Disseminação Segura de Dados Pessoais Vitais Para Apoio às Tomadas de Decisão em Situações Emergenciais

Agnaldo de Souza Batista[1], **Aldri Santos**[1] **(Orientador)**

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – PPGInf – UFPR

{asbatista,aldri}@inf.ufpr.br

Abstract. *Urban wireless networks established dynamically have become possible the quick dissemination of a number of data, making them a promising means to support services that require a prompt response. Network health services (e-health) can benefit from interactions in these networks, anticipating actions to be taken by trained people close to the events until the attendance by the competent health agencies. This dissertation presents the STEALTH system, which employs social trust and communities of interest to control the dissemination of people's sensitive data in emergencies in dynamic environments. An evaluation of STEALTH under a realistic environment has shown its effectiveness in anticipating the identification of people close to assist in critical health events and the reliability for the dissemination of sensitive data of people in an emergency.*

Resumo. *As redes urbanas estabelecidas dinamicamente têm possibilitado a disseminação de dados de maneira rápida, tornando-se um meio promissor ao suporte de serviços que exigem pronta resposta. Os serviços de saúde em redes (e-health) podem se beneficiar das interações nessas redes, e possibilitar ações antecipadas por pessoas capacitadas próximas aos eventos até o atendimento pelos órgãos de saúde competentes. Esta dissertação apresenta o sistema STEALTH, que emprega confiança social e comunidades de interesse no controle da disseminação dos dados sensíveis das pessoas em situações emergenciais em ambientes dinâmicos. Uma avaliação do STEALTH num ambiente realístico mostrou a sua eficácia ao antecipar a identificação de pessoas próximas para auxiliar em eventos críticos de saúde, e a sua confiabilidade na disseminação controlada dos dados sensíveis das pessoas em situação emergencial.*

1. Introdução

As redes de computadores têm possibilitado o provimento de novos serviços online, e auxiliam a população em domínios de aplicação essenciais e críticos como transporte, vigilância, saúde, entre outros. Contudo, a disseminação de dados muitas vezes depende da criação e manutenção de redes locais ou globais estabelecidas dinamicamente. Nessas redes, a mobilidade dos dispositivos naturalmente implica estabelecer e interromper conexões a qualquer instante, dificultando o conhecimento do histórico de interações dos dispositivos (i.e., condição *Zero-Knowledge* [Kim et al. 2015]). Logo, a verificação da robustez da confiança dos dispositivos contribui para a disseminação de dados no momento oportuno e às entidades competentes. Nesse contexto, as informações provenientes dos dispositivos computacionais no momento de suas interações, especialmente aquelas das relações sociais de seus proprietários, colaboram na avaliação da confiança do dispositivo e auxiliam nas tomadas de decisões sobre a disseminação controlada dos dados.

Ambientes de cuidados de saúde, como hospitais e clínicas, normalmente dispõem de infraestrutura de redes específicas, permitindo o acesso a dados em eventos críticos que envolvam alterações nas condições de saúde das pessoas. Discussões éticas sobre o manuseio desses dados buscam proteger a privacidade dos seus proprietários e garantir os benefícios advindos do seu uso, sendo regulado na União Europeia pelo Regulamento Geral de Proteção de Dados [Regulation 2016]. Contudo, em ambientes urbanos e esparsos surgem desafios em razão da mobilidade das pessoas e da fragilidade das infraestruturas das redes, que muitas vezes prejudicam a disseminação de dados sensíveis de saúde, como por exemplo em surtos de doenças ou em cenários de conflitos, e nem sempre é possível entregá-los ao profissional de saúde imediatamente [Organization 2019]. No entanto, os eventos críticos notadamente exigem respostas rápidas e efetivas, sendo crucial o acesso aos dados sensíveis e privados da pessoa em situação emergencial a fim de antecipar e ampliar a eficácia do atendimento. Por exemplo, cada minuto em parada respiratória diminui em 10% a probabilidade de sobrevida de uma pessoa [Pazin-Filho et al. 2003].

A mobilidade dos usuários nos ambientes urbanos possibilita interações dinâmicas entre seus dispositivos, que por sua vez detém, por meio de coleta e troca, diversos tipos de informações, inclusive, por exemplo, os aspectos sociais dos seus proprietários e de suas relações. Nessas condições, conhecer a confiança desses dispositivos para controlar a disponibilidade e o acesso aos dados sensíveis disseminados torna-se um desafio. Embora eficientes, o uso apenas de técnicas tradicionais como reputação e recomendação nem sempre é útil nesses ambientes, devido à dependência do histórico das interações dos dispositivos. Assim, além da criação e manutenção de redes dinâmicas para suportar a disseminação dos dados em ambientes dinâmicos, a verificação da confiança dos dispositivos por meio de aspectos sociais dos seus proprietários e de suas relações possibilita uma disseminação segura e de forma controlada às entidades competentes.

Esta pesquisa apresenta o sistema STEALTH[1] (***S**ocial **T**rust-Based **HEALTH** Information Dissemination Control)*, que estabelece redes locais dinâmicas sem fio e, diante de eventos críticos, suportam a disseminação de dados sensíveis de saúde de maneira controlada. O STEALTH baseia-se em aspectos sociais dos proprietários dos dispositivos e de suas relações para mensurar a confiança dos dispositivos de rede e agrupá-los em comunidades. Essa forma de agrupamento dos dispositivos contribui para as tomadas de decisão acerca da disseminação dos dados sensíveis, limitando-a aos dispositivos de uma mesma comunidade. Em situações emergenciais de saúde do proprietário do dispositivo, o STEALTH dissemina seus dados sensíveis de modo controlado às pessoas competentes, aquelas fisicamente próximas ao evento emergencial e com interesse em saúde. No melhor de nosso conhecimento, este é o primeiro trabalho sobre disseminação de dados de saúde em ambientes urbanos dinâmicos, externos aos ambientes de cuidados de saúde.

Este artigo está organizado da seguinte forma: A Seção 2 descreve o STEALTH e seu funcionamento. A Seção 3 detalha a metodologia de avaliação do sistema e uma análise do desempenho. A Seção 4 apresenta as conclusões e contribuições do trabalho.

2. STEALTH: Controle de Disseminação de Dados Pessoais Sensíveis

O sistema STEALTH dissemina dados sensíveis pessoais diante de um evento emergencial de modo oportuno e de maneira controlada às pessoas fisicamente próximas

[1] http://www.nr2.ufpr.br/~asbatista/stealth.html

e com interesse em saúde. O STEALTH estabelece redes locais dinâmicas sem fio para suportar a formação de comunidades pelo agrupamento dos dispositivos, conforme ilustra a Figura 1. Esses agrupamentos formam-se por meio de aspectos sociais das pessoas e de suas relações. A avaliação da confiança dos dispositivos durante suas interações emprega as informações que eles detém nesses instantes. A arquitetura do STEALTH, retratada na Figura 2, consiste do módulo *Gestão de Comunidades*, responsável por criar e atualizar as comunidades de interesse (CoI) estabelecidas ao longo do tempo a partir da interação entre os dispositivos das pessoas portadoras; e do módulo *Gestão de Eventos Críticos*, responsável por verificar e disseminar os dados sensíveis da pessoa em situação emergencial ao dispositivo da pessoa competente durante eventos críticos.[2]

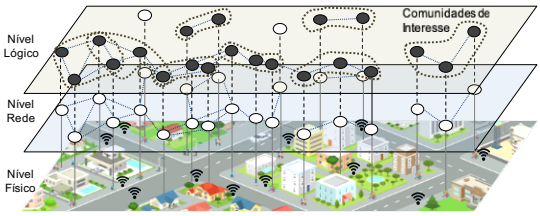

Figura 1. Modelo de Rede

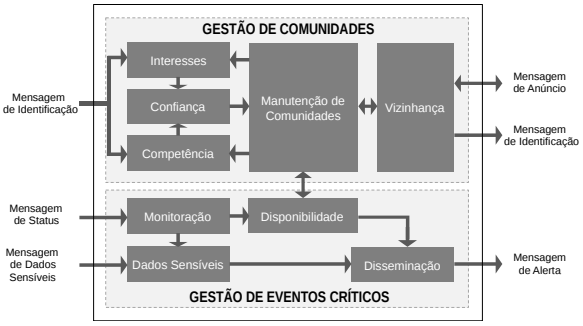

Figura 2. Arquitetura do STEALTH

O funcionamento do STEALTH inicia com a operação dos nós da rede forma isolada e, na medida em que se movimentam, eles encontram outros nós e formam comunidades de interesse. Periodicamente, cada nó inicializa sua lista de vizinhos, anuncia sua presença por mensagens de anúncios em *broadcast* à procura de nós vizinhos e aguarda um intervalo de tempo até um novo anúncio. Quando um nó vizinho percebe que um nó anuncia a sua presença, encaminha a este nó anunciador uma mensagem de identificação, composta pela seu *Id*, competência e interesses. O nó anunciador, ao receber essa mensagem do nó vizinho, verifica a existência de interesse em comum em saúde entre eles. Quando há esse interesse, ele mede a confiança do nó vizinho e o insere na sua lista de vizinhos, dentro da sua comunidade de saúde. A partir dessa confiança (Eq. 1) e da sua competência (Eq. 2), obtém-se a confiança total do nó (Eq. 3). Assim, ao ocorrer um evento crítico com um nó, este nó determina o nó vizinho que ele mais confia, e o dado sensível apropriado a ser disseminado. Em seguida, ele envia uma mensagem de alerta ao nó selecionado com seu dado sensível, e anuncia em *broadcast* a interrupção de sua operação. Ao receber uma mensagem de alerta, o nó confirma seu recebimento.

$$T_{xy}^{I} = \frac{|I_x \cap I_y|}{|I_x|} \quad (1) \qquad T_{xy}^{Skill} = Sim_y \quad (2) \qquad T_{xy} = \frac{T_{xy}^{I} + T_{xy}^{Skill}}{2} \quad (3)$$

Considere uma área urbana onde seis pessoas deslocam-se a pé pelas ruas. Essas pessoas possuem um interesse em saúde e não mantêm relações entre si, mas podem estabelecer **redes locais dinâmicas** em razão da sua proximidade e do interesse em comum. Elas portam dispositivos móveis, *smartphones*, onde o STEALTH executa. O paciente também porta um dispositivo de sensoriamento junto ao corpo para coletar e verificar, por exemplo sua pressão arterial, e reportar a um aplicativo instalado em seu *smartphone*. Esse aplicativo informa ao STEALTH os valores medidos e sua normalidade ao paciente.

[2]Detalhes dos módulos, algoritmos e equações do STEALTH encontram-se na dissertação.

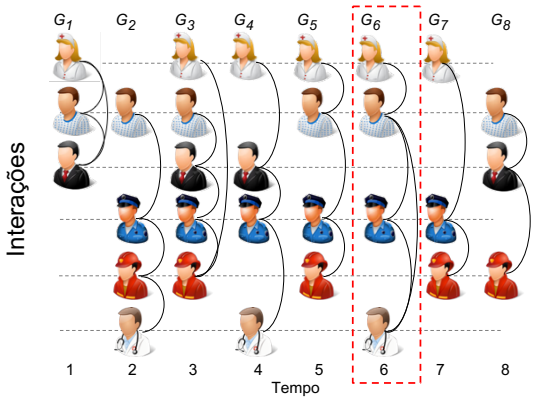

Figura 3. Interações no tempo

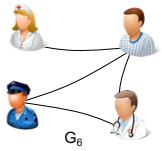

Figura 4. Grafo da rede em t_6

Tabela 1. Medição da confiança

Confiança	Competência		
	Médico	Enfermeira	Policial
T^{Skill}	1	0,33	0,28
T^{CoI}	1	1	1
T	1	0,66	0,64

As interações entre as pessoas ao longo do tempo $t = \{1, 2, ..., 8\}$ estabelecem redes locais, ilustradas na Figura 3, no momento que seus dispositivos criam conexões para trocarem dados entre si. Além disso, assume-se que o paciente entra em uma situação emergencial no tempo t_6. Nesse instante, o seu dispositivo terá interagido com os dispositivos das pessoas próximas, como ilustra o grafo temporal G_6 (Figura 4), e cada um deles formado sua própria comunidade de saúde. O dispositivo do paciente também terá medido a confiança dos vizinhos e armazenado os valores exibidos na Tabela 1. Ao ocorrer o evento crítico em t_6, o STEALTH executando no *smartphone* do paciente recomenda o médico como o maior valor de confiança na sua comunidade de saúde e, assim, dissemina seus dados sensíveis para que ele possa adotar alguma ação.

3. Metodologia da Avaliação e Resultados

O desenvolvimento e a simulação do STEALTH foram realizados no simulador NS-3, versão 3.28.[3] Os resultados exibidos correspondem à média de 35 simulações, com intervalo de confiança de 95%, exceto a evolução das comunidades de interesse em saúde ao longo do tempo, que considerou uma repetição específica da simulação. A análise da disponibilidade dos dados provida pelo STEALTH levou em conta a métrica *Número médio de comunidades de interesse em saúde* (N_C) e a evolução das comunidades. A análise da confiabilidade levou em conta as métricas *Taxa de sucesso no acesso aos dados* (TS), *Taxa de dados não acessados* (TN_a), *Tempo médio de acesso aos dados* (MTA), e *Taxa de sucesso no acesso aos dados por competência* (TS_{Skill}). Os parâmetros empregados nas simulações e os resultados obtidos encontram-se na dissertação.

Tabela 2. Distribuição dos aspectos sociais atribuídos aos dispositivos

Aspectos Sociais	Competências				Interesses				
	Médico	Enfermeiro	Cuidador	Outras	Saúde	Turismo	Música	Filmes	Livros
# de Nós	10	15	20	55	20	30	45	60	15

A configuração dos nós da rede com os aspectos sociais na Tabela 2 aconteceu de maneira randômica a cada repetição de simulação. Assim, cada nó recebeu uma única competência e um conjunto de interesses, com o mínimo de um e máximo cinco. A avaliação do sistema ocorreu por meio dos nós 37, 52 e 70. Assumiu-se que todos os nós

[3]Código disponível em https://github.com/agnaldosb/stealth

possuem um comportamento honesto e há mecanismos de segurança para validar suas identidades e proteção na transmissão dos dados. O alerta de um evento crítico acontece por um dispositivo portado pelas pessoas junto ao corpo, que informa ao STEALTH.

3.1. Análise da Disponibilidade e Confiabilidade

A disponibilidade do STEALTH representa sua prontidão para disseminar com sucesso e de modo controlado os dados sensíveis das pessoas em situação emergencial. O número médio de comunidades de interesse em saúde (N_C) demonstra esse comportamento (Figura 5). As CoI do nó 37, em média, 12 CoI em cada repetição de simulação, caracterizam a dinamicidade das redes locais estabelecidas e de sua topologia. A mobilidade dos nós, associada aos seus aspectos sociais (interesses), impactou na suas comunidades. O STEALTH acompanhou a dinamicidade das redes locais criadas devido à mobilidade dos nós, e ajustou suas CoI (Figura 6). Das 35 repetições de simulações realizadas, numa delas o nó 52 teve um comportamento distinto, quando manteve comunidades em 97,22% do tempo, até entrar em situação emergencial. Neste instante, apenas dois dos seus sete vizinhos pertenciam a sua comunidade de saúde (i.e., nós 13 e 41). Em razão do nó 13 possuir uma competência mais elevada em saúde, *cuidador*, o nó 52 disseminou seus dados para ele.

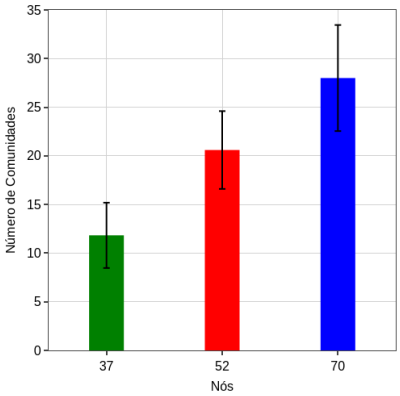

Figura 5. NC do STEALTH

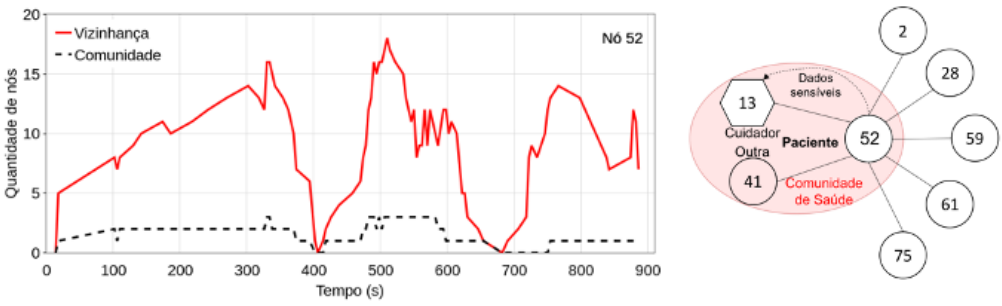

Figura 6. Dinamicidade e tamanho da comunidade de saúde ao longo do tempo

A análise da confiabilidade leva em conta a capacidade do sistema em disseminar com sucesso e de modo controlado os dados sensíveis das pessoas em situação emergencial. O nó 52 foi bem-sucedido (TS) na disseminação de seus dados em 80% das situações emergenciais ao longo das repetições de simulações. A quantidade de dados sensíveis não acessados (TNa) aponta a relevância das comunidades no controle da disseminação. A falta da comunidade do nó 37 impediu que 68,57% de seus dados sensíveis fossem acessados por nós não autorizados. A presença das comunidades dos nós 70 e 52 por mais tempo possibilitou uma efetividade maior na disseminação dos seus dados sensíveis no instante em que entraram em situação emergencial. O MTA representa o custo em relação ao tempo de acesso aos dados sensíveis de um nó. A dinamicidade das redes locais estabelecidas impacta o MTA porque a mobilidade dos nós impõe mudanças à topologia dessas redes. Os resultados na Tabela 3 demonstram que o STEALTH atende à latência máxima de 125ms estabelecida pela IEEE para a entrega de alertas médi-

cos [Association et al. 2012]. O acesso aos dados sensíveis do nó 52 aconteceu mais rapidamente que aos dos demais nós (MTA < 1ms), já os dados do nó 37 foram acessados, em média, após 95ms de sua disseminação, mostrando uma margem confiável de alerta.

Tabela 3. Disseminação dos dados

Métrica		TS	TN_a	MTA
Nó	37	31,43%	**68,57%**	**95 ms**
	52	**80,00%**	20,00%	< 1ms
	70	60,00%	40,00%	2,3 ms

Tabela 4. Controle de disseminação

Métrica		TS_{Skill}
Competência	Médico	30,03%
	Enfermeiro	39,40%
	Cuidador	9,09%

Os interesses e competências, associados às comunidades, além de possibilitarem avaliar a confiança dos dispositivos, proporcionam o controle da disseminação dos seus dados sensíveis. Através da recriação periódica das comunidades de saúde, esse controle desconsidera as interações anteriores entre os dispositivos da rede (i.e., condição *Zero-Knowledge*). O sucesso no acesso aos dados por competência (TS_{Skill}) comprova a relevância das competências das pessoas nas comunidades estabelecidas. Na Tabela 4, observa-se que os *médicos* obtiveram acesso aos dados em 30,03% das situações, assim o STEALTH detectou a melhor competência para tratar as situações emergenciais.

4. Conclusão

Esta dissertação tratou do problema de proporcionar a disseminação de dados sensíveis de saúde de modo robusto em ambientes urbanos dinâmicos, a fim de contribuir para uma ação rápida e efetiva. Para enfrentar esse desafio de cuidados da saúde, apresentou-se o STEALTH, um sistema para disseminar dados sensíveis de saúde de forma controlada em redes locais dinâmicas sem fio. Ele estabelece agrupamentos virtuais por meio de comunidades de interesse e aplica confiança social para permitir aos dispositivos decidirem de maneira robusta sobre a disseminação de dados diante de uma situação emergencial. Uma avaliação do STEALTH com dados reais de mobilidade em ambiente urbano mostrou a sua eficácia ao antecipar a identificação de pessoas próximas para auxiliar em eventos críticos de saúde, e sua confiabilidade na disseminação controlada dos dados sensíveis das pessoas em situação emergencial. As contribuições deste trabalho resultaram na publicação [Batista et al. 2019].

Referências

Association, I. S. et al. (2012). 802.15. 6-2012 IEEE Standards for Local and Metropolitan Area Networks–Part 15.6: Wireless Body Area Networks.

Batista, A., Santos, A., and Nogueira, M. (2019). Disseminação Robusta de Dados Pessoais Sensíveis Baseada em Comunidade de Interesse e Confiança Social para Suportar Situações Emergenciais de Saúde. In *Anais SBSeg 2019*, Porto Alegre, RS, Brasil. SBC.

Kim, S.-K., Yoon, J.-H., Lee, J., and Yang, S.-B. (2015). Hcs: hierarchical cluster-based forwarding scheme for mobile social networks. *Wireless Networks*, 21(5):1699–1711.

Organization, W. H. (2019). Who's work in emergencies: prepare, prevent, detect and respond: annual report 2018. Technical documents, World Health Organization.

Pazin-Filho, A., Santos, J. C., Castro, R. B. P., Bueno, C. D. F., and Schmidt, A. (2003). Parada cardiorrespiratória (pcr). *Medicina (Ribeirão Preto. Online)*, 36(2/4):163–178.

Regulation, G. D. P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union*, 59(1-88):294.