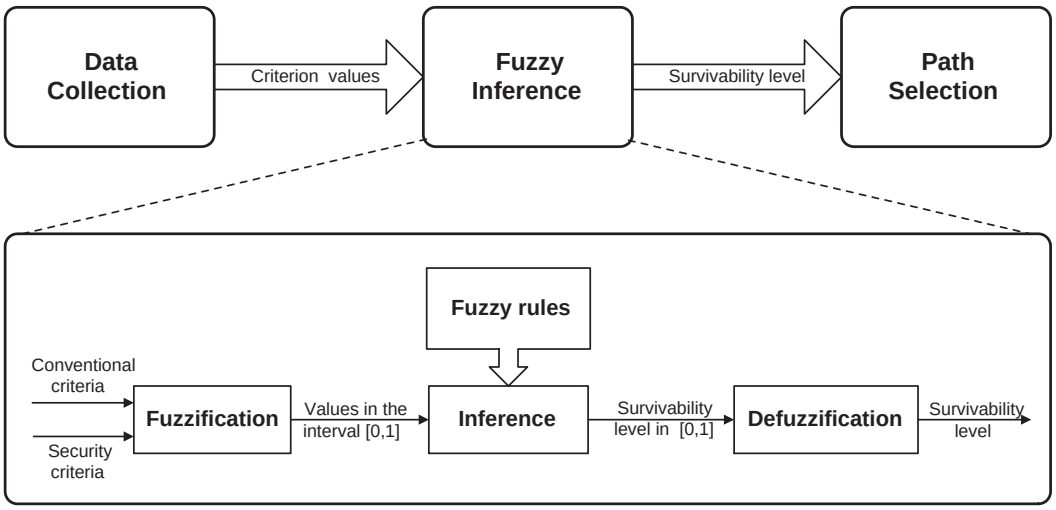


Figure 4.1: Phases of the path selection scheme

CPACK presents eight main fields: *destination IP address*, *source IP address*, *way*, *energy rate*, *reputation*, *validation*, *path degree* and *hop*. Source and destination addresses assist CPACK routing, and the "way" field indicates if CPACK is going to or coming back from the destination node. If "way" value is 0, it is going to destination and data is collected. If "way" value is 1, the packet is just forwarded, without gathering data. "Energy rate", "reputation", "validation" and "path degree" fields store, respectively, the smallest value of remaining energy, node reputation, expiration time and node degrees found in the path. The "hop" field accumulates the number of intermediate nodes in the path.

Figure 4.2 illustrates the data collection phase, where node A is a source and has two routes, R1 and R2, to achieve the destination node B. These routes have been found by the discovery phase of the routing protocol. With a time interval equal to x seconds between one data collection and other, one CPACK is sent for each known path. Data is collected when CPACK is towards the destination node, i.e., when the "way" field is 0. After data collection, the source node calculates the survivability level of each path, as will be described in Section 4.3.2.

CPACKs are lost when they cannot find a route to the destination node or to come back to the source. Thus, the survivability level of this path remains with initial value. As it has the smallest PSL value among other paths, it is not

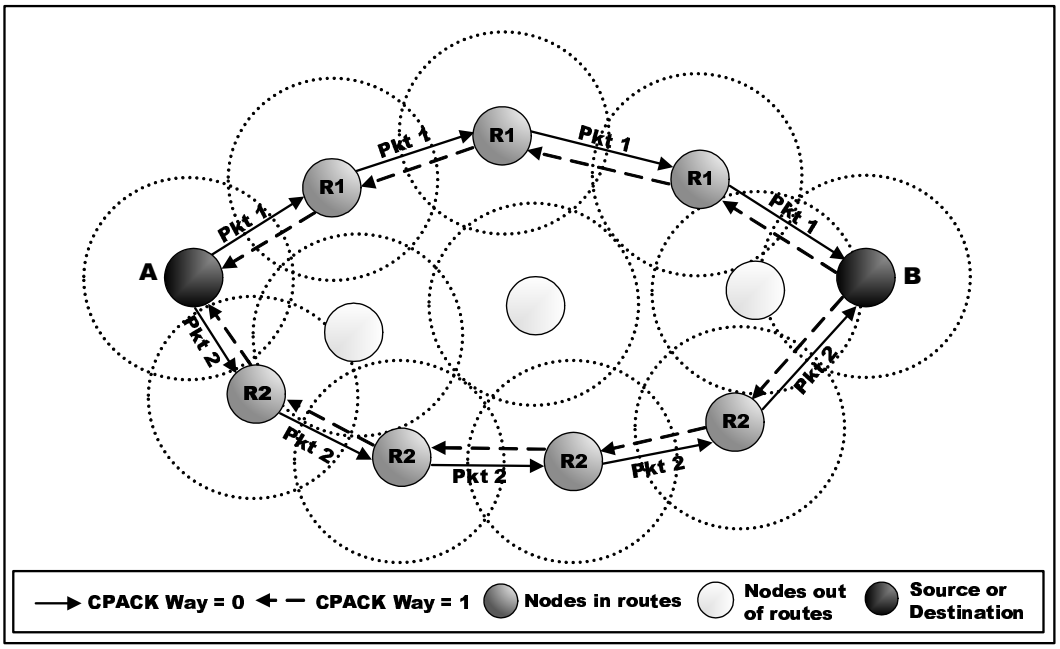


Figure 4.2: Data collection phase

selected. The path survivability level is updated with the next data collection.

4.3.2 Design of the fuzzy inference system

Fuzzy inference is the process of mapping inputs to outputs by fuzzy logic. The mapping is performed by rules that determine the outputs associated to inputs. Fuzzy rules follow the form **if-then** and their inputs and outputs are values in fuzzy sets. These values are in the interval [0.0,1.0], with 0.0 representing absolute falseness and 1.0 representing absolute truth. The set of rules compounds the knowledge base of the system, generating outputs used to make decisions. Path survivability levels are estimated by the fuzzy inference process following the fuzzification, inference and defuzzification steps, as described in this section.

Fuzzification of inputs

Fuzzy rules manipulate values between 0.0 and 1.0, although the inputs of the fuzzy inference system (FIS) are not in this interval. Conventional and security criteria used as input values are represented by linguistic terms, such as “strong”,

"weak", "large", "small". Each criterion has a set of linguistic values, which are mapped to fuzzy intervals by membership functions. This process is called *fuzzification*. We have employed the trapezoidal function as the membership function, since it has been extensively used in real-time applications due to their simple formulas and computational efficiency [59, 107].

Different conditions represented by conventional criteria affect the survivability level. Conventional criteria, as remaining energy, for example, influence the survivability in which nodes with higher energy rate can participate in the path for a longer time period, enhancing the path stability. Stable paths are preferred due to the decrease in the number of route discoveries caused by path breaks. Route discoveries enable the participation of new malicious nodes in the routes, minimizing the probability of survivability. Moreover, paths with high remaining energy can better tolerate overload attacks. Hence, high remaining energy improves the survivability level.

Remaining energy can be represented by the following linguistic terms: *low*, *medium* and *high*, where the membership function of energy rate (E) is shown in Figure 4.3. Fuzzy inference considers the remaining energy of each path (E^i), estimated by the minimum value among the energy rates of all n nodes in the path i. Thus:

$$E^i = min(E^i_1, E^i_2, \ldots, E^i_n) \tag{4.1}$$

Path length (L) represents the number of intermediate hops between the source node and the destination node. Higher path length results in lower performance. For security, higher path length increases the probability of existing malicious nodes in the path. Thus, shorter paths are preferred over longer ones. The path length variable has three fuzzy sets: *short*, *medium* and *long*. Based on results found by Perkins *et. al* [89] for the average path length, paths with 1 or 2 intermediate hops are considered short, paths with 2, 3, 4, 5 and 6 are considered medium, and paths with more than 6 intermediate hops are considered long. Figure 4.4 presents the membership function for path length.

The scheme also employs security criteria generated by preventive, reactive and tolerant defense lines. Certificate expiration time (T), for example, presents

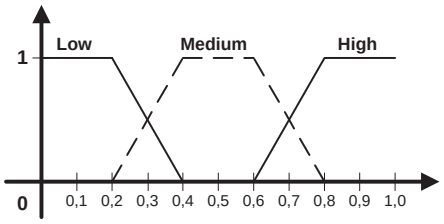


Figure 4.3: Energy (E) function

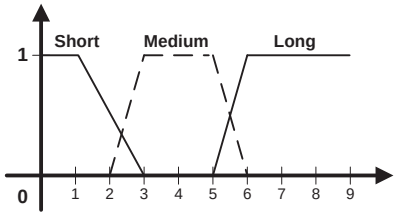


Figure 4.4: Path length (L) function

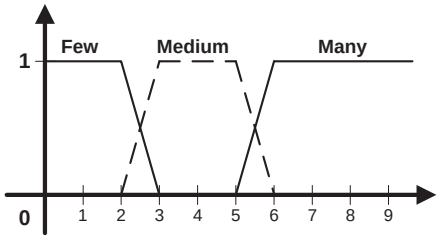


Figure 4.5: Path degree (D) function

two fuzzy sets, *imminent* and *far*. If the certificate expires within 10 seconds (s) or less, it is imminent, and being far when it expires within 60s or more. These values were chosen based on results found by Han *et. al* [36], where it was presented that the majority of path durations is between 10 and 20 seconds. Expiration times smaller than path duration enhance the likelihood of the certificate to be compromised due to updates when the path is still alive. Thus, more imminent certificate expiration time minimizes the survivability level, and this criterion is resulted from the preventive defense line.

For cryptographic key length (K), two fuzzy sets are defined, *short* and *long*, as presented by Nie *et. al* [71]. If the cryptographic key is 40 bits or less, it is considered short, and it is long with 128 bits or more. Longer key lengths make cryptographic mechanisms more resistant to attacks. Thus, the survivability level is directly proportional to the key length.

The reputation (R) of a path i is the lowest node reputation value in the path. The reputation system in the network provides values between 0.0 and 1.0 indicating node behavior. The path reputation linguistic variable has two fuzzy sets, *good* and *bad*. Paths with higher good reputation values are preferred. Good

reputations are those with values equal or higher than 0.8. The reputation of the path i with n nodes is calculated as:

$$R^i = min(R^i_1, R^i_2, \ldots, R^i_n) \tag{4.2}$$

Path degree (D) represents the tolerant defense line, being defined by the minimum node degree of all n nodes participating in the path i (Equation 4.3). The node degree is defined as the number of its direct neighbors. Higher neighbor number augments the probability of finding redundant or alternative paths, and thus can improve survivability. The path degree linguistic variable has three fuzzy sets: *few*, *normal* and *many*. Figure 4.5 presents the membership function for this linguistic variable.

$$D^i = min(D^i_1, D^i_2, \ldots, D^i_n) \tag{4.3}$$

Fuzzy inference process and deffuzification

Fuzzy inferences are based on input values and fuzzy rules. An overview of the fuzzy inference process is presented in Figure 4.1. Input fuzzy sets represented by membership functions are combined by inference mechanism in order to generate values in an output fuzzy set. The inference mechanism follows a function, and it is guided by rules. In this case study, we have used the Larsen's max-product inference function [117] in which algebraic product operations correlate inputs. Inputs are represented by membership functions as energy rate, path length, certificate expiration time, cryptographic key length, reputation and path degree.

Fuzzy logic incorporates a simple rule-based approach. Rules are described in linguistic terms following the form IF X AND Y THEN Z. X and Y are input fuzzy sets, and Z is the output fuzzy set meaning the set of values for the path survivability level (PSL). The linguistic variable of PSL has three fuzzy sets: *low*, *medium* and *high*. The set of rules used in this specific case study is detailed in Appendix B.

For each path, a survivability level is calculated based on the fuzzy logic inference process. Assuming the independence among the six criteria presented,

their relationship can be generalized as follows:

$$PSL \propto E \bullet K \bullet R \bullet D \bullet \frac{1}{L} \bullet \frac{1}{T} \tag{4.4}$$

Only for exemplifying the importance of security criteria and their impact in order to make decision on PSL, Figure 4.6 correlates K and L criteria. Note that with L up to 5, L is not an important factor to improve the PSL, being K more than 50 the main factor. However, for L values higher than 5, both L and K improve the PSL value, although it only achieves 0.45. As defined in Equation 4.4, PSL is reduced by high values of L.

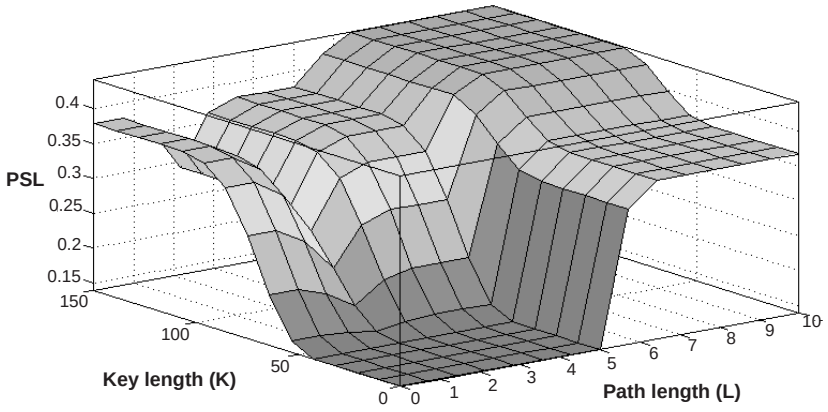


Figure 4.6: Correlating selection criteria and PSL

The final process of the fuzzy inference system is mapping fuzzy values over an output universe of discourse into the crisp control value (non-fuzzy). Fuzzy values are in the interval between 0 and 1. This process, called defuzzification, is important for many practical applications. However, in our case we use as output values without defuzzification.

4.3.3 Path selection

The survivability level found for each path is ranked, being chosen the path with the highest PSL. The chosen path is used until it is broken or until a new data collection phase occurs. If the path is broken before that, the next path

with higher PSL is used. If a new data collection phase finishes and path ranking changes, the source and destination nodes will adapt to use the new most survival path. This process allows routing self-adaptation.

4.4 Evaluation

We analyze the path selection scheme using Network Simulator (NS-2) version 2.30. Simulations were performed considering two networks: an ad hoc network with two-way random mobility, called **CASE 1**, and an urban mesh network employing a realistic node mobility and signal propagation, called **CASE 2**. For the sake of evaluation, the path selection scheme was instantiated on the routing protocol AOMDV (On-demand Multipath Distance Vector Routing in Ad Hoc Networks) [62]. This protocol was modified to provide security criteria values and to execute functionalities defined as *data collection*, *fuzzy inference* and *path selection*. Multipath node-disjoint routes were used in order to provide redundancy.

Analyses evaluate two main aspects: the survivability improvement achieved by the path selection scheme and its impact on network performance. For this, we compare results produced by the AOMDV modification, called AOMDV-SL, with those yielded by AODV and AOMDV in the presence of **blackhole (BH)** or **grayhole (GH)**, and combinations of both attacks with the **sinkhole (Sink)** attack. AOMDV-SL provides preventive, reactive and tolerant security information regardless of a specific secure protocol, reputation scheme, cryptographic mechanism or key distribution infrastructure. AOMDV has no security mechanisms against the entire set of strong colluding attacks; however we have considered them due to their performance.

We have used the following metrics for evaluating the survivability improvement achieved by our scheme and its impact on the network performance. For all these metrics, we have calculated a confidence interval of 95%.

- **Misbehavior drop ratio (MDR)** - measures the proportion of data packets dropped due to attacks over the total of data packets dropped. For the

sake of analyses, we have implemented mechanisms on NS-2 to log data packets dropped due to attacks.

- **Packet delivery ratio (PDR)** - calculates the percentage of data packets delivered at the destination over the total amount of data packets sent by the source.

- **End-to-end delay of data packets (E2E delay)** - consists of propagation delays, queuing delays at interfaces, retransmissions delays at the MAC layer, as well as buffering delays during route discovery step.

4.4.1 CASE 1: Wireless ad hoc networks

Simulation settings

The IEEE 802.11 protocol operating with the distributed coordination function (DCF) is used as medium access control (MAC) protocol. The radio model presents similar characteristics to a commercial Lucent's WaveLAN radio interface with a nominal bit-rate of 2 Megabit per second (Mb/s) for the shared-media radio and nominal radio ranges of 100 and 250 meters. The radio range of 100 meters was used to force a higher number of nodes in multi-hop paths.

The mobility model applied is the random way-point model, in which node speeds are randomly chosen between zero meters per second (m/s) and a maximal speed (M) of 1 m/s or 15 m/s. Pause time was fixed to 100 s minimizing the impact of network dynamism in the results. The data traffic used in the simulations is CBR (Constant Bit Ratio) with 20 source nodes defined randomly. Each source generates data packets of 512 bytes and transmits them with a rate of 4 packets per second (pkt/s). Data traffic sessions happen at a random time in the simulation. The network interface queue size of the nodes was set to 64 packets for routing and data packets.

The network area dimensions were fixed for all simulations in 1000 by 300 square meters, and the total number of nodes n placed randomly in this area is of 50 nodes. In the beginning of each simulation, malicious nodes are chosen randomly from the total number of nodes. The percentage of number of malicious

nodes varies from 0% up to 50%. AODV and AOMDV use configuration parameter values defined in the RFC 3561 [76], since these values were considered as the best ones for the performance of both protocols. Examples of configuration parameters are route lifetime, time to live (TTL) of Internet Protocol (IP) header packets and the interval between hello messages. The total simulation time was 500 seconds and each plotted point is an average of 35 simulations.

Simulation results

First, we analyze the survivability improvements achieved by our scheme. Figure 4.7 compares the MDR resulted from AODV, AOMDV and AOMDV-SL protocols under different attacks. Also in Figure 4.7 we examine the percentage of data packets dropped due to blackhole (BH), sinkhole combined with blackhole (Sink-BH) and sinkhole combined with grayhole (Sink-GH) attacks for all protocols. We observe that BH attacks result always in the highest ratio of packets dropped due to attacks (MDR) independent of the protocol. Considering this aspect, we verify that our scheme has improved the data packet survivability, that is, it has reduced the MDR value in the presence of the three attacks. AOMDV-SL decreases the MDR in relation to other protocols by 30% up to 50% of those produced by AODV or AOMDV in the presence of up to 20% of misbehaving nodes in the network. This reduction tends to decrease with higher percentages of misbehaving nodes. Comparing the behavior of AOMDV-SL when the maximal speed M of nodes is 1 m/s and 15 m/s, we verified that the MDR value is practically the same for both situations, independent of the percentage of misbehaving node.

We performed some experiments to examine the impact of the six criteria in the decision scheme and, consequently, in the results. For this, we compare also in Figure 4.7 the results of simulations where nodes hold radio range (r) equals to 250 m with results where nodes hold r equals to 100 m. In scenarios with r equals to 100 m, some criteria will be forced to yield different behaviors, such as higher path lengths and higher node degree.

In Figure 4.7, we verify that the behavior detected in results for r equals to 250 m is also detected in results for r equals to 100 m. However, we observe that

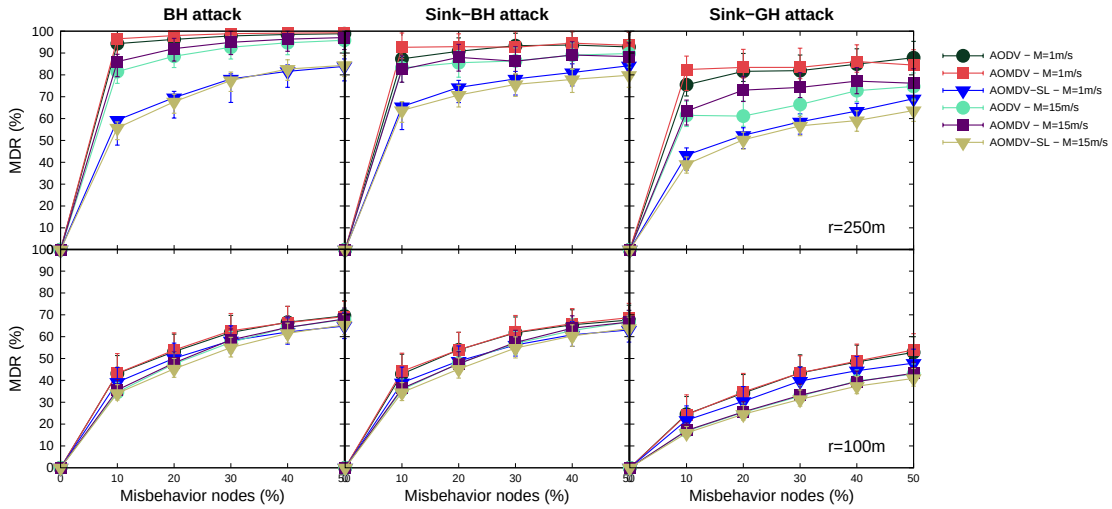


Figure 4.7: MDR in MANETs under different attacks

globally our scheme presents a slighter improvement of data packet survivability for r equals to 100 m than for r equals to 250 m. Further, the ratio of dropped packets due to attacks has been reduced for all protocols independent of attack type. We investigate these aspects by means of Figure 4.8. It compares the criteria values for r equal to 250 m and 100 m in the presence of BH attacks in MANETs. We show values for a percentage of misbehaving nodes equal to 25%. However, based on the results from other percentages of misbehaving nodes and different attacks, we observed that the behavior represented here is independent of the percentage of misbehaving nodes.

In Figure 4.8, we can see that the increase in the value of r results in slight differences for the values of energy (E), reputation (R), cryptography key length used by the nodes (K) and certificate expiration time (T). We emphasize that changes in the energy are small and they cannot be observed in these figures. On the contrary, the increase in r value provides great changes in path length (L) and node degree (D).

With r equals to 250 m (at the right side in Figure 4.8), the network has always higher node degree and short path length, considering both maximal node speed, 1 m/s or 15 m/s. As we have assumed in Section 4.3, short path lengths are better for network survivability since they reduce the probability of misbehaving

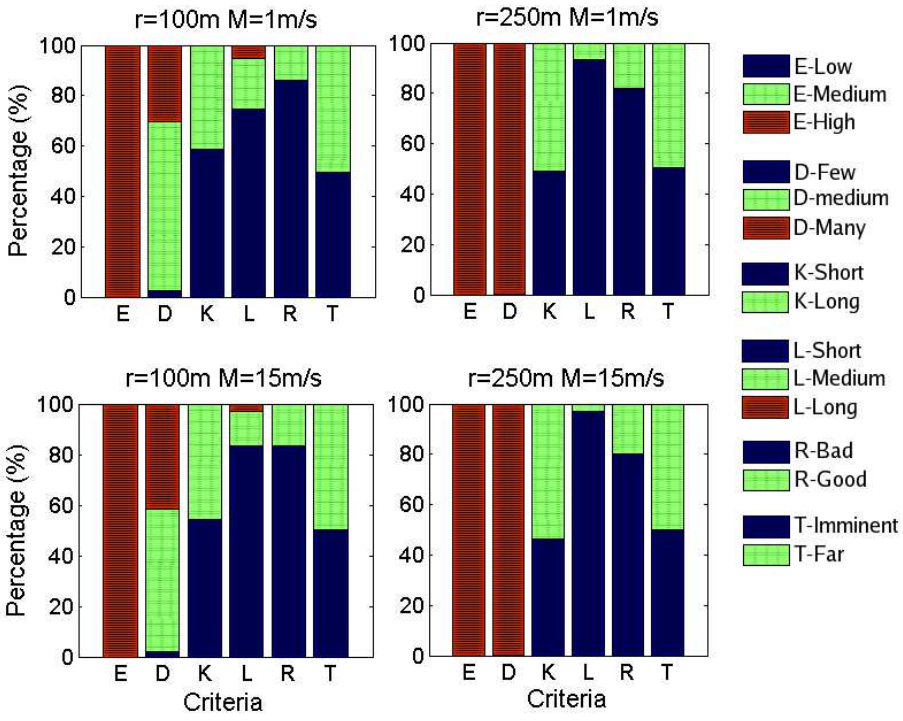


Figure 4.8: Criteria values

nodes in the paths. In the same way, a higher node degree increases the network redundancy due to the possibility of finding more routes from the data source and destination. These considerations are shown in Figure 4.7, where results from simulations with r equal to 250m are better than the those produced by simulations with r equal to 100 m.

Figure 4.9 compares the results of PDR for all evaluated protocols considering, respectively, r equal to 250 m and 100 m. For all protocols, as higher the percentage of attacks, lower is PDR. We observe that AOMDV-SL under BH attacks and r equals to 250 m results in a slight decrease in PDR of about 5% up to 10% in relation to AODV and AOMDV. This decrease tends to be irrelevant when the network is under Sink-BH or Sink-GH attacks, being always into the confidence interval of PDRs provided by other protocols.

As well as for r equal to 250 m, the PDR produced by AOMDV-SL with r equal to 100 m varies in about 5% up to 10% in relation to the PDR of AODV or AOMDV. However, the PDR of AOMDV-SL is higher than those produced by

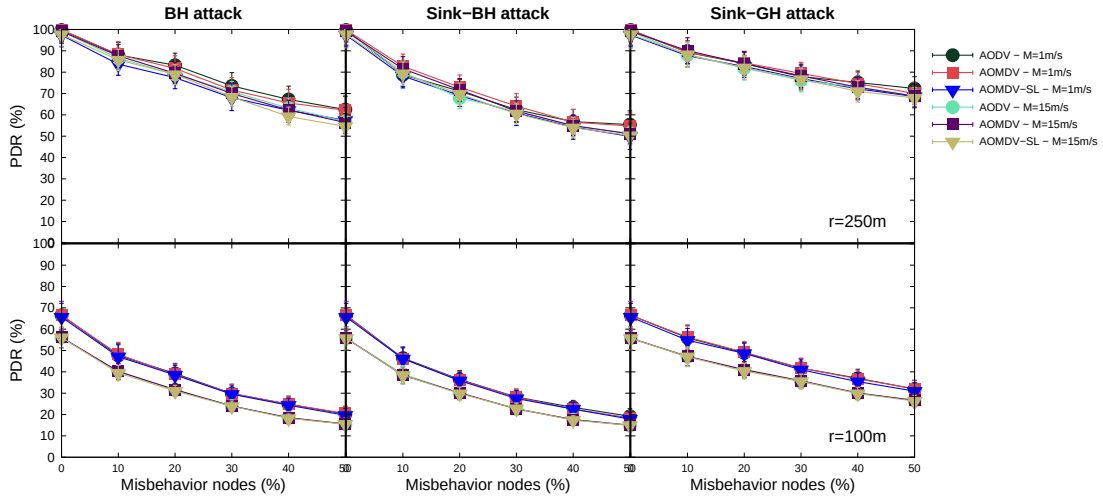


Figure 4.9: PDR in MANETs under different attacks

AODV or AOMDV in lower percentage of misbehaving nodes, and this difference tends to be irrelevant for higher percentages. Moreover, the PDR behavior is similar considering the maximal speed of the nodes 1 m/s or 15 m/s.

In Figure 4.10, we examine the impact of our scheme on the network latency. When r equal to 250 m, AOMDV-SL increases the network latency in about 0.10 s for M equal to 15 m/s, and in about 0.15 s for M equal to 1 m/s. The difference between the latency produced by AOMDV-SL and by other protocols is independent of the attack and is almost constant for all misbehaving node percentages.

For r equals to 100 m, the maximum node speed M presents a great impact in the network latency for all protocols being higher for the cases where M is equal to 15 m/s. When compared the AOMDV-SL latency with the latency of AODV and AOMDV on the same value of M, we verify that their latency is similar. Moreover, we observe that for all protocols the latency tends to decrease with the increase in the percentage of misbehaving nodes. The network latency under Sink-GH attack presented the worst case for all protocols when the percentage of misbehaving nodes is higher than 30%.

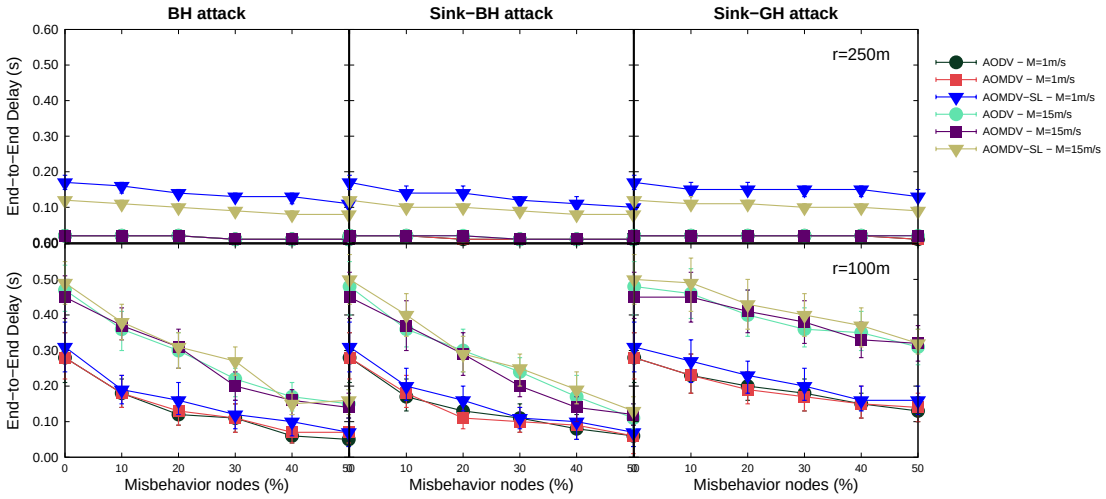


Figure 4.10: Latency in MANETs under different attacks

4.4.2 CASE 2: Wireless mesh networks

Simulation settings

Nodes use the IEEE 802.11 distributed coordination function (DCF) as medium access control (MAC) protocol and IEEE 802.11b as radio model for communication with transmission power of 15 dBm and received card sensitivity of -93 dBm, receiving at 1Mb/s. If the channel gain is lower than -67 dB then it is not possible to decode the transmission with marginal reliability. The used gain margin was 3 dB, requiring above -64 dB of communication channel gain.

We have employed Udel Models in order to have a realistic mobility and signal propagation [92]. Udel Models are composed of signal propagation and mobility patterns in which network environment is considered. The environment includes urban and suburban features, such as buildings, sidewalks, and roads, and within this environment, pedestrian mobile nodes move from office to office through hallways and along sidewalks, while vehicle nodes move along roads and aircraft move anywhere in the three dimensional space above the city. Buildings and other reflective objects in this environment influence the signal propagation, as well as node mobility.

Each simulation was composed of 500 mobile nodes and 29 fixed infrastructure

nodes distributed in an area of 500 by 500 meters square. In these scenarios, we observe our scheme in a high density network. Figure 4.11 illustrates this area representing the core of Chicago city and indicating the positions of the fixed nodes. Mobility and propagation models consider buildings and streets in this area in order to define node movement and its signal propagation. Mobile nodes have pedestrian characteristics, such as the speed of mobility and activities executed throughout the day.

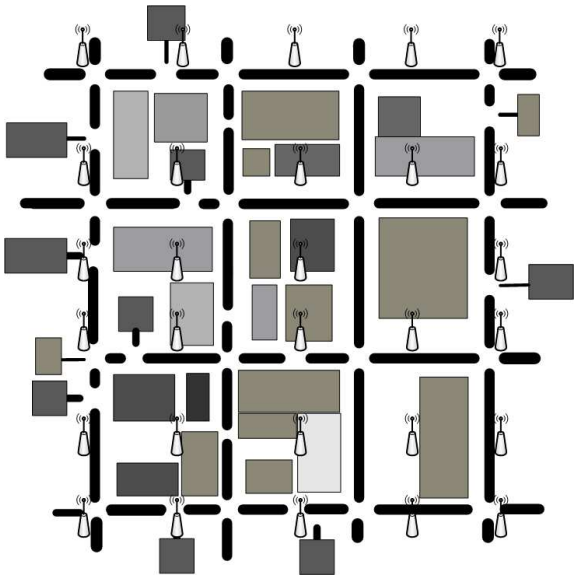


Figure 4.11: Chicago city core: the distribution of fixed nodes

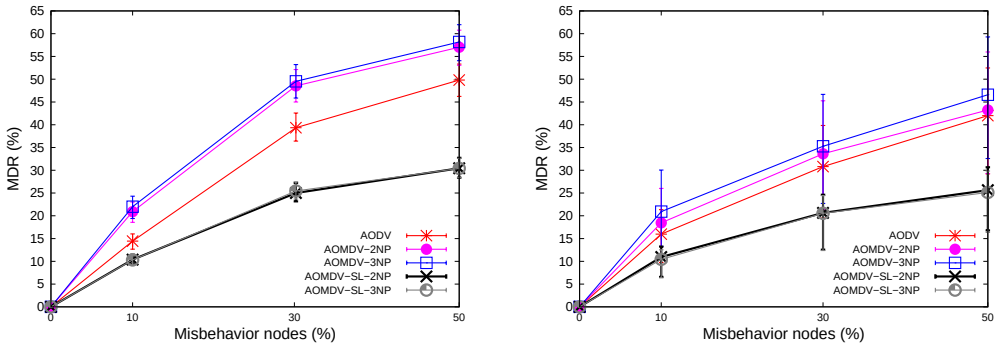
Evaluations investigate two situations. In **Situation 1**, we changed the node mobility and signal propagation for each simulation in order to verify our scheme under different network movement patterns. Further, three different periods of the day were taken into account in order to diversify the sample analyzed since Udel models differentiate pedestrian activities throughout the day. The mobility and propagation scenarios of each simulation are deterministically described by input files. Due to the complexity in generating these files, Udel model web site offers some of them. We used files from version 1.2 and restricted to 15 the number of simulations for the first case because there are only 15 available files. In **Situation 2**, we observed our scheme under 35 independent simulations with

different traffic behavior in each one, but with the same transmission rate (3 pkt/s).

Simulation results

We investigate the behavior of the misbehavior drop ratio (MDR) in Wireless Mesh Networks under Backhole (BH) attacks. These attacks have been chosen for analyses based on the results of the CASE 1. BH attacks produce the highest ratio of packets dropped due to attacks independent of the protocol and for both maximal node speed examined. In Figure 4.12, we consider the maximal number of paths (NP) equals to 2 and 3 for AOMDV and AOMDV-SL.

In Figure 4.12, we observe that our scheme, AOMDV-SL, increases the survivability of data packets since it reduces the ratio of packets dropped due to attacks evaluated by the MDR. This can be observed when compared the MDR yielded by AOMDV-SL with AODV, AOMDV-2NP and AOMDV-3NP. The MDR of AOMDV-SL-2NP and AOMDV-SL-3NP reduces of 5% up to 28% the MDR found by the other protocols. We note also that this reduction is higher in the presence of elevated percentage of misbehaving nodes. We can also see that MDRs resulted from scenarios over different periods of the day (Situation 1) are lower than scenarios where the network was under different traffic behaviors (Situation 2).



(a) Situation 1 (b) Situation 2

Figure 4.12: MDR in WMNs under BH attacks

Figure 4.13 compares for each protocol under 30% of misbehaving nodes the percentage of dropped packets caused by expiration of packet TTL (TTL), the

lack of routes (NRTE), the overload in the queue (IFQ) and misbehaving nodes (MIS). We verify a reduction in the percentage of MIS drops, as well as NRTE drops, resulted from the existence of multiple paths and from the AOMDV failure recovery mechanism. The percentage of TTL drops stays almost the same, whereas the percentage of IFQ drops increased due to data collections of our scheme.

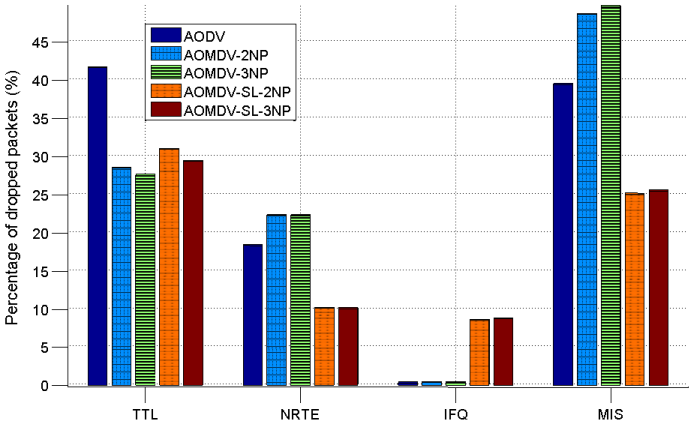
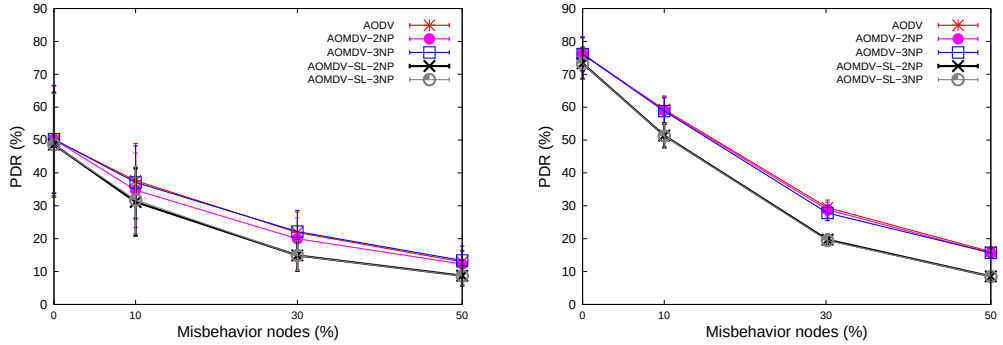


Figure 4.13: Comparing dropped packets

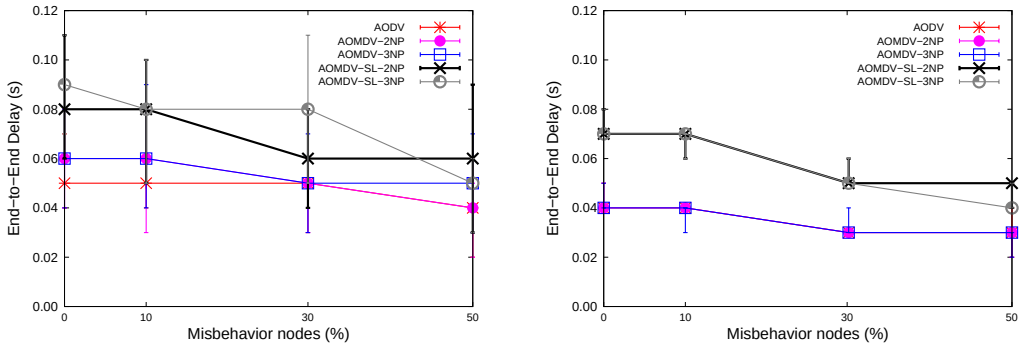
The impact of our path selection scheme on PDR and latency are presented in Figures 4.14 and 4.15, respectively. The PDR of AOMDV-SL, independently of the NP value, decreases in relation to the PDR of AODV or AOMDV. The reduction on PDR using AOMDV-SL tends to increase with the rise in the misbehaving node percentages. However, it is always between 5% and 10%. The PDR for all evaluated protocols is lower in Situation 1, where different periods of the day are considered.

AOMDV-SL increases the network latency in relation to AODV and AOMDV. The rise in latency is of about 0.10 s for Situation 1 and about 0.04 s for Situation 2. This difference tends to be irrelevant for higher percentages of misbehaving nodes in the network.



(a) Situation 1 (b) Situation 2

Figure 4.14: PDR in WMNs under BH attacks



(a) Situation 1 (b) Situation 2

Figure 4.15: Latency in WMNs under BH attacks

4.5 Conclusions

In this chapter the application of SAMNAR is demonstrated the proposal of a path selection scheme for mobile ad hoc and wireless mesh networks. This scheme is protocol-independent and its goal is to increase the survivability of routing service by means of the correlation between security and conventional criteria. Security criteria consist of features provided by preventive, reactive and tolerant defense lines whereas conventional criteria represent network condition. Fuzzy logic is applied to correlate both criterion types, aiming to adaptively select the best survival paths and use them for data transmission.

The survival path selection scheme is composed of three main phases: data collection, fuzzy inference and path selection. Data collection follows a polling

process in which a special kind of packet called CPACK is periodically sent for all routes known by a given node. CPACKs gather data of used criteria from the paths. The fuzzy inference phase employs the fuzzy logic steps – fuzzification, inference and defuzzification – and results in survivability values for each path that a node knows. Routes are ranked by their survivability value in the path selection phase, and the most survivable ones are chosen.

Conventional criteria used in this case study are remaining energy rate in the nodes, and path length represented by the number of intermediate hops between a source and destination nodes. Security criteria consist of certificate expiration time and cryptographic key length, representing a preventive defense; path reputation representing a reactive defense; and path degree representing a tolerant defense. Path reputation and path degree consist, respectively, in the minimum reputation and degree value of each route.

The path selection scheme was instantiated on AOMDV routing protocol and compared with AODV and AOMDV protocols. We evaluated survivability improvements and the performance of the scheme by simulations considering a realistic node mobility and signal propagation for urban mesh networks, and two-way random mobility for mobile ad hoc networks. Three metrics evaluate the effectiveness of the scheme, measuring its ability to delivery packets, the impact of attacks and latency. Simulation results showed a reduction in the percentage of packets dropped due to attacks independently of the network dynamism resulted from node speed. The use of the survival scheme yielded packet delivery ratio similar to those produced by other evaluated protocols. Further, in some scenarios the network latency using the survival scheme is lower than the network latency employing other evaluated protocols.

Chapter 5

Survivable Public Key Infrastructure

Cryptography is used to provide security in different services of self-organizing wireless networks [28, 82, 113]. Particularly, it is used to enforce integrity, confidentiality, authentication and non-repudiation in link-layer connectivity, routing or end-to-end communication. Cryptographic operations, such as encryption or decryption, rely on a keying material and on an algorithm. The keying material includes public/private key pairs, secret keys, initialization parameters and non-secret parameters. It determines the functional output of cryptographic algorithms, controlling the complexity in breaking encrypted messages, authenticating nodes and users, proving their trustworthiness and validating messages.

Keying material must be distributed and managed. Specifically, a proper public key management system, also known as public key infrastructure (PKI), must assure public key distribution, as well as node legitimacy, key generation, availability, storage and revocation. However, designing key management systems for self-organizing wireless networks is a challenging task due to their self-organization and the lack of a central entity. Moreover, changes in network paradigms towards pervasive computing and the increasing dependency on technology compel to design key management systems more dependable, survivable and scalable [38].

This chapter presents a survivable PKI intending to provide key management operations even in face of attacks or intrusions. Our PKI is based on both the

SAMNAR architecture, and on the correlation of different types of evidences to prove the liability of users for their public keys. The SAMNAR architecture proposes the cooperation among preventive, reactive and tolerant defense lines in order to achieve survivability. Further, the social relationship among users of the network is used as evidence to support decisions related to survivability. We evaluate our survivable PKI by simulations, and results show improvements in terms of effectiveness and survivability to attacks.

The remainder of this chapter is organized in five sections as follows. Section 5.1 presents correlated initiatives towards survivable key management systems. Section 5.2 describes the network and attack models considered in this case study. Section 5.3 details the proposed survivable PKI emphasizing its main operations: the creation of public key and certificates, certificate exchanges, certificate revocation and authentication. Section 5.4 presents the methodology of evaluation, simulation environment and results. Finally, Section 5.5 concludes the chapter.

5.1 Related Work

Many approaches for public key distribution have been proposed towards survivability [21, 122]. The first proposals adapt traditional key management systems to the characteristics of self-organizing wireless networks. Those first proposals rely on the existence of a certificate authority (CA) which issues digital certificates binding an identity to its public key. In the threshold CA scheme [122], for instance, Zhou *et. al* designed a fault-tolerant CA, employing both secret sharing and threshold cryptography techniques to reach redundancy. However, the system must have a central trust entity to bootstrap the key management service. Further, it is still vulnerable to attacks when the number of compromised nodes is greater than a threshold. Hence, for improving its weaknesses, many other PKIs have been proposed [67].

Self-organized key management (PGP-like) [21] is another initiative towards survivability. It modifies *Pretty Good Privacy* (PGP) [123], however the CA functionality is fully distributed. All nodes have the same role being responsible for generating their pair of keys and issuing certificates to the public keys of

nodes they trust. The public key validation process consists in finding a chain of certificates in the local repositories of a node. This chain of certificates lies in a sequence of public key certificates originated in a certificate produced by the node wanting to validate the key until reaching the certificate of the key. Although PGP-like seems to be more satisfactory to the self-organization, it is vulnerable to some attacks, such as Sybil, lack of cooperation and masquerade [91].

Some PKI proposals employ the concept of clusters or multicast communication. In a nutshell, they create groups of nodes generating keys per group in order to provide access control. These proposals present characteristics, such as resiliency, fault-tolerance or scalability that can improve survivability [87, 109]. However, they focus mainly on efficiency neither dealing with a complete survivable system, nor reaching all survivable requirements and properties.

Despite of the previous initiatives, none of them has been designed with survivability in mind. For the best of our knowledge, only few works have proposed survivable key management systems, such as that proposed by Chorzempa *et. al* [22]. In that work, a survivable and efficient key management system for wireless sensor network is presented focusing on robustness and recovery. Methods for distributing, maintaining and recovering session keys are defined to operate even in case of compromised nodes. However, only recovery property is handled without considering together resistance, recognition and adaptability properties.

5.2 Models and Assumptions

This section presents assumptions and models considered in this case study. Table 5.1 summarizes the notation used in this chapter.

5.2.1 Network, trust and attack models

Network model: We focus on multi-hop wireless ad hoc network consisting of n mobile or stationary nodes identified by $X_1, X_2, X_3, ..., X_n$. The network is self-organized and nodes are randomly distributed on a given geographical area. Nodes move on this area following a mobility model. No central infrastructure exists for supporting network services, such as routing, access control

Note	Explanation
i	a given user identity
n	number of nodes in the network
X_i	a node identity
X	PKI nodes set
IG_w	identification of a given group w
IG	set of all initiator groups
m	number of users in an initiator group
p_i	public key of a given user i
s_i	private key of a given user i
P_w	public key of a given initiator group w
S_w	private key of a given initiator group w
$C^i_{S_w}$	public key certificate binding the public key of a given identity i signed with the public key of a given group w
$C^{IG_z}_{S_w}$	group certificate binding the public key of the group IG_z and signed with the private key of a group IG_w
T	the expiration time of a certificate
T_{ex}	certificate exchange time
G	group certificate graph
G_i	repository of updated certificates of X_i
G_i^N	repository of non-updated certificates of X_i
$\|Z\|$	Size of a given set Z
$a\|\|b$	a given information a is concatenated with a given information b
$MAC(w)$	message authentication code of a given group identification
$SIGN[a]_{S_w}$	signing a given information a with S_w
$AUTH[X_i \rightsquigarrow X_v]$	X_i is authenticating p_v of X_v
$(P_u \rightsquigarrow P_v)$	certificate chain between P_u and P_v
$IG_w \rightarrow IG_y$	IG_w issues a certificate for the public key of IG_y

Table 5.1: Notation

or network management. Hence, nodes have similar functionality contributing to the network maintenance, routing process and public key management. However, they hold limited computation, memory and storage capabilities.

Two given nodes X_i and X_j have a *physical wireless link*, if their Euclidean distance is no greater than the communication range (r), and, then, X_i and X_j are called neighbors in respect to each other. A *physical path* between two nodes, for example, X_i and X_k, is a set of subsequent physical wireless links. Two nodes

are physically connected if there is a physical path starting at one and ending at the other. We call *physical network* the set of physical wireless links. No node has complete knowledge of the physical network topology requiring routing to communicate with nodes out of its communication range.

Trust model: Trustworthiness among nodes depends on the existing friendship of users participating on the network. If two users, for example, i and j, are friends, they trust each other and their respective devices, X_i and X_j, can exchange their public keys. A given node trusts in another only if both nodes have exchanged their public keys through a side channel (e.g., over an infrared channel) at the time of a given physical encounter. As presented by Zhang *et. al* [119], we consider a bidirectional trustworthiness between two nodes, that is, if X_i trusts in X_j, X_j also trusts in X_i. This assumption lies in the statistical analysis of the "Web of Trust" resulted from existing relationships among users of PGP. This analysis shows that about 2/3 of the links in the large strongly connected social network are bidirectional [3].

Friend relationships form a spontaneous network [32]. This friend network is independent of the physical network, and it presents social network properties, such as small word and scale-free phenomena [24]. The former defines that most nodes can be reached from every other by a small number of hops [110]. The latter describes that few users in the spontaneous network have the highest probabilities of being chosen as friends by new users. This last phenomenon is also called "the rich get richer" paradigm [24].

We assume the existence of a reputation system [84]. It allows all nodes to locally evaluate neighbor behavior by observation and by second-hand information. Each node in the physical network maintains a table with reputation values of all neighbor nodes. Reputation values are in the interval [0.0,1.0] and represent the behavior of nodes in relation to network operation.

Each node has also a preventive level, that is, a normalized value into the interval [0.0,1.0] meaning how much it is protected against attacks attempting to individually compromise it. The preventive level is automatically calculated based on the existence of preventive mechanisms, such as individual firewalls, anti-virus, spywares and others. Preventive mechanisms make difficult damages produced by individual nodes. We consider that preventive level will be securely

calculated and stored, being hard their manipulation by malicious users. Tamper-resistant software or hardware can be used to store securely preventive levels.

Threats model: Different types of attacks can harm PKIs on self-organizing wireless networks. We focus on attacks that can compromise availability, confidentiality, integrity, authenticity and non-repudiation principles in a public key management system. We consider an attack scenario where an adversary is able to compromise one or more nodes and, consequently, to avoid or delay key management system functions. Specifically, we handle the following attacks: Sybil, masquerade and denial of service (DoS) attacks [28].

Sybil: Sybil attacks occur when adversary nodes create multiple identities in the PKI in order to manipulate keys and certificates in their advantage. False node identities can operate as legitimate ones and, thus, they can violate confidentiality, authentication and non-repudiation principles.

Masquerade: a malicious node can forge the identity of a legitimate node, violating the non-repudiation and authentication principles. Malicious nodes can generate these attacks to participate in the key management as a legitimate node. Moreover, through this attack, nodes may be able to compromise the integrity and confidentiality of the messages.

Denial of service (DoS): a misbehavior node may stop providing authentication service, as well as key storage or certificate generation, distribution or revocation. Hence, it decreases the good operation of key management services. The motivation for this attack can only be saving resources, such as storage or processing, while the node still takes part in the key management system. However, a given compromised node can maliciously participate in the key management system to damage it. These attacks are also called *lack of cooperation* in this case study.

5.3 Survivable Key Management System

In this section, we describe our survivable PKI based on the SAMNAR architecture. It is fully distributed and self-managed in which its nodes are organized in groups without requiring cluster heads. These characteristics contrast with

those of other proposals using cluster concepts [26, 70]. We detail PKI operations as group formation, the creation of public keys and public key certificates, authentication, certificate renew and revocation. We explain them focusing on survivability aspects and taking into account the assumptions and models described in Section 5.2.

5.3.1 Overview

Our PKI follows the "WAN-of-LANs" paradigm [14]. This paradigm proposes the creation of realms with different trustworthiness levels in order to separately reach survivability on each realm first, and then achieve survivability of all PKI. The paradigm does not define the granularity level of the realm, which can be a single node. Our PKI defines three main levels of trustworthiness: node level, initiator group level and system level. These three levels intend to achieve survivability requirements for the public key management system, particularly, decentralization, scalability and self-organization.

Each node is responsible individually for reaching the survivability of the PKI. A node generates its pair of keys, private and public, needing to distribute the public one. The node must assure that its public key will not be forged or modified by malicious nodes, as well as the availability of the keying material. Hence, it employs preventive and reactive security mechanisms to protect itself against attacks or intrusions. Digital certificates, for example, prove the liability of nodes for their public keys, and personal firewalls offer individual protection for the node. Further, it possesses information about the reputation of neighbor nodes in order to assist on the decision about which nodes it will exchange its public key. The pair of keys can be stored in a special firmware or disk space which the access is limited by some kind of passwords.

Initiator groups support survivability characteristics of our PKI. An initiator group is composed of m trustful nodes meaning that all of them have mutually exchanged their public keys by a side channel following existing friend relationship among their owners. Initiator groups assist the distribution of public keys and assure the liability between public key and node identity in a decentralized way. Initiator groups also promote redundancy. Members of a group act as witnesses

of public key exchange between pair of nodes. Moreover, a node can participate in different initiator groups as presented in Figure 5.1. In this example, two initiator groups identified by IG_1 and IG_2 have nodes X_4 and X_5 in common.

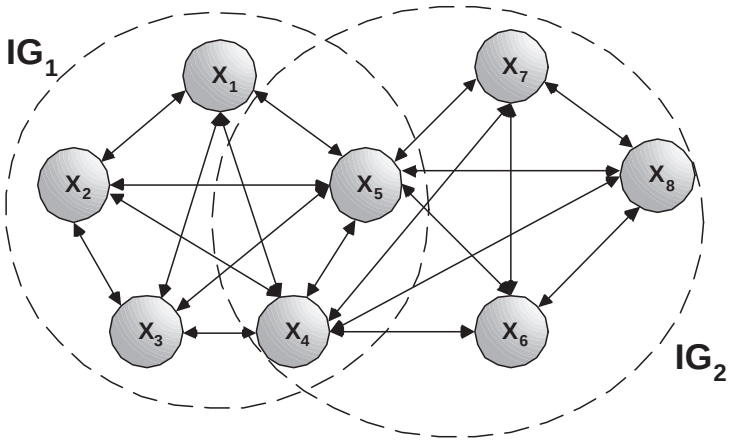


Figure 5.1: Initiator groups

Our PKI depends on initiator groups for executing many operations. Each initiator group owns its pair of keys, being the private one used for signing digital certificates issued by members of the group. Double arrows in Figure 5.1 represent the existence of certificates mutually issued between two nodes. Public key certificates are used to bind a public key to an identity. Hence, in our PKI we have two types of public key certificates: *node certificates* and *group certificates*. Node certificates bind user public keys with user identities, whereas group certificates bind group public keys with group identification. Node certificates are signed with the private key of the group in which the node participates. Group certificates are signed by the private key of another group.

A given node certificate $C^j_{S_w}$ is composed of an expiration time T, the node identity X_j, its public key p_j and the message authentication code (MAC) of X_i initiator group identification. All this information is signed with S_w, that is, the private key of the group IG_w. In addition, certificates also own the X_i initiator group identification. In a nutshell, $C^j_{S_w}$ holds:

$$C^j_{S_w} = (SIGN[T \| X_j \| p_j \| MAC(IG_w)]_{S_w} \| IG_w) \tag{5.1}$$

Group certificates follow the same organization of node certificates. However, a given group certificate $C_{S_w}^{IG_z}$ consists of:

$$C_{S_w}^{IG_z} = SIGN[T \| IG_z \| P_z]_{S_w}, \tag{5.2}$$

where T is the expiration time of the group certificate, IG_z is the group identity, and P_z is the public key of the group IG_z. All this information is signed with the private key of another group, in this example, S_w.

We use an abstract model based on graph theory for supporting the explanation of PKI operations in the next subsections. This approach was used by Hubaux *et. al* [21] and Maurer [65], however, in our model, only group certificates and group public keys are represented in a graph identified by $G(V, E)$. Public keys of groups compose the set of vertices V, and group certificates compose the set of directed edges E. We call G, *group certificate graph*.

Figure 5.2 illustrates a graph G. IG_1, represented by its public key P_1, has issued a certificate for the public key of the groups IG_2 and IG_3, respectively, P_2 and P_3. In the same way, other groups, IG_2, IG_3 and IG_5, have issued certificates for other public keys, P_2, P_4 and P_5. Note that each vertex in the graph corresponds to a set of nodes, their respective public keys and node certificates. Thus, we assume that reaching a group certificate, the system will also be able to reach a node certificate in the group.

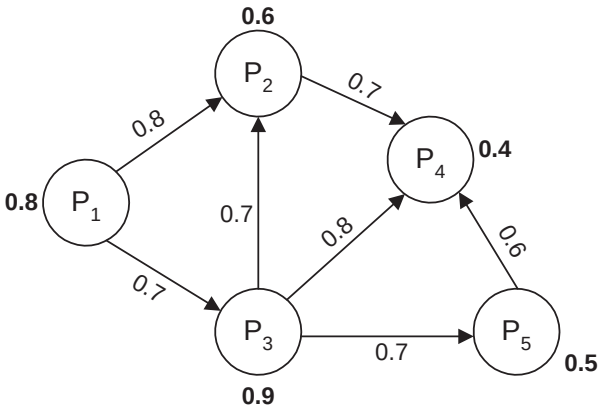


Figure 5.2: Group certificate graph

Vertices and edges of a graph G possess weights. Since each node is associated to a preventive level and a reputation level as described in the trust model of Section 5.2, the weight of vertices in G represents the minimum preventive level among the preventive level of all m nodes of the initiator group. In the same way, the weight of edges in G represents the minimum reputation level among all reputation values of the nodes in an initiator group. The minimum value of preventive or reputation levels demonstrate the weakness of the group in relation to preventive and reactive defense lines.

To summarize the overview of our PKI, Figure 5.3 illustrates models used for explaining PKI operations, and their interrelation. We observe three models. The network model and the trust model were detailed in Section 5.2, and the group certificate graph model was presented in this section. The interrelation among these models is also represented in the figure.

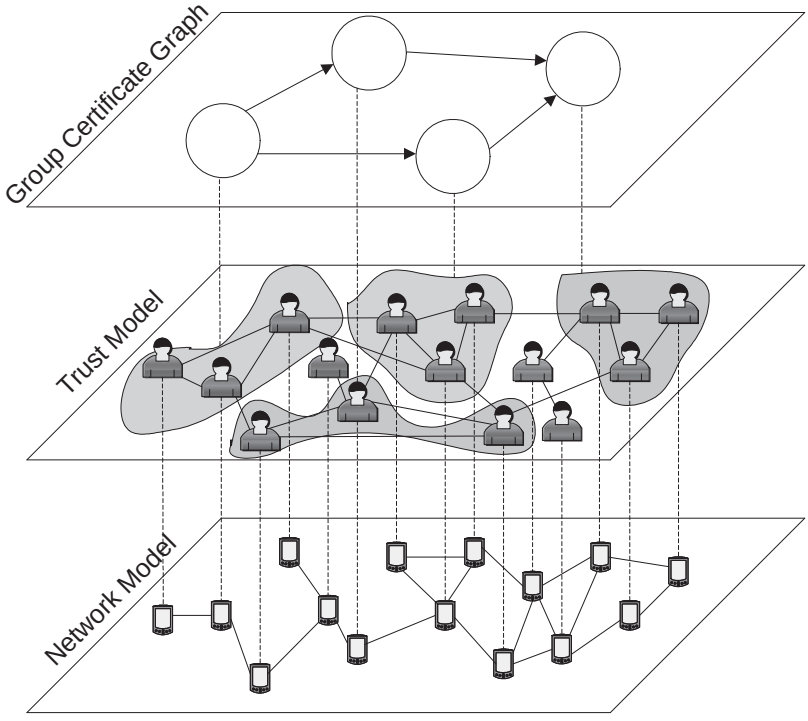


Figure 5.3: Interrelation among all models

The next subsections detail the main operations of our PKI, being them:

- Creating keys and initiator groups;
- Generating pair of group keys;
- Issuing and distributing node and group certificates;
- Exchanging certificates;
- Revoking and renewing certificates;
- Authenticating public keys;
- Validating certificates.

5.3.2 Creation of node keys and initiator groups

Each user i creates individually its pair of keys, p_i and s_i and stores on a node X_i. For participating in the key management system, X_i needs to find $m-1$ **trusted** nodes in order to issue certificates for its public key. Trusted nodes follow the definition presented in Section 5.2 in which a node trusts another only if they have exchanged their public keys through a side channel (e.g., over an infrared channel) at the time of a given physical encounter. The set of m nodes, including X_i, composes a given initiator group IG_w.

Each initiator group owns a unique identification. This feature aims to assist the generation of node and group certificates, as well as other PKI operations. Assuming that the physical network provides unique identification for nodes, such as Media Access Control (MAC) address, we define that the identification of a given initiator group is the hash value generated from the concatenation of all m identifications of members. However, any other approach can be used to identify uniquely initiator groups.

5.3.3 Generating pair of group keys

Initiator groups also own a pair of keys. The m nodes of a given initiator group IG_w generate cooperatively a pair of keys, P_w and S_w, being, respectively, its public and private keys. The generation of P_w and S_w is performed on the initiator

group creation, that is, on the physical encounter of the m nodes. Group key generation follows Pederson's threshold scheme (t, m) [75] being a side channel used to exchange the keying material necessary. However, any other key agreement scheme, that does not need a Third Trust Party (TTP), can be used.

In a nutshell, a share of P_w is generated individually by each node. The generation of shares follows the threshold cryptography scheme. First, a given node X_i of an initiator group IG_w chooses at random (uniform distribution) a secret v_i belonging to $\mathbb{Z}_q$. Then, it calculates individually $P_{w_i} = g^{v_i}$, where:

1. q and p denote large primes such that q divides $p - 1$;
2. $\mathbb{Z}_q$ is the set of positive integers less than q;
3. g is a element of G_q;
4. G_q is the unique subgroup of $\mathbb{Z}_q^*$ of order q.

Each share P_{w_i} is sent for all $m - 1$ nodes in IG_w. When a node receives all $m - 1$ shares, it can calculate P_w by the product of all m shares. As all members receive all shares, they know P_w.

For creating the private key S_w, each node X_i chooses randomly a polynomial function $f_i(z)$ of degree $(t - 1)$, in which $f_i(0) = v_i$, being v_i a secret randomly chosen by X_i. Then, each node X_i calculates a $s_{ij} = f_i(j)$ for every node X_j in the group, where $j = 1, 2, 3, \ldots, m$. X_i sends then s_{ij} to X_j. After receiving $m - 1$ subparts, X_j calculates its share of S_w by $S_{w_j} = \sum_{i=1}^{m} s_{ij}$.

Group keys are generated in a way that public key is known by all members in an initiator group, and the private key is shared with all members of the initiator group by a threshold scheme (t, m). This means that each node in a group owns a share of its private key, and the private key can be built by at least t nodes. This approach aims at increasing PKI availability and resistance against attacks.

5.3.4 Issuing and distributing node and group certificates

After generating P_w and S_w, each node in a given IG_w issues certificates for the public keys of the $m - 1$ other nodes. These certificates are signed with S_w and

locally stored. For signing certificates, S_w must be reconstituted by at least t members of the initiator group, in which t is a value less than m. In the end of this phase all nodes in IG_w possess certificates for all other $m-1$ nodes.

The public key P_w of a given initiator group IG_w also needs to be certified. Groups can issue certificates among themselves binding a given P_w with its identity. IG_z can issue a certificate $C_{S_z}^{IG_w}$ for IG_w, if IG_z believes in IG_w. Many reasons exist for an initiator group IG_z believes that a public key P_w belongs IG_w. The reasons are defined in this study case as:

- if at least one node in IG_z trusts two or more nodes in IG_w;
- two or more nodes in IG_z also participate in IG_w;

The required redundancy with two or more nodes intends to improve the reliability in evaluating public key liability.

5.3.5 Certificate exchange

Nodes periodically exchange their group certificates with their physical neighbors depending on node reputation and preventive level. On the moment of initiator group formation, each node knows certificates of the groups that it participates, and those certificates that have been issued by it or by other members in its group. With the periodic certificate exchange, nodes increase the number of group certificates in their repositories.

A given node X_i requests to its physical neighbors the list of group certificates they keep. Each neighbor responds with a message containing the *hash* values of group certificates in its local repository. This message can piggyback other messages of network protocols, such as those used for discovering neighbor nodes. X_i verifies which certificates it already holds in its repository and requests to their neighbors for missing ones. Hence, neighbor nodes send to X_i only those missing certificates.

Certificate exchanges are performed in time interval T_{ex}. In this case study, we assume that all nodes follow the same value of T_{ex} and that exchanges are not synchronized. Hence, if a given node X_i is sending its certificates to a node X_j, this does not mean that X_j is also sending its certificates to X_i at the same time.

5.3.6 Revoking and renewing certificates

Each node possesses two local repositories to store updated and non-updated certificates. The updated repository of a given node X_i is represented by G_i. This kind of repository holds node or group certificates that are still valid. When the certificate time T expires, it becomes a non-updated certificate and it will be moved on the non-updated repository. The non-updated repository of a given node X_i is represented by G_i^N.

Two kinds of certificate revocation exist: *implicit* and *explicit*. Implicit revocations occur when the validity of the certificate expires, once certificates are issued with an expiration time. This process happens automatically and locally for all certificates stored in the updated repository of each node. No intervention of other nodes in the PKI is requested. Node or group certificates can be implicitly revoked based on the validity period of certificates.

However, many reasons may cause a certificate to become invalid prior to the expiration time. Examples of these reasons are changes in the relationship status between certificate issuer and the key pair owner (e.g., two users have no more friendship relations), and a suspicion that the private key associated with the certificate was compromised. Under such situations, the certificate issuer wants to revoke explicitly the certificate.

Algorithm 1 and Algorithm 2 present, respectively, the procedure of explicit node and group certificate revocation. In Algorithm 1, a node X_v, member of a group IG_y, wants to revoke the node certificate $C_{S_y}^i$ of a node X_i. In this case, node X_v creates a message msg with two information, message type and the node certificate to be revoked. This message is sent to members of all groups that have issued a certificate for IG_y.

Receiving a *nodeRevocation* message, all nodes store revoked node certificate in a local Certificate Revocation List (CRL). If the receiver node is member of a given group, certificate issuer of IG_y, then it also sends this revocation message for all nodes that have requested an updated of $C_{S_w}^{IG_y}$. Members of a given IG_y keep a list L containing all nodes that had requested an update of certificates.

Algorithm 2 presents the explicit revocation of a given group certificate $C_{S_y}^{IG_w}$ by a node X_v. X_v creates a message of the type *groupRevocation*. Then, X_v

Algorithm 1 REVOKE($C^i_{S_y}$)

1: $msg.type \leftarrow$ nodeRevocation
2: $msg.certificate \leftarrow C^i_{S_y}$
3: **for all** $IG_w \in IG : (IG_w \rightarrow IG_y) \in G$ **do**
4: **for all** $X_j \in IG_w$ **do**
5: $send(msg, X_j)$
6: **end for**
7: **end for**

node $X_j \in IG_w$ ***receiving the*** msg

1: $CRL_j \leftarrow CRL_j \cup msg.certificate$
2: $L \leftarrow$ List of nodes requested $C^{IG_y}_{S_w}$ update
3: **for all** $X_l \in L$ **do**
4: $send(msg, X_l)$
5: **end for**

node X_l ***receiving the*** msg

1: $CRL_l \leftarrow CRL_l \cup msg.certificate$

Algorithm 2 REVOKE($C^{IG_w}_{S_y}$)

1: $L \leftarrow$ List of nodes requested $C^{IG_w}_{S_y}$ update
2: $msg.type \leftarrow$ revoke
3: $msg.certificate \leftarrow C^{IG_w}_{S_y}$
4: **for all** $X_j \in L \cup IG_y \setminus X_i$ **do**
5: $send(msg, X_j)$
6: **end for**

node X_j ***receiving a revoke message***

1: $C^{IG_w}_{S_y} \leftarrow msg.certificate$
2: $G_j \leftarrow G_j \setminus C^{IG_w}_{S_y}$
3: $G^N_j \leftarrow G_j \cup C^{IG_w}_{S_y}$
4: $CRL_j \leftarrow CRL_j \cup C^{IG_w}_{S_y}$

sends msg for all nodes that have requested an updated of $C^{IG_w}_{S_y}$. Receiving a *groupRevocation* message, a node moves revoked group certificate from its local non-updated certificate repository to its local updated certificate repository.

Algorithm 3 UPDATE($C_{S_y}^{IG_w}$)

1: $L \leftarrow$ List of nodes requested $C_{S_y}^{IG_w}$ update
2: $msg.type \leftarrow$ groupRenewing
3: $msg.certificate \leftarrow C$
4: **for all** $X_j \in L \cup IG_y \setminus X_i$ **do**
5: $\quad send(msg, X_j)$
6: **end for**

node X_j ***receiving an update message***

1: $C_{S_y}^{IG_w} \leftarrow msg.certificate$
2: $Update\_Counter_{C_{S_y}^{IG_w}} \leftarrow Update\_Counter_{C_{S_y}^{IG_w}} + 1$
3: **if** $Update\_Counter_{C_{S_y}^{IG_w}} \geq t$ **then**
4: $\quad G_j \leftarrow G_j \cup C_{S_y}^{IG_w}$
5: $\quad G_j^N \leftarrow G_j \setminus C_{S_y}^{IG_w}$
6: **end if**

Before node certificates have their time expired, their initiator group can issue a new version of the certificate. If a subset of t members in a given IG_y do not have any reason to revoke a given node certificate $C_{S_y}^i$, they can issue a updated certificate with a new expiration time. Using t nodes, instead of the m nodes of the group, minimizes the overhead in the physical network without losing redundancy feature. After updating a node certificate, one copy is sent for all nodes in a given initiator group.

Group certificates can also be renewed by a subset of t nodes of the group that has originally issued the certificate. A new version of the certificate, with a new expiration time, is sent for all nodes in the issuer group and for all nodes that have previously requested it. In order to minimize the communication overhead, a node can send the updated certificate only to nodes that had requested a validation of this certificate recently. If a node does not receive an updated version of an expired certificate, it will move this certificate to its non-updated repository.

Algorithm 3 presents the procedure for renewing a given group certificate $C_{S_y}^{IG_w}$ by a node X_i. In the example, X_i creates a message of the type *groupRenewing*. Then, X_i sends this message for all nodes that had requested a validation of this certificate. The message receiver node will wait for at least t messages be-

fore considering this certificate as updated. Finally, the receiver node stores the certificate in the update repository.

5.3.7 Authenticating public keys

Supposing X_i a node possessing the public key p_j of a node X_j, X_i must authenticate it before using. In a nutshell, the authentication process consists of:

- X_i requests to X_j a certificate issued for its public key.
- X_j replies with all certificates issued for its public key. If X_j participates in only one group, then just one certificate is replied, else different certificates are replied. Each certificate is signed with the private key of the initiator group that has issued the certificate.
- X_i selects one of the certificates and validates it. The validation of the certificate is performed using the public key of the initiator group that issued it. For example, if X_i selected the certificate $C^j_{S_w}$, then the public key P_w will be required to validate it.
- if X_i cannot validate the certificate then the authentication of the public key is not possible.

If X_i has chosen $C^j_{S_w}$, it needs to use P_w to validate the certificate. However, before using P_w, it needs to be authenticated. The authentication of P_w is performed by chains of group certificates. Then, for authenticating P_w, X_i searches, in its updated repository, at least two disjoint chains of valid group certificates between its group and the initiator group IG_w.

A chain of group certificates is a sequence of group certificates in which:

1. the first certificate is authenticated directly by a given node X_i using the public key of its group;
2. other certificates are authenticated by the public key found in the previous certificate;

3. the last certificate has the public key of the initiator group that issued the certificate $C^{j}_{S_w}$.

As an example, supposing that Figure 5.2 represents the group certificate repository of a given node X_i, member of IG_1, and that it wants to authenticate the public key of a given node X_j in IG_4. Thereby, X_i must find at least two chains of valid certificate connecting P_1 and P_4 in its local group certificate repository. In the example, X_i can use the chains $P_1 \rightarrow P_2 \rightarrow P_4$ and $P_1 \rightarrow P_3 \rightarrow P_4$ to authenticate the public key P_4, and then, authenticate the public key of X_j.

If X_i does not find at least two chains in its updated repository, it merges its updated repository with those of X_j. Then, X_i searches again for at least two chains of group certificates. If even after merging the repositories, X_i does not find the chains of certificates, it tries to find them in the union of its updated and non-updated repositories. In the successful case, X_i needs to verify if the binding between identity and public key into non-updated certificates is still valid. The validation is performed by any node in the group that has initially issued the certificate. If none of these cases happen, X_i will not be able to authenticate the group public key or the node public key.

Algorithm 4 presents pseudo-codes of authentication procedure. On Algorithm 4, node X_i wants to authenticate the public key of node X_j, using AUTHENTICATION(X_j) function.

5.3.8 Validating certificates

Certificates are issued with an expiration time T. When a node X_i needs to use a certificate, it must verify if the certificate is still valid, that is, if its time has not expired. This process is called validation of the certificate, and for performing validation the public key used to sign the certificate is essential. After authenticating the public keys as described in previous section, the node uses it to verify if the certificate was not modified, accessing the value of T.

If T has not expired, the node can use data existing in the certificate. If T has expired, X_i sends a message, called Validate Request (VREQ), for all members of the issuer initiator group of a certificate $C^{IG_w}_{S_y}$, wanting to validate. X_i waits for at least t messages, called Validate Reply (VREP), from the members of the

Algorithm 4 AUTHENTICATION(X_j)

1: $IG_{X_i} \leftarrow$ Initiator groups of X_i
2: $IG_{X_j} \leftarrow$ Initiator groups of X_j
3: $Counter_{i \to j} \leftarrow 0$
4: **for all** $IG_i \in IG_{X_i}$ and $IG_j \in IG_{X_j}$ **do**
5: **if** $\exists(IG_i \rightsquigarrow IG_y) \in G_i$ **then**
6: $Counter_{i \to j} = Counter_{i \to j} + 1$
7: **else if** $\exists(IG_i \rightsquigarrow IG_j) \in G_i \cup G_j$ **then**
8: $Counter_{i \to j} = Counter_{i \to j} + 1$
9: **else if** $\exists(IG_i \rightsquigarrow IG_j \in G_i \cup G_i^N$ **then**
10: $validate(C_{S_y}^{IG_w})$ $\forall$ $C_{S_y}^{IG_w}$ not updated in chain.
11: **if** all $C_{S_y}^{IG_w}$ are validated **then**
12: $Counter_{i \to j} = Counter_{i \to j} + 1$
13: **end if**
14: **end if**
15: **end for**
16: **if** $Counter_{i \to j} \geq 2$ **then**
17: **return true**
18: **else**
19: **return false**
20: **end if**

initiator group. If X_i does not receive these replies in a timeout period, it will not be able to validate the certificate. This process is used to assure that no new version of the expired certificate was issued. In general, all certificates stored on the non-updated repository require validation. Algorithm 5 summarizes the process of certificate validation.

5.4 Evaluation

The main purpose of our evaluations is to analyze the practicability of our assumptions, show the survivability of our PKI against attacks, and quantify its communication cost and effectiveness. In this section, we describe the evaluation environment, present analytical analyses and provide results.

Algorithm 5 VALIDATE($C_{S_y}^{IG_w}$)

on requesting node X_i***:***

1: $Reply\_Counter_{C_{S_y}^{IG_w}} \leftarrow 0$
2: $msg.type \leftarrow VREQ$
3: $msg.certificate \leftarrow C_{S_y}^{IG_w}$
4: **for all** $X_k \in IG_y$ **do**
5: $\quad send(msg, X_k)$
6: **end for**

X_i ***receiving a*** **true** $VREP$***:***

1: $C_{S_y}^{IG_w} \leftarrow msg.certificate$
2: $Reply\_Counter_{C_{S_y}^{IG_w}} \leftarrow Reply\_Counter_{C_{S_y}^{IG_w}} + 1$
3: **if** $Reply\_Counter_{C_{S_y}^{IG_w}} \geq t$ **then**
4: $\quad$ **return true**
5: **end if**

nodes of IG_y ***receiving a*** $VREQ$***:***

1: $msg.type \leftarrow VREP$
2: **if** $msg.certificate$ still valid **then**
3: $\quad reply(msg, \textbf{true})$
4: **else**
5: $\quad reply(msg, \textbf{false})$
6: **end if**

5.4.1 Investigating the viability of initiator group formation and redundancies

The trust model presented in Section 5.2 provide support for many assumptions and PKI operations. This trust model is the base for initiator group formation and for the existence of redundant relationships among groups. Since forming an initiator group is a requirement for a node to participate in the PKI, in this section we analyze the practicability of having such groups in a friend social network. In the same way, we also evaluate the viability of having the required redundancies among groups.

For all analyses, we have used a practical example of friend social network, the PGP. As in our trust model, in PGP public keys are exchanged in a self-organized manner and certificates are signed based on the friend relationship.

Clique Size	# of Cliques	# of Maximal Cliques
> 0	293431	29070
1	956	9
2	14557	1921
3	47661	4460
4	78016	6599
5	77160	6395
6	49150	4893
9	716	351

Table 5.2: Clique statistics for the PGP graph with $|V| = 956$ and $|E| = 14647$

Hubaux et. al [101] have demonstrated that this network formed by public keys and certificates reflects existing social relationships between users. This network presents small world and scale free phenomena.

For analyzing the viability of existing initiator groups and redundant relationships among them, we use the PGP database at http://keyring.debian.org/, and we have applied the methodology and metrics proposed by Latapy *et. al* [55]. Initially, we observe the PGP database as a symmetric graph $G = (V, E)$, in which V is the set of public keys representing the vertices of G, and E is the set of certificates representing its edges. For G, we have extracted maximal cliques of different sizes. Cliques in a graph G means a subset of V such that any two its vertices are connected by an edge of E. A clique is called maximal if it is included in no other clique. For our PKI, cliques represent initiator groups in which its vertices correspond to users or nodes and, thus, the edges symbolize that all vertices have symmetrically changed their public keys.

Table 5.2 presents statistics about cliques in the PGP graph. We have used algorithms proposed by Uno *et. al* [100] for finding cliques. We compare the number of general cliques with the number of maximal cliques. We observe that only 9 vertices, in toto 0.9% of the vertices in PGP graph, do not participate in groups. As expected, the number of maximal cliques is lower than the number of cliques. In general, the number of cliques with a size equal to 4 or 5 is greater than others.

In order to evaluate redundancies in PGP graph, we have transformed G in a bipartite graph $G_b = (\top, \bot, E)$. In G_b, $\top$ and $\bot$ are disjoint set of vertices,

respectively, the top and bottom vertices, and $E \subseteq \top$ x $\bot$. Following the methodology presented in [55], $\top$ is a set of vertices representing maximal cliques of the graph. The bottom set is composed of vertices participating in cliques. Links exist only between top and bottom vertices. Relating these concepts to our PKI, bottom vertices are public keys representing their users or nodes, and top vertices are initiator groups. Edges represent the participation of nodes or users into initiator groups.

First, we have verified basic statistics in PGP graph. In Figure 5.4, we observe the distribution of vertex degree, respectively, for top and bottom vertices. Vertex degree represents the number of neighbors of a given vertex. As observed in other social networks [55], PGP graph also follows the power law for the bottom degree distribution, while the top degree distribution is Poisson shaped.

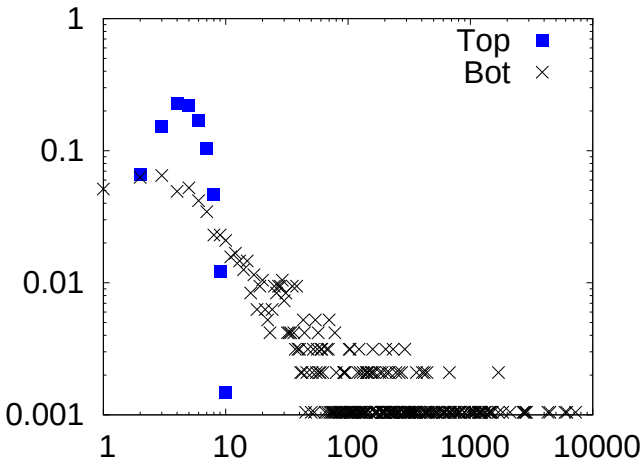


Figure 5.4: Degree distributions

We use the redundancy coefficient of a given user v, $rc(v)$, to analyze the redundancy between initiator groups in PGP. Considering the trust model presented in Section 5.2, the $rc(v)$ is a fraction of pairs of neighbors of v linked to another user than v. Being $N(v)$ the set of neighbors of a user node v, redundancy coefficient is defined as presented in Equation 5.3.

In Figure 5.5, we observe cumulative distributions of redundancy coefficient for top and bottom vertices. For bottom ones, 60% of them has redundancy coefficient equal or higher than 80%, whereas 80% of these vertices has redundancy

$$rc(v) = \frac{|\{\{u,w\} \subseteq N(v), \exists v' \neq v, (v',u) \in E \text{ and } (v',w) \in E\}|}{\frac{|N(v)(N(v)-1)|}{2}} \tag{5.3}$$

coefficient equal or higher than 50%. This shows the high redundancy of PGP graphs. As expected, the redundancy coefficient is lower for top vertices.

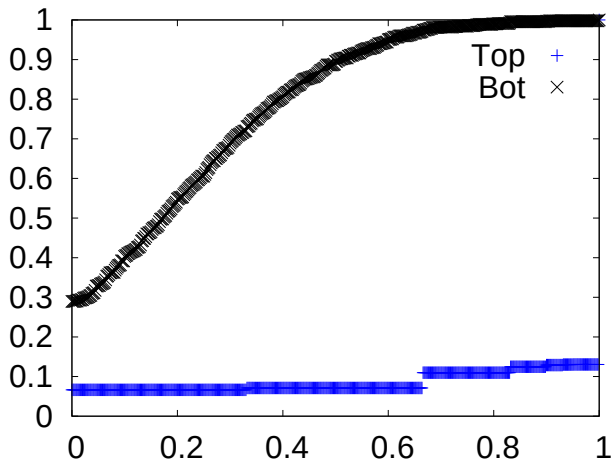


Figure 5.5: Redundancy distributions

5.4.2 Discussing survivability to threats

Following the threat model of Section 5.2, malicious users can compromise a PKI in many ways. A dishonest user may try to trick other users into believing in a false user-key binding by issuing false node certificates. For example, the user may issue a certificate that binds a key p_v to a user f instead of user v or other variation of this case.

In our PKI, the probability of the dishonest user to have success is minimal. First, for using the false node certificate, the dishonest user needs to validate it. Knowing that the certificate must be signed with a private key of a given initiator group and, for validating it, a group public key will be used after its validation, if the false node certificate is not signed, it will not be validated.

Supposing that the dishonest user/node has generated $m-1$ false identities and created its own group, this group will need to be trusted by another group.

That is, at least two nodes of the false group must participate in an honest group, and hence, the dishonest user will need to convince $m - 2$ honest users, in the worst case.

Another situation is the dishonest user to convince only one user in the honest group to trust in at least two users in the false group. However, for this, the honest user will be based on the preventive levels of the correspondent nodes and on their reputation levels. Considering that the reputation level will be calculated following recommendations of different and random nodes, convincing an honest node to trust false identities can be more difficult than the first situation.

Considering that the false group manages to get a certificate for its public key. The validation of this certificate for its posterior use is another obstacle for the dishonest user. In our PKI, at least two disjoint chains of certificates must be found in the group certificate graph for validating a group certificate. It means that at least two different groups must have issued certificates for a false group. For achieving this, the dishonest user needs to persuade many other honest users, decreasing the probability of a false node certificate being successfully authenticated.

Other threats can happen in a given PKI, such as masquerade or DoS attacks. Masquerade attacks are prevented in our proposal by the formation of initiator groups where users know well the identity of the others. Our PKI can easily survive to DoS attacks, once that preventive mechanisms will minimize the possibility of individual nodes to be compromised; misbehaviors, such as lack of cooperation can be detected by reputation systems or other mechanisms; and the existing redundancy and fully distribution contributes to increase the tolerance to successful attacks or intrusions.

5.4.3 Analyzing communication cost

In this section, we analyze the communication overhead of our PKI generated by certificate authentication, revocation and renewing operations. Communication cost is measured in quantity of messages.

Certificate Authentication

In our PKI, when node X_i wants to authenticate the public key of a given node X_v, most operations must be performed locally by X_i itself. As discussed in Section 5.3.7, only if X_i does not find two valid chains in its repositories, it will use its non-updated certificate repository.

For each non-updated certificate on the chains used to validate the certificates of X_v, node X_i must request to the issuers of the certificate. Thereby the total cost to authenticate depends on the quantity of non-updated certificates exist on found chains. In our PKI, the overhead communication to validate a given group certificate $C_{S_y}^{IG_w}$, denoted by $VCO(C_{S_y}^{IG_w})$, is:

$$VCO(C_{S_y}^{IG_w}) = \sum_{X_j \in IG_y} (VREQ + VREP) \; . \; \Delta h \tag{5.4}$$

in which Δh is the average number of hops between PKI nodes. As two messages are needed for each member of issuer group, the cost of validating a group certificate is $O(2m)$ messages.

Certificate Revocation

For revoking explicitly a group certificate, each member of group revoking a certificate sends a message for all other members of its group, and for all other nodes that requested an update of this certificate. Remembering that all nodes keep a list L of nodes that requested certificates validation. Let be L as the list of nodes that requested an updated of $C_{S_y}^{IG_w}$, so the overhead communication to revoke a group certificate $C_{S_y}^{IG_w}$, denoted by $RCO(C_{S_y}^{IG_w})$, is:

$$RCO(C_{S_y}^{IG_w}) = \sum_{X_j \in L \cup IG_y} (\text{revoke msg}) \; . \; \Delta h \tag{5.5}$$

in which Δh is the average number of hops between PKI nodes. The total cost depends on the quantity of nodes that had requested validation of the certificate has been revoked.

Certificate Renewing

When t nodes of a given group want renewing a group certificate $C_{S_y}^{IG_w}$, they send the new certificate version for all nodes that requested an update of the certificate and for all other member of group. Let be L as the list of nodes that requested an updated of $C_{S_y}^{IG_w}$, the overhead communication to update/renew a group certificate $C_{S_y}^{IG_w}$, denoted by $UCO(C_{S_y}^{IG_w})$, is:

$$UCO(C_{S_y}^{IG_w}) = \sum_{X_i \in IG_y} \sum_{X_j \in L} (\text{update msg}) \; . \; \Delta h \tag{5.6}$$

in which Δh is the average number of hops between PKI nodes.

5.4.4 Simulation analysis

This section presents metrics and the simulation environment used to evaluate our PKI in face of DoS and Sybil attacks.

Metrics

Considering two given certificates represented by their public keys, P_u and P_v, in a group certificate graph, $(P_u \rightsquigarrow P_v)$ represent a certificate chain between the two vertices. An association $(X_i \rightsquigarrow X_j)$ between two given nodes, X_i and X_j, means that X_i is able to authenticate the certificate of X_j, that is, X_i can find at least two disjoint paths connecting any initiator group of X_i with any one of X_j. Also, let be V as PKI node set and IG as initiator group set.

For evaluating our PKI, we use the following metrics: *Group Certificate Exchange Convergence* (CE), *Ratio of User Authentication* (UA), *Group Reachability* (GR), *Non-Compromised Group* (NCG) and *Non-Compromised Authentication* (NCA). CE, UA and GR are used to evaluate scenarios under DoS attacks, whereas NCG and NCA are used to evaluate scenarios under Sybil attacks. These metrics are defined as:

- CE is the average percentage of group certificates in the local repositories of the nodes at time t. It also represents the time needed by all nodes to reach all groups of the PKI. The ideal value for this metric is 100%, however

some conditions, such as the PKI initialization, group formation, attacks and others can decrease this percentage. CE can be defined as follows:

$$CE(t) = \frac{\sum_{i \in X} CE_i(t)}{|X|} \quad \text{in which} \tag{5.7}$$

$$CE_i(t) = \frac{\sum_{IG_w, IG_y \in IG} (P_w \rightsquigarrow P_y) \in (G_i \cup G_i^N)}{\sum_{IG_z, IG_x \in IG} (P_z \rightsquigarrow P_x) \in G} \tag{5.8}$$

- UA is the average percentage of user authentications after the convergence time. This metric is quantified by the certificate chains in updated and non-updated repositories of a node X_i. User authentications are counted only if two or more disjoint certificate chains are found for authenticating the node. Under attack, this metric will also indicate the survivability of the PKI evaluating if nodes will be able to authenticate others even in face of DoS attacks. UA can be defined as follows:

$$UA = \frac{\sum_{i \in X} UA_i}{|X|} \quad \text{in which} \tag{5.9}$$

$$UA_i = \sum_{j \in X} (X_i \rightsquigarrow X_j) \in (G_i \cup G_i^N) \tag{5.10}$$

- GR is the average percentage of certificate chains for achieving group certificates in the updated and non-updated group repositories of a node X_i at time t. The difference in relation to UA is that we quantify only group certificates without needing to find two or more disjoint certificate chains for authentication. Let IG_{X_i} as the initiator groups of X_i, so GR can be defined as follows:

$$GR(t) = \frac{\sum_{i \in X} GR_i(t)}{|X|} \quad \text{in which} \tag{5.11}$$

$$GR_i(t) = \sum_{\substack{IG_w \in IG_{X_i} \\ IG_z \in IG}} (P_w \rightsquigarrow P_z) \in (G_i \cup G_i^N) \tag{5.12}$$

- NCG is the percentage of non-compromised groups even in the presence of dishonest nodes in the network. This metric represents the survivability of the PKI against Sybil attacks.

$$NCG = \frac{\sum_{IG_w \in IG} NCG_w}{|IG|} \quad \text{in which} \tag{5.13}$$

$$NCG_w = \begin{cases} 1 & \text{if} \quad \nexists\, f \in IG_w : f \text{ is a false identity} \\ 0 & \text{otherwise} \end{cases} \tag{5.14}$$

- NCA is the percentage of groups that do not have their public key authentication compromised by dishonest nodes. This metric represents the survivability against Sybil attacks of the authentication process. Let be F the set of Sybil nodes, NCA can be defined as follows:

$$NCA = \frac{\sum_{i \in X} NCA_i}{|X|} \quad \text{in which} \tag{5.15}$$

$$NCA_i = \begin{cases} 1 & \text{if} \quad \nexists\, (P_i \rightsquigarrow P_f) \quad \forall f \in F \\ 0 & \text{otherwise} \end{cases} \tag{5.16}$$

Environmental setup

We use the Network Simulator 2 (NS-2), version 30 to evaluate the performance and survivability of our PKI in face of DoS and Sybil attacks. To evaluate our PKI, a DoS attacker does not collaborate with the PKI services, mainly in the certificate exchange mechanism.

In the simulations, 100 nodes use the IEEE 802.11 distributed coordination function (DCF) as medium access control protocol. Their radio propagation follows two-ray ground propagation model and the communication range is 120m.

Nodes move on an area of about 1000 sq meters following the random waypoint model with a maximal speed of 20m/s and pause time equal to 20s. The total time of simulations is 1500s and results are averages of 35 simulations with 95% confidence interval.

Public and private keys are created by nodes only during group formation. Certificates are also issued during group formation and there is no misbehavior detection mechanism in the network. Certificate exchange interval T_{ex} is 60 seconds.

According to Table 5.2, social networks present a great number of cliques with a size equal to 3, 4, 5 and 6. We evaluate our PKI varying values for m between 3 and 6. The goal is to verify the impact of the initiator group size in the effectiveness and survivability. Trust relationships are formed following the model proposed by Viger and Latapy [105].

Table 5.3 compares values found in PGP graphs with those of random graphs. It was considered following parameters: the clustering coefficient, that is the probability of graph vertices forming a clique, the redundancy between cliques and the distance between nodes. Note that parameters in PGP and our graphs are similar, that means that used graphs present a social behavior.

Parameters	PGP graphs	Random graphs
clustering coefficient	0.030	0.037
redundancy between cliques	0.213	0.282
distance between nodes	3.739	3.726

Table 5.3: Comparison of parameters between PGP and random graphs

5.4.5 Results

Initially, we analyze the effectiveness of our PKI scheme by means of the *Group Certificate Exchange Convergence* (CE) metric. Figure 5.6 compare the self-organized public key system proposed by Hubaux et. al [21] (we called PGP-Like) and our PKI considering initiator groups of 3, 4, 5 and 6 members. Scenarios without attackers and scenarios with 5%, 10% and 20% of misbehavior nodes are observed. We consider that misbehavior nodes issue certificates and form

groups, but do not cooperate in the certificate exchange mechanism. That is, they request and store certificates in their local certificate repository, but do not reply requests.

In our PKI, CE reaches 100% of convergence before PGP-Like achieves, independently of the groups size and the number of misbehavior nodes. When m is equal to 6, CE reaches 100% approximately after 500 seconds of network lifetime. Already for m equal to 3, 4 and 5, 100% of CE is achieved before 300 seconds of network lifetime. Again, this behavior is independent of the percentage of attackers.

Figure 5.7 presents results for the *Group Reachability* (GR) metric in scenarios with the presence of 0%, 5%, 10% and 20% of misbehavior nodes. We observe that independent of percentage of misbehavior nodes, GR presents same behavior. With m equal to 3, 4 and 5, GR reaches 100% approximately after 200 seconds of simulation lifetime. When m is equal to 6, GR does not reach 100%, however it presents values close to 90%.

Figure 5.8 compares results found for the *Ratio of User Authentication* (UA) after convergence time. Different group sizes are considered, as well as different percentage of misbehavior nodes. Results show that UA present same values

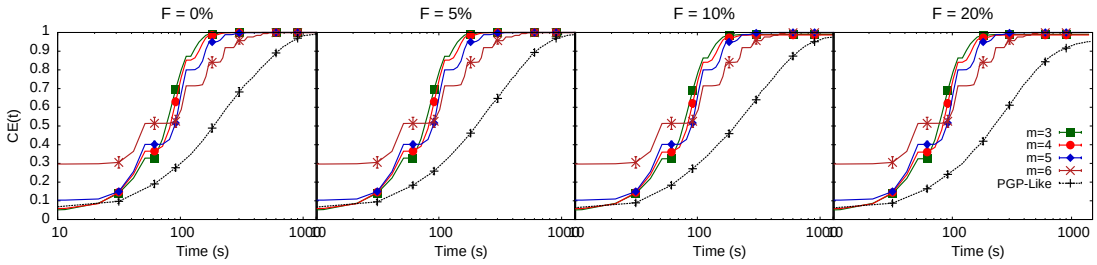


Figure 5.6: Comparing convergence time of CE under DoS attacks

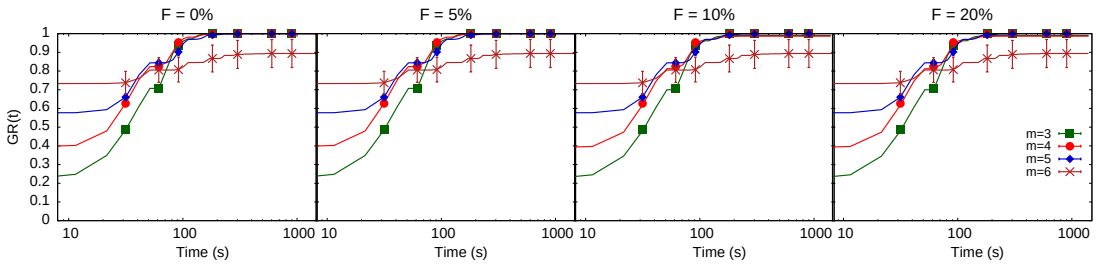


Figure 5.7: Comparing convergence time of GR under DoS attacks

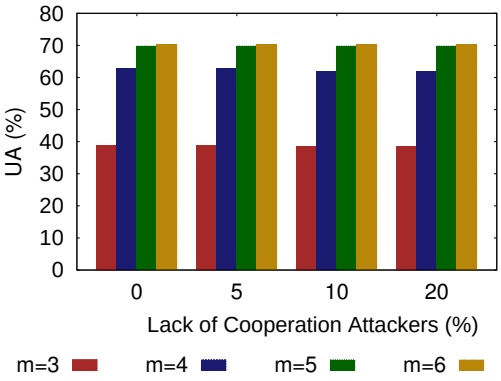


Figure 5.8: UA under DoS attacks

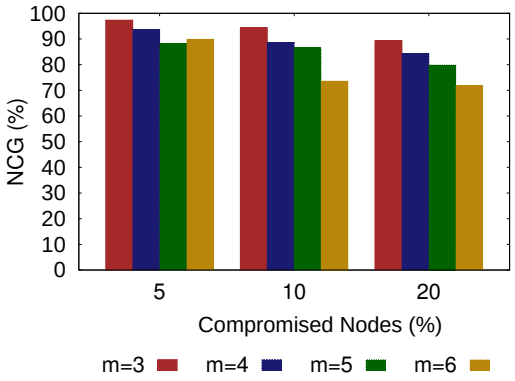


Figure 5.9: NCG under Sybil attacks

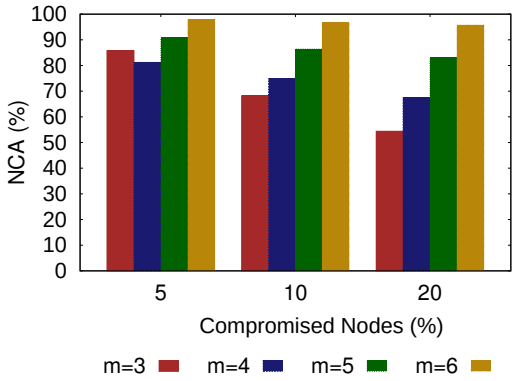


Figure 5.10: NCA under Sybil attacks

independently of misbehavior node percentage. We observe the influence of initiator group size in the percentage of authentications. Further, results show that while group size increases, the percentage of user authentication also increases. When m is equal to 6 or 5, for example, UA reaches 70% of valid user authentications, whereas when m is equal to 3, this value is about 40%. We observe also that higher percentage of attacks does not result in a reduction of the user authentication ratio when compared with the results without attacks. This behavior shows the survivability of our PKI to DoS attacks. Though lower initiator groups present lower UA, no difference is observed between its results under 0% of attack and other percentages.

Figure 5.9 and Figure 5.10 present results related to *Non-Compromised Group*

Ratio (NCG) and *Non-Compromised Authentication Ratio* (NCA) respectively. These metrics evaluates the survivability of our PKI in the presence of Sybil attacks. In our simulation, malicious nodes create fake nodes or impersonate authentic identities, forming initiator groups with them. After, they try to compromise authentic nodes and persuade them to issue certificates to false groups or nodes. The objective of malicious nodes is to compromised a great number of PKI nodes. If two nodes of a same group are compromised, this group can issue a certificate to a fake group. Higher number of compromised groups results in higher probability of a false identity to be authenticate by a valid node.

Figure 5.9 analyzes the survivability of our PKI to the Sybil attacks. Results show that in the presence of 5% of misbehavior nodes, more than 90% of groups are not damaged independently of the group size. When m is 3 this value is close to 99%. When the percentage of misbehavior nodes is 10% and m is equal to 3, NCG is about 95%. This value decreases when m is equal to 4 and 5, being close to 90%. When the number of members in the initiator group is is 6, NCG is still about 70%. This occurs because in larger groups the probability of find two or more nodes is higher, then a malicious nodes are able to compromise more groups. When the percentage of misbehavior nodes is 20%, more groups are driven to issue certificates to a fake groups. However, results still show the survivability of our PKI. When m is equal to 3 almost 90% of groups are not affected, and when m is equal to 4 and 5 this value is about 85% and 80%, respectively. Only when m is 6, NCG presents a lower value, about 70%.

Finally, Figure 5.10 presents the impact of Sybil attack and the group size to the authentication process. Results show that when m is equal to 6, the percentage of valid nodes that do not authenticate false identities is about 98% when PKI is under 5% of attackers. This value is close to 97% in the presence of 10% of attackers and higher than 95% when percentage of attackers is 20%. When our PKI is under 5% of attackers, the percentage of valid nodes that do not authenticate a false identity is higher than 80%. When m is equal to 5, this value is about 90%. When the percentage of attackers is 10% and m is equal to 5 or 6, NCA is higher than 80%. With m equal to 4 or 3, this value is 74% and 68%, respectively. When PKI is under a high number of attackers (20%) the NCA presents a value lower than 70%, to m equal to 3 or 4. However, when m

is equal to 5 this value is higher than 80% and when m is equal to 6, it is about 95%.

5.5 Conclusions

This chapter presented a survivable Public Key Infrastructure (PKI) for self-organizing wireless networks. Its goal consists in making public key management system able to provide its services and distribute keying material even in face of attacks or intrusions. In order to reach survivability, our PKI follows the SAM-NAR architecture approach in which preventive, reactive and tolerant defense lines are employed together and coordinated in adaptive way. It attains the survivability properties by different mechanisms, such as the employment of different evidences to prove the liability of users for their public keys, the formation of initiator groups based on social relationships, and the use of redundancy in many PKI operations.

Survivability is gradually achieved on three levels: node, initiator groups and all system. First, each node is responsible for its protection against attacks. Preventive mechanisms, such as personal firewalls or anti-virus, are employed to attain this goal. Further, the node is also responsible for deciding in which neighbor it will trust. To support this decision, reactive mechanisms are applied, such as reputation systems or even the trust model used. Nodes follow social relationships existing among users as trust model. Individually, a node generates its pair of keys, private and public. It securely stores the private one and distributes the public key.

The second level of survivability is achieved by initiator groups. These groups are composed of m trustful nodes, meaning a set of nodes whose owners have a mutual friend relationship among them. Trusted nodes exchange their public keys by a side channel and generate a pair of keys for the initiator group. These pair of keys is issued in a collaborative way by all m members of the initiator group and, in this case study, a threshold cryptography scheme was employed to support this operation. The private key of the group is used to sign certificates issued for the public keys of the nodes. Node certificates with the public key of the node are distributed among all members of the initiator group. The number

of members in an initiator group must be higher than two, since the goal is that third nodes provide a kind of witness for the exchange of public keys between pair of nodes. Finally, each initiator group presents a preventive and reputation levels resulted from how much nodes in the initiator group are protected against attacks and their reputation.

The third level of survivability is the system level. Initiator groups are employed to accomplish the survivability on keying material distribution for a set of nodes. However, to attain the survivability for all the PKI, initiator groups must be integrated. In this way, certificates are also issued for public key of groups in order to allow the authentication of node public keys for all nodes participating in the network. Certificates for groups are issued by other groups if one group trusts another one. A group trusts another, if one node in a given group 1 trusts at least two nodes of the group 2, or if at least two nodes are mutual for both groups. The redundancy is required to reinforce the tolerant defense line of the PKI. Public keys are authenticated finding two chains of certificates between initiator groups. A chain of certificates consists in a sequence of public key certificates originated in a certificate produced by the node wanting to authenticate the key until a certificate for the key. In the chain of certificate each previous certificate owns a public key that authenticate the next certificate.

Different analyses were performed in relation our PKI. We evaluated the viability of initiator group formation showing a higher probability of forming groups with 4 or 5 members. We analyzed the cost of communication for performing the main operations of our PKI. And we evaluated the survivability of our PKI under different percentage of attacks DoS attacks (also called lack of cooperation attacks) and Sybil attacks. For the survivability evaluation, we defined a set of metrics as *Group Certificate Exchange Convergence*, *Ratio of User Authentication*, *Ratio of Group Reachability*, *Percentage of Non-Compromised Group* and *Percentage of Non-Compromised Authentication*. Simulation results demonstrated that our PKI requires less seconds to converge than other compared public key infrastructures. Further, we observed a high percentage of group certificate reachability or user authentication even in the presence of high percentage of DoS attacks. In relation to Sybil attacks, even in the presence of high percentage of

fake nodes in the PKI, we still observed a high percentage of groups or authentication that was not compromised by fake nodes. In relation to the best number of members for an initiator group, in general, the best results were produced when initiator groups own 4 or 5 members.

Chapter 6

Directions for Survivable Link-layer Connectivity

This chapter provides research directions for reaching survivability in link-layer connectivity. Albeit wireless link-layer connectivity to be provided by different communication technologies [31, 37, 57], we take as reference the cognitive radio (CR) technology since it naturally supports one of the survivability properties – adaptation. This technology has been envisioned to provide high bandwidth for mobile users through dynamic spectrum access techniques and optimum use of the radio frequency spectrum [6, 7, 30, 96]. Cognitive radio concepts propose the opportunistic access of the spectrum and the capability of sharing wireless channels with licensed user holders (also known as primary users). We outline survivability directions considering the unlicensed user perspective. These users, also called secondary or cognitive radio user, can adaptively exploit idle spectrum bands without obstructing primary user operations.

Security has received few attention on wireless link-layer connectivity, particularly, in cognitive radio technology. Companies, governmental agencies and researchers have focused on the development of radio frequency spectrum management functionalities without handling security issues [6]. Protocols, architectures and standards have been created, but only few of them consider the employment of security mechanisms. Moreover, proposals applying security techniques restrict themselves to use conventional ones, such as cryptography, intrusion detection system and authentication. IEEE 802.22 standard [98], for example, provides a

security sub-layer designed in order to provide confidentiality, authentication and data integrity by cryptographic transformations in MAC data units.

However, conventional security mechanisms are not enough to prevent wireless link-layer connectivity against attacks and intrusions [19]. Preventive security mechanisms, as cryptography, provide confidentiality, integrity and authentication, but in general they are inefficient against overload, interception or manipulation attacks, such as DoS and jamming. Reactive security mechanisms, as intrusion detection systems (IDS), are based on network behavior analysis, or previous known attack and intrusion actions. Since new communication technologies are more dynamic and adaptive, attacks are forced to be more intelligent bypassing easily these security mechanisms [19, 120].

Based on the SAMNAR architecture, we provide directions of a framework for survivable link-layer using the cognitive radio technology. The framework follows a cross-layer approach in order to analyze the network situation and takes adequate decisions for security parameters. The framework intends to offer self-reconfiguration of the security mechanisms, such as their parameter values, cryptography key length, cryptography algorithm, rules and policies.

This chapter is organized in three sections as follows. Section 6.1 provides an overview of cognitive radio communication. Section 6.2 presents directions for a framework aiming to provide survivability on wireless link-layer connectivity. Finally, Section 6.3 concludes the chapter.

6.1 Cognitive Communication Overview

The most used medium for wireless communications is the spectrum of radio frequency (RF). RF lies in a frequency or rate of oscillation within the range of about 3 Hz to 300 GHz. This range, also called radio spectrum, defines allowable or usable channels of frequency for specific radio transmission technologies. Radio spectrum is typically Government regulated, and in some cases sold or licensed to operators of private radio transmission systems, such as cellular telephone operators or broadcast television stations.

Radio spectrum is physically limited by the static assignment policy. Governmental agencies assign subsets of the radio spectrum to license holders on

a long-term basis for large geographical regions. Each license holder uses their frequency bands for communication. However, even if license holders do not use their bands, no other user can transmit on them, resulting in idle bands. Recently, due to the popularization of wireless communication, the demand for band has increased resulting in the spectrum scarcity of specific bands of frequencies. In contrast, a large portion of the assigned spectrum is used sporadically, leading to no use of a significant amount of spectrum.

Researchers have developed dynamic spectrum access (DSA) techniques to solve issues related to the inefficient use of the spectrum. One of the exiting proposals is the Next Generation (xG) program from the Defense Advanced Research Projects Agency (DARPA). Its goal consists in accessing dynamically the spectrum of frequency by means of cognitive radio technology. CR is a radio that can change its transmitter parameters, such as power transmission, modulation code and frequency, based on interaction with the environment in which it operates. Hence, the main characteristics of CR are (1) the capability of interacting with its environment in real-time and identifying portions of the spectrum that are unused at a specific time or location; (2) the reconfiguration of transmitter parameters in order to transmit or receive on a variety of frequencies. These characteristics allow that in real time the best spectrum available can be selected, shared with other CR users, and exploited without interference with the licensed user.

Based on these characteristics, Akyildiz et. al identified a set of spectrum management functions. These functions design and guide how those characteristics are reached considering the challenges imposed by the coexistence of primary and secondary users using the spectrum and diverse Quality-of-Service (QoS) requirements. In a nutshell, the spectrum management consist of four main functions [6]:

- **Spectrum sensing:** Since a CR user allocates only unused portions of the spectrum, it must monitor spectrum bands, capture their information and detect those unused portions. Spectrum sensing is responsible for these tasks.

- **Spectrum decision:** Based on the spectrum availability, CR users allocate a channel. This allocation depends on spectrum availability, QoS requirements, and internal (and possibly external) policies.
- **Spectrum sharing:** Because there may be multiple CR users trying to access the spectrum, CR network access must be coordinated to prevent multiple users colliding in overlapping portions of the spectrum.
- **Spectrum mobility:** CR users are regarded as visitors to the spectrum. Hence, if the specific portion of the spectrum in use is required by a primary user, the communication must be continued in another vacant portion of the spectrum.

Figure 6.1 presents a framework for spectrum management proposed by Akyildiz et. al [6]. This framework correlates spectrum management functions with protocol stack layers, employing a cross layer design approach. Based on this framework, we present in Section 6.2 directions for a survivable link-layer connectivity framework.

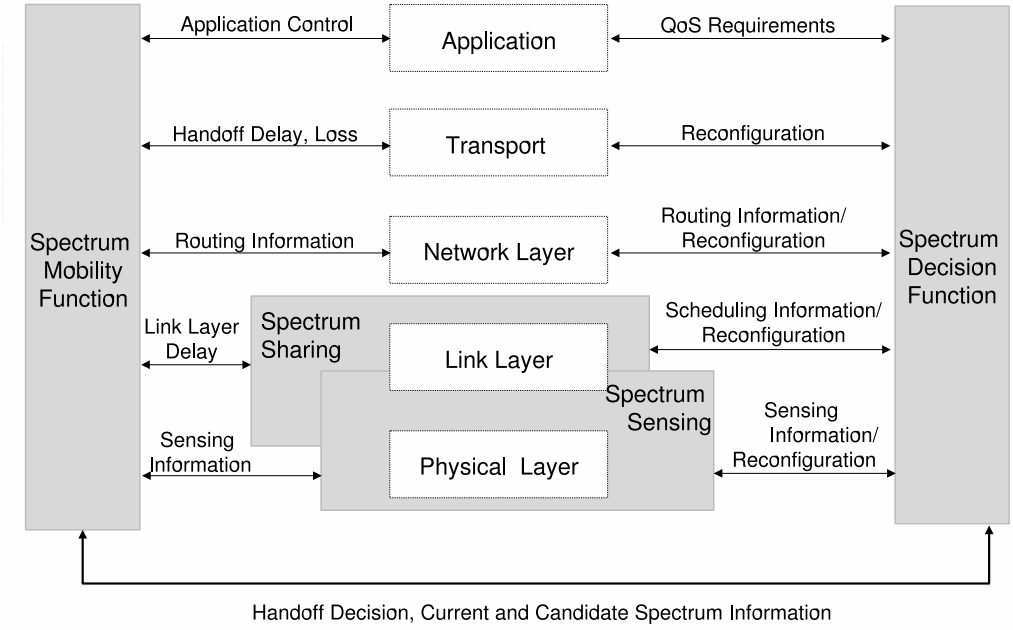


Figure 6.1: Spectrum management framework for CR

6.2 Directions for a Survivable Framework

Considering that link-layer connectivity is envisaged to be more and more adaptive, we present some directions of a survivable framework. Based on SAMNAR architecture and on the spectrum management functions of cognitive radio, our framework is illustrated in Figure 6.2. We took as reference the spectrum management framework for cognitive radio proposed by Akyildiz et. al [7] and we added security aspects towards a survivable link-layer connectivity.

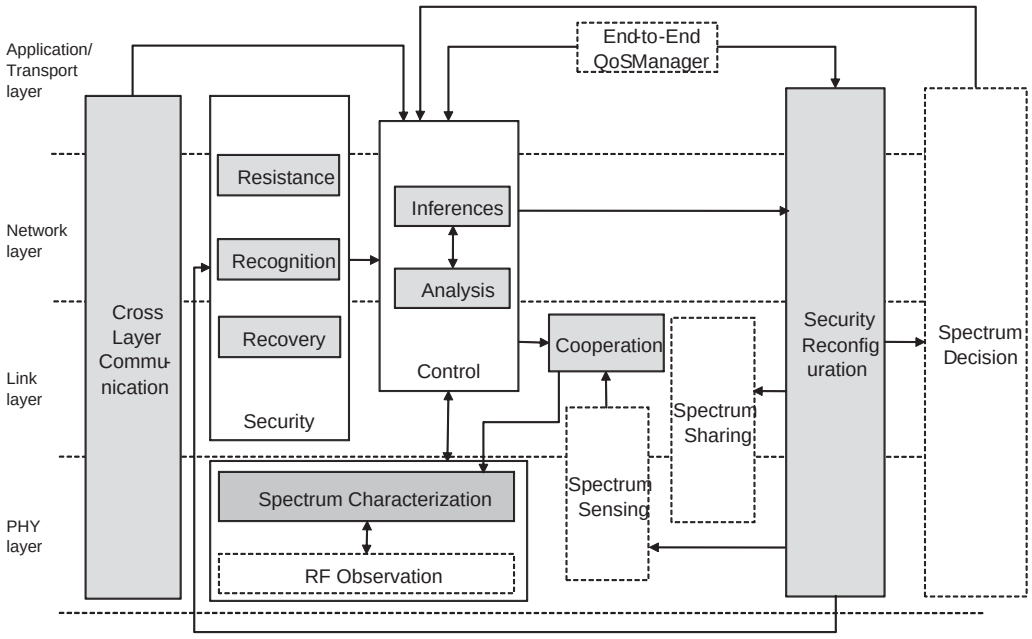


Figure 6.2: Framework for survivable link-layer connectivity

Our survivable framework follows also a cross-layer design. Despite of aiming to improve survivability in link-layer, information to support decisions are offered by different layers of the protocol stack. This characteristic is expected in the SAMNAR architecture, and in this framework the exchange of information among layers is provided by the cross-layer communication module. This module consists of techniques to store and collect information from different layers. Information is in general related to network environment and, particularly, it can be QoS requirements, handoff-delay, packet loss, routing information, link layer delay and others. The cross-layer communication module can also provide mechanisms to

preprocess the information, and then it sends information to the control module. The cross-layer module possesses functionalities defined on the collect module and on the inter-layer communication component of the communication module designed on the SAMNAR architecture.

A cooperation module is defined on the framework. This module owns all the functionalities defined on the inter-node communication component of the SAMNAR architecture. It is composed of techniques to provide the communication among the nodes. Further, as input it has information on the availability of spectrum bands identified by the techniques from the spectrum sensing module. The cooperation among the nodes provides input for the spectrum characterization indentifying the behavior of the spectrum, as well as the CR user or primary user activities.

The control module is the core of this framework. It is responsible for analyzing the information received from the other modules, making inferences and taking decisions about the adaptation necessary. The control module results in inputs for the security reconfiguration module, that defines the best security mechanisms to be used in the resistance, recovery and recognition modules based on the received analyses. Security reconfigurations are also influenced by the QoS requirements asked for applications.

6.3 Conclusions

This chapter presented general directions for a survivable framework for link-layer level. The framework is supported by the cognitive radio technology due to its characteristic of adaptation. Further, it extends the spectrum management framework proposed by Akyildiz et. al in order to include the SAMNAR architecture. The spectrum management is composed of main functions, spectrum sensing, spectrum decision, spectrum sharing and spectrum mobility. The main idea of our framework is to provide security in each function considering the approach proposed by SAMNAR architecture.

Hence, our framework is composed of different modules, being the security, control and reconfiguration the main modules. Security module owns security

mechanisms provided by the three defense lines, prevention, reaction and tolerance. Control module makes inferences base on information offered by modules other modules. In a nutshell, this information is related to network conditions, Quality-of-Service requirements, spectrum conditions, and security information related to the node and its neighbors. Based on inferences and decisions taken by the control module, the security reconfiguration module is responsible for reconfiguring the other modules in relation to security. This means to adapt security mechanisms used by other modules or even replacing a security mechanism by another depending on the inferences reached by the control module.

6. DIRECTIONS FOR SURVIVABLE LINK-LAYER CONNECTIVITY

Chapter 7

Conclusions

This chapter summarizes the thesis conclusions and future directions. The objective is to reinforce the contributions we have achieved and point out some directions we envision for proceeding with the research. Hence, we first highlight the main contributions of the thesis in Section 7.1. Then, we present in Section 7.2 its limitations and future directions for research on survivable wireless security management. Finally, in Section 7.3, we emphasize the list of publications resulted from this thesis.

7.1 Main Contributions

This thesis motivates a new approach for security management in self-organizing wireless networks. The main goal consisted in providing survivability of the network, meaning to offer essential services even in the presence of attacks or intrusions. Our approach is inspired on the human body immune system, and it lies in the adaptive management of different security mechanisms. Particularly, security mechanisms from preventive, reactive and tolerant defense lines are coordinated and adapted to network conditions, aiming to maintain link-layer connectivity, routing or end-to-end communication even in face to attacks or intrusions.

Based on the bio-inspired approach, the main contribution of this thesis is a general architecture, called SAMNAR. It assists in the design of survivable self-organizing wireless networks, being composed of three main modules: survival, communication and collect. These modules are integrated in order to achieve the

survivability goals. The survival module is the core of the SAMNAR architecture composed of five components: resistance, recognition, recovery, adaptation and control. Resistance holds preventive security mechanisms, such as cryptographic algorithms, firewall and access control. Recognition owns reactive security mechanisms, such as intrusion detection systems and reputation systems. Recovery is composed of tolerant techniques, such as redundancy or data recovery. Adaptation is responsible for the reconfiguration of the previously mentioned components. It is supported by analyses, inferences and decisions taken by the control component.

We enhanced the use of SAMNAR architecture in two study cases. As first one, we developed a survival path selection scheme in order to improve the survivability on routing. The scheme employs fuzzy logic technique as control module for making inferences and taking decisions about the most survival path. Different criteria are used to evaluate paths, such as cryptography key length, expiration time of digital certificates, node reputation, node degree, remaining energy of nodes and path length. These criteria are correlated considering their impact on survivability. Simulations have been used to evaluate survivability improvements achieved by the path selection proposed. In different scenarios, results have presented a reduction in the impact of different attacks, and maintaining routing performance in terms of packet correctly delivered and end-to-end latency, similar from that produced by routing without the survivable scheme.

As second study case, we proposed a survivable public key infrastructure. Following the SAMNAR architecture guidelines, the proposed PKI is fully decentralized and supported by the creation of groups. These groups are formed by nodes and guided by the social relationship existing among users owning those nodes. Each group generates in a decentralized way a pair of cryptographic key for the group. The survivable PKI correlates different kind of evidences in order to prove the liability of users for their public keys. These evidences must be provided by at least three different type of security mechanisms. Public key certificates are validated by chains of group certificates, being the validation process assisted by resistance, recognition and recovery levels. Simulations have been performed to evaluate the survivability of our survivable PKI under different attacks. Results demonstrated its survivability achieving in few minutes the

maximum convergence of all certificates on the system, and presenting a high percentages of non-compromised groups or authentication under high percentage of malicious nodes.

Finally, as last contribution of this thesis, we provide directions for a framework aiming to improve the survivability in link-layer connectivity. We consider the use of cognitive radio technology as support for link-layer connectivity because it owns naturally the adaptation property required in survivability. Our framework extends the spectrum management framework proposed by Akildyz et. al. That framework consists in several functions, and each function must be protected by a coordinated association among different kind of security mechanisms.

7.2 Limitations and Outlook

Some limitations can be identified in the current state of the research, and such limitations lead to future work. First, SAMNAR is a conceptual and generic architecture assigning guidelines for reaching a survivable self-organizing wireless networks. Since, the main goal of a research is always to develop solutions as practical as possible, SAMNAR must be exploited towards the definition of a framework, its functions, and implementation of an API (Application Program Interface) in order to allow its practical use. Further, the framework must consider differences in case studies and must be flexible allowing the addition of new functions when necessary.

Another limitation is related to metrics for survivability evaluation. Actually, how to measure survivability is a topic that produces many discussions in this field. Hence, the definition of metrics specifically with this proposal is a request. We have included in this work some new metrics with this proposal, however in our point of view, it is not enough. We envisage still a long path with discussions about this topic considering the self-organizing wireless networks characteristics.

This thesis also presents limitations in relation to the communication module of the SAMNAR architecture. We did not deal with communication issues related to the diffusion of information, for example. Due to the decentralized characteristic of self-organizing wireless networks, we believe that solutions must

be proposed in order to minimize the impact on performance and improve their efficiency. Further, solutions considering survivability requirements and goals must be proposed, particularly, the network situation must be addressed. Creating a strategy of communication to adapt or change the used techniques with the network situation is a good direction of research. The development of adaptive solutions, algorithms and protocols considering survivability aspects is expect to support network survivability.

7.3 Publications

This section presents the list of publications resulted from this thesis.

- *A Survey of Survivability in Mobile Ad Hoc Networks.* Michele N. Lima, Aldri L. Santos, Guy Pujolle. **IEEE Communications Surveys and Tutorials**, 2009.

- *Analyzing the Effectiveness of Self-Organized Public Key Management on MANETs under Lack of Cooperation and Impersonation attacks.* Eduardo da Silva, Michele N. Lima, Aldri L. dos Santos, Luiz C. P. Albini. Book Chapter. Published by Springer in the book **E-Business and Telecommunication Networks**, 2009.

- *Survivable Keying for Wireless Ad Hoc Networks.* Michele N. Lima, Eduardo Silva, Luiz C. P. Albini, Aldri L. dos Santos, Guy Pujolle. In 11th **IFIP/IEEE International Symposium on Integrated Network Management (IM 2009)** - Mini-Conference, New York, June, 2009.

- *An Architecture for Survivable Mesh Networking.* Michele N. Lima, Helber W. da Silva, Aldri L. dos Santos, Guy Pujolle. In **IEEE Globecom 2008 Ad Hoc, Sensor and Mesh Networking Symposium (GC'08 AHSN)**, New Orleans, USA.

- *Identity-Based Key Management in Mobile Ad Hoc Networks: Techniques and Applications.* Eduardo da Silva, Michele N. Lima, Aldri L. dos Santos, Luiz C. P.Albini. Special issue on 'Dependability Issues with Ubiquitous

Wireless Access' - **IEEE Wireless Communications Magazine**, October 2008.

- *Quantifying Misbehaviour Attacks Against the Self-Organized Public Key Management on MANETs.* Eduardo da Silva, Michele N. Lima, Aldri L. dos Santos, Luiz C. P. Albini. **International Conference on Security and Cryptography (SECRYPT)** 2008, Porto, Portugal, pp. 128-135, July 2008. (Selected as best paper for publication of extension version)

- *Requirements for survivable routing in MANETs.* Michele N. Lima, Helber W. da Silva, Aldri L. dos Santos, Guy Pujolle. **IEEE International Symposium on Wireless Pervasive Computing (ISWPC)**, Santorini, Greece, pp. 441-445, Maio 2008.

- *Virtual Structure Effects in Two Hybrid Routing Protocols for Ad Hoc Networks.* Luiz C. P. Albini, A. Brawerman, Michele N. Lima, S. Chessa, P. Maestrini. **IEEE International Symposium on Wireless Pervasive Computing (ISWPC)**, Santorini, Greece, pp. 425-432, Maio 2008.

- *Survival multipath routing for MANETs.* Michele N. Lima, Guy Pujolle, Helber W. da Silva, Aldri L. dos Santos. In **IEEE/IFIP Network Operations and Management Symposium (NOMS)**, pp. 425-432, 2008.

- *The Impact of Byzantine Attacks on Survivability of MANET Routing Protocols.* Michele N. Lima, Helber W. da Silva, Zeinab Movahedi, Aldri L. dos Santos. **Networking and Eletronic Commerce Research Conference (NAEC)**, Riva del Garda, Italy, October 2007.

- *A Survey of Survivability in Mobile Ad Hoc Networks.* Michele N. Lima, Aldri L. Santos, G. Pujolle. **Technical Report - LIP6 2007/001**, UPMC, Paris, France, 2007.

The following manuscripts are in preparation for submission or are under review.

- *Routing Survivability in Wireless Ad Hoc Networks.* Michele N. Lima, Helber W. Silva, Aldri L. Santos, Guy Pujolle. To be submitted for **IEEE Transactions on Network and Service Management (TNSM)**.
- *Survivable Public-Key Management for Self-Organized Wireless Ad Hoc Networks.* Eduardo da Silva, Michele N. Lima, Aldri L. dos Santos, Luiz C. P. Albini. Manuscript in preparation to be submitted for a journal.
- *Biologically Inspired Survivable Architecture for Self-Organized Wireless Networks.* Michele N. Lima, Aldri L. dos Santos, Guy Pujolle. Manuscript in preparation to be submitted for a magazine, 2009.

Appendix A

Survivable Initiatives on Routing

This appendix describes some initiatives on building survivable routing self-organizing wireless networks. Despite they do not present a proposal with all survivability properties, their characteristics are more correlated to survivability goals than just preventive or reactive defense lines. We focus on propositions that aggregate more than one defense line and apply at least one technique of tolerance, such as redundancy.

We categorize the initiatives found in the literature in two main groups: *route discovery* and *data forwarding*. The former lies in approaches trying to make the route discovery phase of routing protocols more resistant and tolerant to attacks and intrusion. The latter is composed of initiatives specialized on data forwarding using preventive or reactive security mechanisms and one technique of tolerance.

A.1 Route Discovery

Routing is essential for the operation of self-organizing wireless networks. Many routing protocols have been proposed in the literature including proactive (table-driven), reactive (demand-driven) and hybrid solutions. Most of them have assumed these networks as a trust environment in which nodes can trust and cooperate with themselves. However, these networks are vulnerable to attacks and intrusions as discussed in this thesis.

Due to vulnerabilities on routing service, secure routing protocols have been proposed [15, 40, 41], such as SRP (secure routing protocol) [72], SAODV (Secure

Ad hoc On-Demand Distance Vector) [118], SAR (security aware routing) [115]. These protocols are mostly based on authentication and encryption algorithms, being inefficient to put all intruders and attacks off. Therefore, some research groups have built intrusion tolerant routing approaches, such as TIARA (Techniques for Intrusion-resistant Ad Hoc Routing Algorithms) [81], BFTR (Best-Effort Fault Tolerant Routing) [112], ODSBR (An On-Demand Secure Byzantine Routing Protocol) [10] and BA (Boudriga's Approach) [16].

TIARA defines a set of design techniques to mitigate the impact of Denial of Service (DoS) attacks and can be applied on routing protocols to allow the acceptable network operation in the presence of these attacks. The main techniques established by TIARA are: *flow-based route access control (FLAC)*, *distributed wireless firewall*, *multipath routing*, *flow monitoring*, *source-initiated flow routing*, *fast authentication*, *the use of sequence numbers* and *referral-based resource allocation*. For its effective implementation, TIARA should be adapted to a routing protocol, being incorporated more easily into on-demand protocols, such as DSR and AODV.

In the FLAC technique, a distributed wireless firewall and a limited resource allocation are applied together to control packet flows and to prevent attacks based on resource overload. Each node participating in the ad hoc network contains an access control list, where authorized flows are defined. A threshold is defined for allocating limited amount of network resources for a given flow. Many routes are discovered and maintained, but only one route is chosen to data forwarding. The flow monitoring technique checks the network failures sending periodic control messages, called *flow status packets*. If a path failure is identified, an alternative path found in the discovery phase will be selected. The authentication process in TIARA consists in placing the path label of the packet in a secret position. Each node can define a different position for the label within the packet being its authentication information.

Best-effort fault-tolerant routing (BFTR) is a source routing algorithm exploring path redundancies of ad hoc networks. Its goal is to maintain packet routing service with high delivery ratio and low overhead under misbehaving nodes. BFTR never attempts to conclude whether the path, or any node along it, is good or bad. It considers existing statistics to choose the most feasible path,

such as each one with the highest packet delivery ratio in the immediate past. By means of existing statistics and receiver's feedback, different types of attacks can be indistinctly detected, such as packet dropping, corruption, or misrouting.

BFTR is based on DSR flooding to retrieve a set of paths between source and destination nodes, whenever necessary, and it chooses initially the shortest path to send packets. If a route failure is reported, the protocol will discard the current routing path and proceed with the next shortest path in the route cache. The algorithm considers that the behavior of any good node is to delivery packets correctly with high delivery ratio. Hence, a good path consists of nodes with high delivery ratio. Any path with low delivery ratio is thus discarded and replaced by the next shortest path. BFTR requires no security support from intermediate nodes. The source and destination nodes of connections are assumed well-behaved. A previous trust relationship between end nodes is required, being possible the authentication between them during data communication.

ODSBR is a routing protocol providing a correct routing service even in the presence of Byzantine attacks [39]. ODSBR operates using three sequential phases: (i) least weight route discovery, (ii) Byzantine fault localization and (iii) link weight management. The first phase is based on double secure flooding and aims to find lowest cost paths. Double flooding means that route discovery protocol floods with route request and response messages in order to ensure path setting up. In this phase, cryptography operations guarantee secure authentication and digital signature. The second phase discovers faulty links on the paths by means of an adaptive probing technique. This technique uses periodic secure acknowledgments from intermediate nodes along the route and the integrity of the packets is assured by cryptography. The last phase of ODSBR protocol manages the weight assigned to a faulty link. Each faulty link has a weight to identify bad links, being this information stored at a weight list and used by the first phase of the protocol.

Results have shown the good performance of ODSBR in many scenarios for different metrics. However, some important points are not evaluated or well defined. For example, ODSBR assumes the use of RSA cryptography and digital signatures without considering open issues as public key distribution, node pair key initialization or the iteration among nodes to guarantee authenticity. These

operations are essential for the good ODSBR functionality influencing results. Moreover, it is based also on acknowledgments that could not be assured due to mobility and dynamic topology.

Boudriga *et. al* [16] propose a new approach for building intrusion tolerant MANETs. It consists of a multi-level trust model and a network layer mechanism for resource allocation and recovery. The multi-level trust model assumes that the network is divided into two virtual sets: the resource's domain and the user's domain. Each resource assigns a unique trust level for each type of activity that it is involved with and each location where it appears. Based on this trust level and on the activity, users or applications allocate resources by a distributed scheme. It allocates available resources attempting to maximize the usage and minimize costs. For each application, only a fraction of a resource is allocated at a given node.

Intrusion tolerance is reached through a distributed firewall mechanism, a technique for detecting and recovering intruder-induced path failures, a trust relation between all nodes, an IPsec-based packet authentication, and a wireless router module that enable survivability mechanisms to DoS attacks. The distributed firewall aims to protect the MANET against flooding attacks and each node maintains a firewall table containing the list of all packets passing through it and successfully accepted by their destination. After a handshake between the sender and the receiver of a related flow, the entries in a firewall table will be maintained automatically and refreshed when failures, intrusion occurrences or other abnormal behavior are detected. Based on those entries, the node can forbid any flood of spurious traffic. Three parameters are managed by the nodes to detect anomalies as packet loss rate, duplicate packet rate and authentication failure rate.

A.2 Data Forwarding

Some works have proposed secure routing mechanisms to defend against more than attack [51, 47, 48, 27]. Despite of those protocols ensure the correctness of the route discovery, they cannot guarantee secure and undisrupted delivery of data. Intelligent attackers can easily gain unauthorized access to the network,

follow the rules of the route discovery, place themselves on a route, and later redirect, drop or modify traffics, or inject data packets. In a nutshell, an adversary can hide its malicious behavior for a period of time and then attack unexpectedly, complicating its detection. For these reasons, mechanisms to provide data confidentiality, data availability and data integrity are necessary for guaranteeing secure data forwarding.

Several mechanisms have been proposed for securing data forwarding. Lightweight cryptographic mechanisms as Message Authentication Code (MAC) [52], for example, are used to data integrity. Nuglets [20], Friends and Foes [69], Sprite [121] and others [114, 93] propose mechanisms to stimulate node participation in data forwarding, trying to guarantee data availability. CORE [68] and CONFIDANT [17] are examples of reputation systems that provide information to distinguish between a trustworthy node and a bad node. This information also encourages nodes to participate in the network in a trustworthy manner.

Some solutions to provide data confidentiality and data availability have attempted to apply techniques as redundancy and message protection to be more resilient to attacks. In SPREAD [60], SMT [73] and SDMP [23], for example, the message is divided into multiple pieces by a *message division algorithm*. These pieces are simultaneously sent from the source to the destination over multiple paths. In [13], a cross-layer approach is investigated to improve data confidentiality and data availability, using directional antennas and intelligent multipath routing with data redundancy.

The Secure Protocol for Reliable Data Delivery (SPREAD) scheme proposes the use of some techniques to enhance data confidentiality and data availability. Initially, messages are split into multiple pieces by the source node, using the threshold secret sharing scheme [90]. Each piece is encrypted and sent out via multiple independent paths. Encryption between neighboring nodes with a different key is assumed, as well as the existence of an efficient key management scheme. SPREAD focuses on three main operations: to divide the message, to select multiple paths and to allocate message pieces into paths.

Messages are split by the threshold secret sharing algorithm and each piece is allocated into a selected path aiming to minimize the probability of harm. SPREAD selects multiple independent paths taking into account security factors,

such as the probability of one path being compromised. The goal of SPREAD is to achieve an optimal share allocation way, where the attacker should damage all the paths to recover the message.

The goal of the secure message transmission (SMT) protocol is to ensure data confidentiality, data integrity, and data availability, safeguarding the end-to-end transmission against malicious behavior of intermediary nodes. SMT exploits four main characteristics: end-to-end secure and secure feedback mechanism, dispersion of the transmitted data, simultaneous usage of multiple paths, and adaptation to the network changing conditions. It requires a security association (SA) [64] between the two end communicating nodes, so no link encryption is needed. This trust relationship is indispensable for providing data integrity and authentication of end nodes, necessary for any secure communication scheme. The two end nodes make use of a set of node-disjoint paths, called Active Path Set (APS), being a subset of all existing paths between them.

Data message is broken into several small pieces by the information dispersal scheme [80]. Data redundancy is added to allow recovery, being also divided into pieces. All pieces are sent through different routes existent in APS, enhancing statistically the confidentiality and availability of exchanged messages. At the destination, the dispersed message is successfully reconstructed only if a sufficient number of pieces are received. Each piece carries a Message Authentication Code (MAC), allowing its integrity verification by the destination. The destination validates the incoming pieces and acknowledges the successfully received ones thought a feedback to the source. The feedback mechanism is also protected by cryptography and is dispersed to provide fault tolerance. Each path of APS has a reliability rate calculated by the number of successful and unsuccessful transmissions on this path. SMT uses this rate to manage the paths in APS, trying to determine and maintain a maximally secure path-set, and adjusting its parameters to remain effective and efficient.

The Secured Data based MultiPath (SDMP) protocol exploits also multiple paths between network nodes to increase the robustness and data confidentiality. The protocol assumes Wired Equivalent Privacy (WEP) link encryption/decryption of all the frames between neighboring nodes, which provide link layer confidentiality and authentication. SDMP can work with any routing protocol

which provides topology discovery and supports the use of multipath for routing. SDMP distinguishes between two types of path: signaling and data. Signaling type requires only one path of the path-set existent between source and destination nodes, being the other paths available for data transmission.

The protocol divides the message into pieces using the Diversity Coding approach [12]. Each piece has a unique identifier and all of them are combined in pairs through an XOR operation related to a random integer number. Each pair is sent along a different path. All information necessary for message reconstruction at the destination is sent by the signaling path. Unless the attacker can gain access to all of the transmitted parts, the probability of message reconstruction is low. That is, to compromise the confidentiality of the original message, the attacker must get within eavesdropping range of the source/destination, or simultaneously listen to the used paths and decrypt the WEP encryption of each transmitted part. However, it is possible to deduce parts of the original message from only a few of the transmitted pieces, especially since one piece of the original message is always sent in its original form on one of the paths.

In contrast to previous solutions, a cross-layer approach is investigated in [13]. The solution uses directional antennas and intelligent multipath routing to enhance end-to-end data confidentiality and data availability. Unlike an omnidirectional antenna that transmits or receives radio waves uniformly in all directions, a directional antenna transmits or receives radio waves in one particular direction. Directional antennas make eavesdropping more difficult and reduce the areas covered by packet transmissions, minimizing the overlap of message pieces sent by multiple paths. Thus, the use of directional antennas is justified by the reduction on the likelihood that an adversary is able to simultaneously gather all of the message pieces at the source or destination nodes.

A self-adaptive transmission power control mechanism is used together with directional antennas to reduce the message interception probability. This mechanism allows the transmitter to employ only enough transmission power in order to reach the intended receiver, minimizing the radiation pattern for a given radio transmission and the possibility of an attacker to intercept the message transmission. Dynamically the transmission power is adjusted depending of the data packet type exchanged between neighboring nodes. Multipath routing is also

used. Thus, messages are divided based on threshold secret sharing algorithm, and then the shares are sent by multiple node-disjoint paths. Two intelligent routing schemes are proposed to reduce message interception probability. The former minimizes the physical distance of hops and the latter minimizes the path-set correlation factor.

Appendix B

Fuzzy Rules

This appendix presents the Fuzzy rules applied in the case study of the Chapter 4.

Fuzzy Rules
if R is *bad* **then** PSL is *low*.
if E is *low* **then** PSL is *low*.
if T is *imminent* **then** PSL is *low*.
if K is *short* **then** PSL is *low*.
if (L is *long*) and (K is *large*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *medium*) and (D is few) and (K is *large*) and (E is *medium*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *medium*) and (D is few) and (K is *large*) and (E is *high*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *small*) and (D is few) and (K is *large*) and (E is *medium*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *small*) and (D is few) and (K is *large*) and (E is *high*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *medium*) and (D is *normal*) and (K is *large*) and (E is *medium*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *medium*) and (D is *normal*) and (K is *large*) and (E is *high*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *small*) and (D is *normal*) and (K is *large*) and (E is *medium*) and (R is *good*) and (T is far) **then** PSL is *medium*.
if (L is *small*) and (D is *normal*) and (K is *large*) and (E is *high*) and (R is *good*) and (T is far) **then** PSL is *high*.
if (L is *medium*) and (D is *many*) and (K is *large*) and (E is *medium*) and (R is *good*) and (T is far) **then** PSL is *high*.
if (L is *medium*) and (D is *many*) and (K is *large*) and (E is *high*) and (R is *good*) and (T is far) **then** PSL is *high*.
if (L is *small*) and (D is *many*) and (K is *large*) and (E is *medium*) and (R is *good*) and (T is far) **then** PSL is *high*.
if (L is *small*) and (D is *many*) and (K is *large*) and (E is *high*) and (R is *good*) and (T is far) **then** PSL is *high*.

Table B.1: Fuzzy rules

In Table B.1, each symbol means:

- **R** is the smallest reputation value among all reputations of nodes in a given path;
- **E** is the minimal remaining energy rate existing among the nodes of a given path;
- **T** is the most imminent expiration time among all certificates existing in a given path;
- **D** is the minimal node degree among all nodes participating in a given path;
- **K** is the minimal cryptographic key length among all keys used by nodes in a given path;
- **L** is the path length measured by the number of hops from the source node to the destination;
- **PSL** is the output of the Fuzzy inference phase meaning path survivability level;

Values related to the linguistic fuzzy variables *low*, *medium*, *high*, *good*, *bad*, *imminent*, *far*, *small*, *normal*, *large*, *few*, *many* follow the description of Chapter 4.

Bibliography

[1] Malicious- and accidental-fault tolerance for internet applications (MAFTIA), 2006. Access: August 2006.

[2] Organically assured and survivable information system (OASIS), 2006. Access: August 2006.

[3] Keyanalyze - analysis of a large OpenPGP ring, 2008. Access: August 2008.

[4] I. Aad, J.-P. Hubaux, and E. W. Knightly. Denial of service resilience in ad hoc networks. In *Proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 202–215, New York, NY, USA, 2004. ACM Press.

[5] I. Akyildiz and X. Wang. A survey on wireless mesh networks. *IEEE Communications Magazine*, 43(9):23–30, 2005.

[6] I. Akyildiz, L. Won-Yeol, M. Vuran, and S. Mohanty. A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, 46(4):40–48, April 2008.

[7] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer Network*, 50(13):2127–2159, 2006.

[8] T. Aura and S. Mäki. Towards a survivable security architecture for adhoc networks. In *Proceedings of the International Workshop on Security Protocols*, pages 63–73, London, UK, 2002. Springer-Verlag.

[9] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. Mitigating byzantine attacks in ad hoc wireless networks. Technical report, Center for Networking and Distributed Systems, Computer Science Department, Johns Hopkins University, 2004.

[10] B. Awerbuch, R. Curtmola, D. Holmer, H. Rubens, and C. Nita-Rotaru. On the survivability of routing protocols in ad hoc wireless networks. In *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 327–338, Washington, DC, USA, 2005. IEEE Computer Society.

[11] B. Awerbuch, D. Holmer, H. Rubens, and R. D. Kleinberg. Provably competitive adaptive routing. In *Proceedings of IEEE INFOCOM*, pages 631–641, 2005.

[12] E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self-healing and fault-tolerant communication networks. *IEEE Transactions on Communications*, 41(11):1677–1686, november 1993.

[13] V. Berman and B. Mukherjee. Data security in MANETs using multipath routing and directional transmission. In *Proceedings of the IEEE International Conference on Communications (ICC)*, volume 5, pages 2322–2328. IEEE Computer Society, 2006.

[14] A. N. Bessani, P. Sousa, M. Correia, N. F. Neves, and P. Verissimo. The CRUTIAL way of critical infrastructure protection. *IEEE Security & Privacy*, 6(6), 2008.

[15] R. B. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh. Bootstrapping security associations for routing in mobile ad-hoc networks. In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, volume 3, pages 1511–1515, 2003.

[16] N. A. Boudriga and M. S. Obaidat. Fault and intrusion tolerance in wireless ad hoc networks. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, volume 4, pages 2281–2286. IEEE Computer Society, 2005.

[17] S. Buchegger and J.-Y. L. Boudec. Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Lausanne, CH, June 2002. IEEE.

[18] S. Buchegger, J. Mundinger, and J.-Y. L. Boudec. Reputation systems for self-organized networks. *IEEE Technology and Society Magazine*, 27(1):41–47, 2008.

[19] J. Burbank. Security in cognitive radio networks: The required evolution in approaches to wireless network security. In *Proceedings of the International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pages 1–7, May 2008.

[20] L. Buttyán and J.-P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Network Application*, 8(5):579–592, 2003.

[21] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 2(1):52–64, 2003.

[22] M. Chorzempa, J.-M. Park, and M. Eltoweissy. Key management for long-lived sensor networks in hostile environments. *Computer Communication*, 30(9):1964–1979, 2007.

[23] R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya. On designing MAC protocols for wireless networks using directional antennas. *IEEE Transactions on Mobile Computing*, 5(5):477–491, 2006.

[24] L. F. Costa, F. A. Rodrigues, G. Travieso, and P. R. V. Boas. Characterization of complex networks: A survey of measurements. *Advances In Physics*, 56:167–242, 2007.

[25] Y. Deswarte and D. Powell. Internet security: an intrusion-tolerance approach. *Proceedings of the IEEE*, 94(2):432–441, 2006.

[26] S. Dhurandher and G. Singh. Weight based adaptive clustering in wireless ad hoc networks. In *IEEE International Conference on Personal Wireless Communications*, pages 95–100, January 2005.

[27] D. Djenouri and N. Badache. Struggling against selfishness and black hole attacks in MANETs. *Wireless Communications and Mobile Computing*, 2007.

[28] D. Djenouri, L. Khelladi, and A. N. Badache. A survey of security issues in mobile ad hoc and sensor networks. *Communications Surveys & Tutorials, IEEE*, 7(4):2–28, 2005.

[29] R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead. Survivable network systems: an emerging discipline – CMU/SEI-97-TR-013. Technical report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1997.

[30] F. C. C. R. ET Docket No. 03-108. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies, 2003.

[31] K. Etemad. Overview of mobile wimax technology and evolution. *Communications Magazine, IEEE*, 46(10):31–40, 2008.

[32] L. Feeney, B. Ahlgren, and A. Westerlund. Spontaneous networking: an application oriented approach to ad hoc networking. *IEEE Communications Magazine*, 39(6):176–181, June 2001.

[33] J. Fraga and D. Powell. A fault- and intrusion-tolerant file system. In *Proceedings of the Third International Conference on Computer Security*, pages 203–218, 1985.

[34] A. K. Ghosh and J. M. Voas. Inoculating software for survivability. *Communications of the ACM*, 42(7):38–44, 1999.

[35] Y. Han, R. J. La, and H.Zhang. Path selection in mobile ad-hoc networks and distribution of path duration. In *Proceedings of IEEE INFOCOM*, pages 758–762, Washington, DC, USA, 2006. IEEE Computer Society.

[36] Y. Han, R. J. La, A. M. Makowski, and S. Lee. Distribution of path durations in mobile ad-hoc networks: Palm's theorem to the rescue. *Computer Networks*, 50(12):1887–1900, 2006.

[37] P. Henry and H. Luo. Wifi: what's next? *IEEE Communications Magazine*, 40(12):66–72, December 2002.

[38] L. Hoffman. In search of dependable design. *Communications of the ACM*, 51(7):14–16, 2008.

[39] D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: an on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. *ACM Transactions on Information Systems Security (TISSEC)*, 2007.

[40] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Journal Ad Hoc Networks*, 01:175–192, 2003.

[41] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1-2):21–38, 2005.

[42] E. Y. Hua and Z. J. Haas. Path selection algorithms in homogeneous mobile ad hoc networks. In *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 275–280, New York, NY, USA, 2006. ACM Press.

[43] Y. Huang and W. Lee. A cooperative intrusion detection system for ad hoc networks. In *First ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 135–147, New York, NY, USA, 2003. ACM Press.

[44] S. Jiang, D. He, and J. Rao. A prediction-based link availability estimation for routing metrics in MANETs. *IEEE/ACM transactions on networking*, 13(6):1302–1312, 2005.

[45] K. John, C. Dennis, H. Alexander, W. Antonio, C. Jonathan, H. Premkumar, and D. Michael. The willow architecture: comprehensive survivability for large-scale distributed applications. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks*, Washington, DC, USA, 2002. IEEE Computer Society.

[46] D. Johnson, D. Maltz, and J. Broch. *DSR - the dynamic source routing protocol for multihop wireless ad hoc networks*, chapter 5, pages 139–172. Addison-Wesley, 2001.

[47] M. Just, E. Kranakis, and T. Wan. Resisting malicious packet dropping in wireless ad hoc networks. In *Proceedings of the International Conference on AD-HOC Networks and Wireless (ADHOC-NOW)*, pages 151–163, 2003.

[48] F. Kargl, A. Klenk, S. Schlott, and M. Weber. Advanced detection of selfish or malicious nodes in ad hoc networks. In *Proceedings of the First European Workshop on Security in Ad Hoc and Sensor Networks (ESAS)*, volume 3313 of *Lecture Notes in Computer Science*, pages 152–165. Springer, 2004.

[49] M. Kefayati, H. R. Rabiee, S. G. Miremadi, and A. Khonsari. Misbehavior resilient multi-path data transmission in mobile ad-hoc networks. In *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, pages 91–100, New York, NY, USA, 2006. ACM.

[50] A. Keromytis, J. Parekh, P. N. Gross, G. Kaiser, V. Misra, J. Nieh, D. Rubenstein, and S. Stolfo. A holistic approach to service survivability. In *Proceedings of ACM Workshop on Survivable and Self-Regenerative Systems*, pages 11–22, New York, NY, USA, 2003. ACM.

[51] I. Khalil, S. Bagchi, and C. Nita-Rotaru. DICAS: detection, diagnosis and isolation of control attacks in sensor networks. In *Proceedings of International ICST Conference on Security and Privacy in Communication Networks (SECURECOMM)*, pages 89–100, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[52] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-hashing for message authentication. RFC 2104, Internet Engineering Task Force, February 1997.

[53] O. Kreidl and T. Frazier. Feedback control applied to survivability: a host-based autonomic defense system. *IEEE Transactions on Reliability*, 53(1):148–166, 2004.

[54] J.-C. Laprie, B. Randell, A. Avizienis, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transaction Dependable Security Computer*, 1(1):11–33, 2004.

[55] M. Latapy, C. Magnien, and N. D. Vecchio. Basic notions for the analysis of large two-mode networks. *Social Networks*, 30(1):31–48, 2008.

[56] S. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. In *Proceedings of the IEEE International Conference on Communications (ICC)*, pages 3201–3205, 2001.

[57] W. Lehr and L. W. McKnight. Wireless internet access: 3G vs. WiFi? *Telecommunications Policy*, 27(5-6):351–370, 2003.

[58] R. C. Linger, N. R. Mead, and H. F. Lipson. Requirements definition for survivable network systems. In *Proceedings of the Third International Conference on Requirements Engineering*, pages 1–14, Washington, DC, USA, 1998. IEEE Computer Society.

[59] H. Liu, J. Li, Y.-Q. Zhang, and Y. Pan. An adaptive genetic fuzzy multipath routing protocol for wireless ad hoc networks. In *Proceedings of the ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN)*, pages 468–475, Washington, DC, USA, 2005. IEEE Computer Society.

[60] W. Lou, W. Liu, and Y. Fang. SPREAD: enhancing data confidentiality in mobile ad hoc networks. In *Proceedings of IEEE INFOCOM*, volume 4, pages 2404–2413, Washington, DC, USA, 2004. IEEE Computer Society.

[61] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang. URSA: ubiquitous and robust access control for mobile ad hoc networks. *IEEE/ACM Transaction Network*, 12(6):1049–1063, 2004.

[62] M. Marina and S. Das. On-demand multipath distance vector routing in ad hoc networks. In *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, pages 14–23, 2001.

[63] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 255–265, New York, NY, USA, 2000. ACM Press.

[64] D. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet security association and key management protocol (ISAKMP). RFC 2408, Internet Engineering Task Force, November 1998.

[65] U. Maurer. Modelling a public-key infrastructure. In *European Symposium on Research in Computer Security (ESORICS)*, pages 325–350, London, UK, 1996. Springer-Verlag.

[66] D. Medhi and D. Tipper. Multi-layered network survivability – models, analysis, architecture, framework and implementation: an overview. In *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX)*, pages 173–186, Los Alamitos, California, 2000. IEEE computer society Press.

[67] J. V. Merwe, D. Dawoud, and S. McDonald. A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Computing Surveys*, 39(1):1–45, 2007.

[68] P. Michiardi and R. Molva. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *IFIP TC6/TC11*, pages 107–121, Deventer, The Netherlands, 2002. Kluwer, B.V.

[69] H. Miranda and L. Rodrigues. Friends and Foes: Preventing selfshness in open mobile ad hoc networks. In *Proceedings of the IEEE International Conference on Distributed Computing Systems Workshop (ICDCSW)*, page 440, Los Alamitos, CA, USA, 2003. IEEE Computer Society.

[70] E. Ngai and M. Lyu. Trust- and clustering-based authentication services in mobile ad hoc networks. In *International Conference on Distributed Computing Systems Workshop*, pages 582–587, March 2004.

[71] J. Nie, J. Wen, J. Luo, X. He, and Z. Zhou. An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks. *Fuzzy Sets and Systems*, 157(12):1704–1712, 2006.

[72] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In *SCS communication networks and distributed systems modeling and simulation conference CNDS*, 2002.

[73] P. Papadimitratos and Z. J. Haas. Secure data transmission in mobile ad hoc networks. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 41–50, New York, NY, USA, 2003. ACM Press.

[74] P. Papadimitratos, Z. J. Haas, and E. G. Sirer. Path set selection in mobile ad hoc networks. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 1–11, New York, NY, USA, 2002. ACM Press.

[75] T. P. Pedersen. A threshold cryptosystem without a trusted party. In *EUROCRYPT*, pages 522–526, 1991.

[76] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. Ad hoc on-demand distance vector (aodv) routing. RFC Experimental 3561, Internet Engineering Task Force, July 2003.

[77] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, Los Alamitos, CA, USA, 1999. IEEE Computer Society.

[78] A. Pras, J. Schonwalder, M. Burgess, O. Festor, G. Perez, R. Stadler, and B. Stiller. Key research challenges in network management. *IEEE Communications Magazine*, 45(10):104–110, October 2007.

[79] Y. Qian, K. Lu, and D. Tipper. A design for secure and survivable wireless sensor networks. *IEEE Wireless Communications*, 14(5):30–37, 2007.

[80] M. O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal ACM (JACM)*, 36(2):335–348, 1989.

[81] R. Ramanujan, S. Kudige, and T. Nguyen. Techniques for intrusion-resistant ad hoc routing algorithms TIARA. In *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX)*, volume 02, page 98, Los Alamitos, CA, USA, 2003. IEEE Computer Society.

[82] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, pages 11–21, New York, NY, USA, 2005. ACM.

[83] M. T. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy. A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In *Proceedings of the Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MOBIQUITOUS)*, pages 3–11, Washington, DC, USA, 2005. IEEE Computer Society.

[84] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation systems. *Communications of the ACM*, 43(12):45–48, 2000.

[85] J. Reynolds, J. Just, E. Lawson, L. Clough, R. Maglich, and K. Levitt. The design and implementation of an intrusion tolerant system. In *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 285–292, Washington, DC, USA, 2002. IEEE Computer Society.

[86] N. B. Salem and J.-P. Hubaux. Securing wireless mesh networks. *IEEE Wireless Communications*, 13(2):50–55, 2006.

[87] J. Salido, L. Lazos, and R. Poovendran. Energy and bandwidth-efficient key distribution in wireless ad hoc networks: a cross-layer approach. *IEEE/ACM Transactions on Networking*, 15(6):1527–1540, 2007.

[88] J. Schoenwaelder. Overview of the 2002 IAB network management workshop, 2003.

[89] K. Seada, K. Westphal, and C. Perkins. Analyzing path accumulation for route discovery in ad hoc networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference*, pages 4377–4382, Washington, DC, USA, 2007. IEEE Computer Society.

[90] A. Shamir. How to share a secret. *ACM Communications*, 22(11):612–613, 1979.

[91] E. Silva, M. N. Lima, A. L. Santos, and L. C. P. Albini. Identity-based key management in mobile ad hoc neworks: Techniques and applications. *IEEE Wireless Communications*, 15, October 2008.

[92] V. Sridhara and S. Bohacek. Realistic propagation simulation of urban mesh networks. *Computer Networks*, 51(12):3392–3412, 2007.

[93] V. Srinivasan, P. Nuggehalli, C.-F. Chiasserini, and R. R. Rao. Cooperation in wireless ad hoc networks. In *Proceedings of INFOCOM*, 2003.

[94] W. Stallings. *SNMP, SNMPv2, and CMIP: The practical guide to network management standards*. Addison-Wesley, 1993.

[95] W. Stallings. *Cryptography and network security - fourth edition*. Prentice Hall, 2006.

[96] G. Staple and K. Werbach. The end of spectrum scarcity. *IEEE Spectrum*, 41(3):48–52, March 2004.

[97] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. Jackson, D. Levin, R. Ramanathan, and J. Zao. Survivable mobile wireless networks: issues, challenges, and research directions. In *Proceedings of the ACM Workshop on*

Wireless Security (WiSe), pages 31–40, New York, NY, USA, September 2002. ACM Press.

[98] C. Stevenson, G. Chouinard, L. Zhongding, H. Wendong, S. Shellhammer, and W. Caldwell. IEEE 802.22: The first cognitive radio wireless regional area network standard. *IEEE Communications Magazine*, 47(1):130–138, January 2009.

[99] A. Tsirigos and Z. Haas. Analysis of multipath routing-part i: the effect on the packet delivery ratio. *IEEE Transactions on Wireless Communications*, 3(1):138–146, 2006.

[100] S. Tsukiyama, M. Ide, H. Ariyoshi, and I. Shirakawa. A new algorithm for generating all the maximal independent sets. *SIAM Journal on Computing*, 6(3):505–517, 1977.

[101] S. Čapkun, L. Buttyán, and J.-P. Hubaux. Small worlds in security systems: an analysis of the PGP certificate graph. In *Proceedings of the New Security Paradigms Workshop (NSPW)*, pages 28–35, New York, NY, USA, 2002.

[102] P. Veríssimo, N. F. Neves, C. Cachin, J. Poritz, D. Powell, Y. Deswarte, R. Stroud, and I. Welch. Intrusion-tolerant middleware: the road to automatic security. *IEEE Security & Privacy*, 4(4):54–62, 2006.

[103] P. E. Veríssimo, N. F. Neves, and M. P. Correia. Intrusion-tolerant architectures: concepts and design. Technical Report DI-FCUL TR-03-5, University of Lisbon, Department of Informatics, University of Lisbon, 1749-016, Lisbon, Portugal, 2003.

[104] P. Veríssimo. Intrusion tolerance: concepts and design principles. a tutorial. DI/FCUL TR 02–6, Department of Informatics, University of Lisbon, July 2002.

[105] F. Viger and M. Latapy. Efficient and simple generation of random simple connected graphs with prescribed degree sequence. In *Proceedings of 11th Annual International Conference of Computing and Combinatorics (COCOON 2005)*, volume 3595 of *LNCS*, pages 440–449. Springer, 2005.

[106] F. Wang and R. Upppalli. SITAR: a scalable intrusion-tolerant architecture for distributed services. In *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX)*, volume 2, pages 153–155, 2003.

[107] S. T. Welstead. *Neural Network and Fuzzy Logic Applications in C/C++*. John Wiley & Sons, New York, NY, USA, 1994.

[108] B. Wu, J. Chen, J. Wu, and M. Cardei. *Wireless/mobile network security*, chapter A survey on attacks and countermeasures in mobile ad hoc networks. Springer, 2006.

[109] B. Wu, J. Wu, E. B. Fernandez, M. Ilyas, and S. Magliveras. Secure and efficient key management in mobile ad hoc networks. *Journal of Network and Computer Applications*, 30(3):937–954, 2007.

[110] J. Wu and D. J. Watts. Small worlds: the dynamics of networks between order and randomness. *ACM SIGMOD Record*, 31(4):74–75, 2002.

[111] J. Wylie, M. Bigrigg, J. Strunk, G. Ganger, H. Kiliççöte, and P. Khosla. Survivable information storage systems. *IEEE Computer*, 33(8):61–68, 2000.

[112] Y. Xue and K. Nahrstedt. Providing fault-tolerant ad hoc routing service in adversarial environments. *Wireless Personal Communications: An International Journal*, 29(3-4):367–388, 2004.

[113] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications*, pages 38–47, February 2004.

[114] H. Yang, X. Meng, and S. Lu. Self-organized network-layer security in mobile ad hoc networks. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 11–20, New York, NY, USA, 2002. ACM.

[115] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 299–302, New York, NY, USA, 2001. ACM Press.

[116] Y. Yuan, S. Wong, S. Lu, and W. Arbaugh. ROMER: resilient opportunistic mesh routing for wireless mesh networks. In *Proceedings of IEEE Workshop on Wireless Mesh Networks (WiMesh)*, Washington, DC, USA, 2005. IEEE Computer Society.

[117] L. A. Zadeh. Fuzzy logic. *Computer*, 21(4):83–93, 1988.

[118] M. G. Zapata. Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE*, 6(3):106–107, 2002.

[119] C. Zhang, Y. Song, and Y. Fang. Modeling secure connectivity of self-organized wireless ad hoc networks. In *IEEE INFOCOM*, pages 251–255, 2008.

[120] Y. Zhang, G. Xu, and X. Geng. Security threats in cognitive radio networks. In *Proceedings of thhe IEEE International Conference on High Performance Computing and Communications*, pages 1036–1041, September 2008.

[121] S. Zhong, J. Chen, and Y. Yang. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *Proceedings of IEEE INFOCOM*, volume 3, pages 1987– 1997, 2003.

[122] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

[123] P. R. Zimmermann. *The official PGP user's guide*. MIT Press, Cambridge, MA, USA, 1995.