Disseminação Robusta de Dados Pessoais Sensíveis Baseada em Comunidade de Interesse e Confiança Social para Suportar Situações Emergenciais de Saúde

Agnaldo Batista[1], **Michele Nogueira**[1], **Aldri Santos**[1]

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

{asbatista,michele,aldri}@inf.ufpr.br

Abstract. *E-health services deal with sensitive personal data, which must be preserved in the delivery and from unauthorized access. Dissemination control mechanisms have currently focused on health structured environments, like hospitals, and still do not adequately support the moments from an emergency takes place until health care in urban dynamic environments, as streets and avenues. Social aspects from people and their relationships contribute to preserving data delivery. This paper presents STEALTH, a system that employs social trust and communities of interest (CoI) to control the dissemination of people's sensitive data in emergencies on dynamic environments. NS-3 Simulations demonstrate its ability to ensure data dissemination to people who can contribute to efficient service. STEALTH achieved up to 80% of reliability in access to data with maximum latency of 95ms, up to 98,8% of availability for emergency situations.*

Resumo. *Os serviços de saúde em redes (e-health) lidam com dados pessoais sensíveis, que devem ser preservados na entrega e do acesso não autorizado. Os mecanismos de controle de disseminação atualmente se voltam principalmente aos ambientes de saúde estruturados, como hospitais, mas ainda não atendem adequadamente nos momentos entre o surgimento de uma emergência e o seu atendimento em ambientes urbanos dinâmicos, como ruas e avenidas. Aspectos sociais das pessoas e de suas relações contribuem para a entrega confiável desses dados. Este trabalho apresenta STEALTH, um sistema que emprega confiança social e comunidades de interesse (CoI) para controlar a disseminação dos dados sensíveis das pessoas em situações emergenciais em ambientes dinâmicos. Simulações no NS-3 demonstram sua capacidade de assegurar a disseminação de dados sensíveis às pessoas que possam contribuir para um atendimento eficiente. STEALTH obteve uma confiabilidade de até 80% no acesso aos dados disseminados, uma latência máxima de 95ms e uma disponibilidade de até 98,8% para atender situações emergenciais.*

1. Introdução

O uso de redes de computadores, especialmente da Internet, permite disponibilizar uma quantidade cada vez maior de serviços online. Eles auxiliam a população em domínios de aplicação como transporte, vigilância, saúde, entre outros. Geralmente esses serviços coletam e entregam dados, muitas vezes por contatos oportunísticos, quando as interações permitem a comunicação com pessoas próximas geograficamente [Garyfalos and Almeroth 2008]. Contudo, entregar dados implica seu compartilhamento

e exige observar questões como a frequência, o local e o conteúdo a ser disseminado [Vivekavardhana and Sudhindra 2014]. Muitos destes serviços, em razão das suas caraterísticas, naturalmente têm exigido o suporte da criação e manutenção de redes locais ou globais, estabelecidas dinamicamente, para garantir o seu funcionamento.

A interação entre dispositivos computacionais móveis e as pessoas tem sido intensificada e estabelecido redes locais temporárias, onde se trocam informações com diferentes propósitos e normalmente por um certo período de tempo. Essas redes locais podem ser estabelecidas através de redes ad hoc sem fio, embora as redes de telefonia móvel, por exemplo, ofereçam uma cobertura cada vez maior nas cidades. Contudo, elas não permitem uma comunicação direta entre dispositivos, muitas das vezes podendo influenciar no tempo de atendimento de eventos críticos. Dispositivos móveis, como *smartphones*, dada sua presença massiva, coletam vários tipos de dados a fim de apoiar melhorias nos serviços de vigilância, transportes e saúde, entre outros. Particularmente nos serviços de saúde, os *smarphones* possibilitam interconectar dispositivos médicos das pessoas à Internet, que, eventualmente, disseminam dados ignorando suas consequências [Williams et al. 2016] e comprometem sua segurança. Os serviços de saúde em redes (*e-health*) auxiliam a acompanhar remotamente o estado de saúde dos cidadãos e os *feedbacks* auxiliam a mudar comportamentos nocivos ao seu bem estar. Por exemplo, em uma área urbana onde pessoas deslocam-se a pé pelas ruas, uma delas pode sentir-se mal e ser auxiliada por aquelas ao seu redor. Os alertas médicos devem ser transmitidos imediatamente [Movassaghi et al. 2014], com uma latência máxima de 125ms [Association et al. 2012], visto que perdas ou atrasos desses alertas acarretam consequências graves à saúde dos pacientes [Latré et al. 2011].

Atualmente, há diversas plataformas para interação social das pessoas, onde aspectos das suas relações são observados e empregados no controle das trocas de dados. Muitas dessas plataformas online potencializam a distribuição de informações, causam vazamentos de dados e comprometem sua segurança, como aconteceu com o Facebook [Silverstein 2019]. Logo, um serviço seguro (*safety*) de disseminação de dados em redes entrega os dados às pessoas corretas e evita vazamentos [Lima et al. 2009]. Embora diversos trabalhos na literatura tratem essa segurança em redes não estruturadas nos contextos de IoT [Al-Hamadi and Chen 2017, Bao et al. 2013], MANETs [Nogueira et al. 2012] e P2P [Vasilomanolakis et al. 2017], as soluções geralmente se destinam a ambientes centralizados e necessitam conhecer as interações anteriores para a tomada de decisões no manuseio dos dados. Poucas pesquisas voltam-se aos ambientes onde interações anteriores são desconhecidas (*Zero-Knowledge* [Feige et al. 1988]), nos quais há informações apenas de interações atuais. Dessa forma, essas soluções não são adequadas aos ambientes urbanos dinâmicos e esparsos, pois consideram a existência prévia de uma infraestrutura de rede para atender à disseminação de dados.

O controle da disseminação dos dados em redes pretende garantir a entrega de dados às entidades corretas e no tempo adequado. Alguns trabalhos encontrados na literatura empregam confiança como critério para esse controle [Al-Hamadi and Chen 2017]. Entende-se por confiança como a vontade de uma pessoa de arriscar-se, baseada numa crença subjetiva de que aquele em quem ela confia exibirá um comportamento confiável. A confiança social provém das relações entre essas pessoas no ambiente das redes sociais. [Cho et al. 2015] e é empregada para agrupar nós da rede, estabelecendo comuni-

dades de interesse baseadas em aspectos sociais dos proprietários dos dispositivos de rede e de suas relações [Bao et al. 2013]. Embora adequados às redes não estruturadas, esses trabalhos empregam reputação e recomendação para avaliar a confiança, que são técnicas dependentes de informações relativas às interações passadas entre os dispositivos.

Este trabalho apresenta o sistema STEALTH (***S**ocial **T**rust-Based **HEALTH** Information Dissemination Control)* para disseminar dados sensíveis de saúde de maneira controlada em redes locais dinâmicas sem fio. Ele estabelece comunidades ao agrupar os dispositivos com interesses em comum e emprega aspectos sociais dos proprietários dos dispositivos e de suas relações a fim de mensurar sua confiança. Na presença de situações emergenciais de saúde do proprietário do dispositivo, o sistema dissemina seus dados sensíveis de maneira controlada. O STEALTH foi avaliado no simulador NS-3 para analisar sua robustez na disseminação de dados sensíveis em situações emergenciais às pessoas adequadas, isto é, aquelas fisicamente próximas ao evento emergencial e com interesse em saúde. No melhor de nosso conhecimento, este é o primeiro trabalho voltado para disseminação de dados de saúde em ambientes urbanos dinâmicos, externos às estruturas hospitalares. Os resultados mostram que a confiabilidade do STEALTH na disseminação e acesso aos dados atingiu 80% e uma latência máxima de 95ms, enquanto sua disponibilidade para atender situações emergenciais chegou a 98,8%.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve os modelos de redes e de agrupamento de comunidades de interesse para a disseminação de dados. A Seção 4 descreve o sistema proposto e detalha o funcionamento dos seus módulos e componentes. A Seção 5 detalha a avaliação e os resultados obtidos. A Seção 6 apresenta a conclusão e os trabalhos futuros.

2. Trabalhos Relacionados

O emprego de técnicas de confiança para garantir a segurança no compartilhamento de dados é investigado por diversos trabalhos na literatura [Cho et al. 2015]. Nas redes não estruturadas e distribuídas, emprega-se técnicas de recomendação [Al-Hamadi and Chen 2017] e de reputação [Truong et al. 2017], além de comunidades de interesse [Bao et al. 2013] para avaliar a confiança dos dispositivos. A recomendação e a reputação demandam conhecer as interações anteriores entre os nós, a fim de permitir observar seu comportamento ao longo do tempo. Contudo, poucos focam nos ambientes *Zero-Knowledge*, onde manter históricos de interações nem sempre é viável.

Um protocolo baseado em recomendação e no compartilhamento de informações entre dispositivos de saúde na IoT foi proposto para tomada de decisão acerca do acesso a determinados locais [Al-Hamadi and Chen 2017]. Avalia-se ambientes frequentados pelos proprietários dos dispositivos em um momento e local específicos usando recomendações, para se construir uma base de dados coletiva desses ambientes. A performance do protocolo foi avaliada mediante simulação no NS-3. As recomendações incorporam características das relações sociais dos proprietárias dos dispositivos às tomadas de decisão. No entanto, exigem interações frequentes entre os dispositivos, às vezes eventuais em ambientes de rede dinâmicos e insuficientes para a construção da base de dados.

O trabalho [Truong et al. 2017] apresentou uma abordagem distribuída para avaliação de confiança chamada REK. Ela compreende o uso de três indicadores de confiança: reputação - opinião pública acerca de quem é avaliado; experiência - oriunda das intera-

ções prévias com o avaliado; e conhecimento - entendimento a respeito do avaliado. Os autores propuseram modelos de avaliação desses indicadores, mas não apresentaram resultados. A confiança é composta de maneira indireta, a partir de informações obtidas de outros nós da rede. O uso de reputação permite distinguir certos nós para executar tarefas mais importantes. Porém, ela demanda conhecimento das interações dos nós ao longo do tempo. Essa abordagem é adequada às redes IoT, pois atua de maneira distribuída. Adicionalmente, obter indicadores subjetivos como conhecimento e experiência é um grande desafio, assim como sua mensuração é complexa [Cho et al. 2015].

O agrupamento de nós de rede em comunidades de interesse (CoI) foi empregado por [Bao et al. 2013] em um protocolo escalável para gerenciar a confiança em ambientes de IoT social dinâmicos. Essas comunidades formam-se a partir de atributos relacionais de confiança oriundos das relações sociais dos proprietários dos dispositivos, tais como honestidade e cooperatividade, entre outros. Os nós agrupam-se ou deixam os agrupamentos a qualquer momento. Eles são avaliados por observações diretas dos nós e por recomendações. Como recomendações dependem do histórico de interações entre dispositivos, isso inviabiliza o uso do protocolo em ambientes com interações eventuais. Contudo, as CoI restringem em alguma medida a comunicação aos seus dispositivos, atendem à escalabilidade da rede e limitam o acesso aos dados trafegados aos seus nós.

Diante dos aspectos abordados, este trabalho apresenta um sistema para disseminação controlada de dados sensíveis de pessoas em situação emergencial, externa aos ambientes das instituições de saúde. Seu funcionamento é possível mediante o emprego de comunidades de interesse estabelecidas com base em atributos de confiança das pessoas envolvidas. Essas características possibilitam avaliar a confiança dessas pessoas num certo instante, descartando o emprego dos históricos de interações entre elas.

3. Visão Geral dos Modelos de Redes e de Competência

Esta seção apresenta uma visão geral dos modelos do ambiente físico, de infraestrutura de rede e de agrupamento lógico dos dispositivos onde o sistema proposto, chamado STEALTH e descrito na próxima seção, executa. Ele baseia-se em aspectos sociais dos proprietários dos dispositivos e de suas relações para criar redes locais ao longo do tempo, a fim de manter comunidades de interesse. Diante de eventos críticos, ele dissemina os dados sensíveis da pessoa em situação emergencial a uma pessoa adequada que esteja fisicamente próxima, na medida da sua competência em saúde, para apoiar o atendimento emergencial da pessoa necessitada, em complemento às estruturas hospitalares.

O STEALTH executa sobre um conjunto de dispositivos portáveis (nós) interligados numa rede de comunicação sem fio denotados por $D = \{d_1, d_2, d_3, ..., d_j\}$, onde $d_j \in D$. Esses nós possuem capacidade de processamento e de comunicação para agrupar nós e disseminar dados. Assume-se que cada nó possui um identificador único (Id), que o identifica ao longo do tempo, e competência e interesses como atributos individuais de confiança. O conjunto de competências $S = \{s_1, s_2, s_3, ..., s_k\}$, tal que $|S| \neq 0$, onde uma competência s_n representa uma habilidade, perícia ou conhecimento em uma determinada área de atuação, tal como médico, policial, enfermeiro, etc. Assume-se, também, que cada nó venha a ter um conjunto de interesses $I_n = \{i_1, i_2, i_3, ..., i_z\}$, tal que $|I_n| \neq 0$ e $I_n \subset I$, onde I é o conjunto de todos os interesses. Um interesse é um *hobby*, gosto ou preferência, tal como música, saúde, entre outros. Os nós se agru-

pam por interesses em comum e formam comunidades por um dado período de tempo. Uma comunidade C é um conjunto de tuplas distintas $\langle$nó, período, interesse$\rangle$, onde $C = \{\langle d_1, P_l, i_z\rangle, \langle d_2, P_l, i_z\rangle, ..., \langle d_n, P_l, i_z\rangle\}$ e $P_l = ((t_{s0}, t_{e0}), (t_{s1}, t_{e1}), ..., (t_{sl}, t_{el}))$, com $t_{s*} \leq t_{e*}$[1]. A eficiência do uso dos interesses dos nós como critério para formação das comunidades está associado à sua similaridade, enquanto a competência somente será efetiva no âmbito interno de cada comunidade estabelecida. Por simplicidade, assume-se que os nós desconectados ou com falhas intermitentes não atuam na rede. Além disso, os nós conectados possuem comportamento honesto, sendo desconsiderada a ocorrência de ataques sobre o funcionamento do sistema.

4. STEALTH: Controle de Disseminação de Dados Pessoais Sensíveis

Esta seção descreve os componentes do sistema STEALTH (***S**ocial **T**rust-Based **HEALTH** Information Dissemination Control*), bem como as suas interações e modo de funcionamento. A arquitetura do STEALTH é composta de dois módulos, como ilustra a Figura 1: o módulo **Gestão de Comunidades**, responsável por criar e atualizar as comunidades de interesse estabelecidas ao longo do tempo a partir da interação entre os dispositivos das pessoas portadoras; e o módulo **Gestão de Eventos Críticos**, responsável por verificar e disseminar os dados sensíveis da pessoa em situação emergencial ao dispositivo da pessoa adequada na presença de eventos críticos.

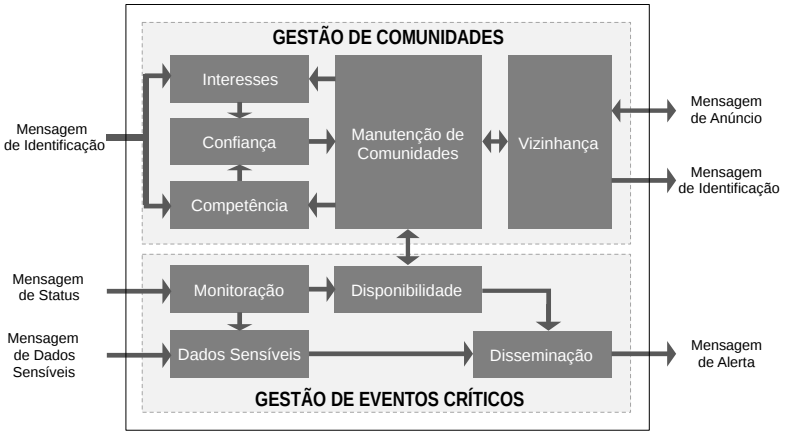

Figura 1. Arquitetura do STEALTH

4.1. Módulo Gestão de Comunidades

Este módulo mede a confiança dos dispositivos (nós) que estejam próximos e os inclui em uma comunidade ao receber sua mensagem de identificação, composta pelo seu *Id*, interesses e competência. Ele também é responsável por se identificar perante um nó que esteja em busca de nós vizinhos para formar suas próprias comunidades. Esse módulo é composto por cinco componentes: o componente *Vizinhança* busca por nós vizinhos e também encaminha uma mensagem de identificação a outros nós que também buscam por vizinhos, com o objetivo de identificar sua vizinhança; o componente *Interesses* verifica os interesses dos nós próximos ao recebê-los do nó vizinho, identifica interesses em comum para agrupar os nós e formar comunidades de interesse; o componente *Competência* trata da competência dos nós vizinhos ao receber suas informações de competência, a

[1]Definição adaptada do conceito de comunidades dinâmicas proposto por [Coscia et al. 2011] e revisado por [Rossetti and Cazabet 2018]

fim de saber o seu nível de competência em saúde; o componente *Confiança* mensura a confiança dos nós vizinhos ao receber seus interesses e competência, diante dos próprios interesses, a fim de verificar na sua comunidade de saúde o nó vizinho com a competência mais elevada em saúde; e o componente *Manutenção de Comunidades* coordena a criação, extinção e modificação das CoIs, a partir das informações de interação com os nós vizinhos. Assim, ele garante que as comunidades de interesse acompanhem a evolução das redes locais estabelecidas ao longo do tempo.

Algoritmo 1: Gestão de Comunidades

```
1  for each node d ∈ D do
2      procedure SEARCHNEIGHBORS( )
3          while (true) do
4              NeighborList ← 0
5              SendAnnounce( )
6              WaitInterval( )
7          end while
8      end procedure
9      procedure RECEIVEANNOUNCE( )
10         neighskill ← GetSkill( )
11         neighinterest ← GetInterests( )
12         AnswerAnnounce(id, neighskill, neighinterest)
13     end procedure
14     procedure RECEIVEANSWER (id, neighskill, neighinterests)
15         if (CommonInterests(neighinterests) AND HealthInterest(neighinterests))
16             neightrust ← EvaluateNeighborTrust(neighskill, neighinterests)
17             NeighborList ← RegisterNeighbor(id, neighskill, neighinterests, neightrust)
18         end if
19     end procedure
20     procedure EVALUATENEIGHBORTRUST (neighskill, neighinterests)
21         skilltrust ← GetSkillTrust(skill, SkillsTaxonomy)
22         numcommoninterests ← GetNumCommonInterests(interests)
23         numnodeinterests ← GetNumNodeInterests( )
24         interesttrust ← numcommoninterests / numnodeinterests
25         return (skilltrust + interesttrust) / 2
26     end procedure
```

Os nós da rede iniciam sua operação de forma isolada e, na medida em que se movimentam, encontram outros nós e estabelecem comunidades de interesse. Como descrito no Algoritmo 1, periodicamente, cada nó inicializa sua lista de vizinhos (*l*.3), anuncia sua presença por mensagens de anúncios em *broadcast* (*l*.4) à procura de nós vizinhos e aguarda um intervalo de tempo até um novo anúncio (*l*.5). Quando um nó vizinho percebe que um nó anuncia a sua presença (*l*.8), encaminha a este nó anunciador uma mensagem de identificação, composta pela seu *Id*, competência e interesses (*l*.11). O nó anunciador, ao receber essa mensagem do nó vizinho, verifica a existência de interesse em comum em saúde entre eles (*l*.14). Quando há esse interesse em comum, ele mede a confiança do nó vizinho (*l*.15) e o insere na sua lista de vizinhos (*l*.16), dentro da sua comunidade de saúde. Essa medição leva em conta a confiança do nó vizinho acerca da sua competência (*l*.20) e dos interesses em comum que eles possuem (*l*.21-23).

4.1.1. Medição da Confiança

A medição da confiança ocorre a partir de aspectos sociais do nó avaliado: um individual - *Competência* - e um outro relacional - *Similaridade*. A confiança é um valor

variável e aumenta à medida que a competência em saúde do nó avaliado se aproxima da competência *médico*. A similaridade refere-se aos interesses em comum entre o nó avaliador e o avaliado. Logo, o valor da confiança aumenta à medida que o número de interesses em comum aumenta. A medição ocorre quando o nó avaliado tem, pelo menos, o interesse em saúde, implicando um valor mínimo de confiança sempre maior que 0.

Um nó x que encontra um nó y mede sua confiança acerca dos interesses em comum que possuem entre si, T^I_{xy}. Ela equivale à razão entre seus interesses em comum, $I_x \cap I_y$, e os interesses do nó avaliador, I_x. Dessa forma, quantifica-se a similaridade entre os interesses de ambos os nós, onde os interesses do nó avaliador são a referência. A T^I_{xy} é obtida pela Equação 1, baseada no trabalho de [Bao and Chen 2012]. Seus valores variam na faixa $[0, 1]$ (Equação 2), ressaltando-se que a medição da confiança ocorre apenas se o nó y possuir interesse em saúde.

$$T^I_{xy} = \frac{|I_x \cap I_y|}{|I_x|} \quad (1) \qquad T^I_{xy} = \begin{cases} 0, & se\ \ I_y \not\supset \{saúde\} \\ ]0,1[, & se\ \ I_x \cap I_y \neq 0\ \ e\ \ I_x \neq I_y\ e\ \{saúde\} \subset I_x \cap I_y \\ 1, & se\ \ I_x = I_y\ \ e\ \ \{saúde\} \subset I_x \cap I_y \end{cases} \quad (2)$$

A confiança do nó x em relação à competência do nó y (T^{Skill}_{xy}) é computada pela verificação da similaridade da sua competência em relação a do *médico*, considerada pelo STEALTH a mais elevada em saúde e estabelecida a partir da taxonomia de competências (T), baseada em [Carminati et al. 2016] e [Mohammad and Hirst 2012]. A T^{Skill}_{xy} equivale à distância (D_T) da competência s_y em relação à competência de *médico* dentro dessa taxonomia. Neste trabalho, assume-se que há uma função distância $D_T(S)$, que recebe como entrada uma competência S do nó avaliado e retorna um valor que indica a proximidade da competência informada com a de *médico* na taxonomia T. A D_T é mensurada com base na medida estabelecida por [Wu and Palmer 1994] e, posteriormente, revisada por [Resnik 1999]. Os valores possíveis de T^{Skill}_{xy} variam na faixa $[0, 1]$ (Equação 4).

$$T^{Skill}_{xy} = Sim_y \quad (3) \qquad T^{Skill}_{xy} = \begin{cases} 0, & se\ s_y\ \in \{outras\} \\ ]0,1[, & se\ s_y\ \notin \{outras, médico\} \\ 1, & se\ s_y\ \in \{médico\} \end{cases} \quad (4)$$

A confiança do nó x sobre o nó y, T_{xy}, é 0 se $T^I_{xy} = 0$. Caso contrário, corresponde à soma da confiança relacionada aos seus interesses em comum, T^I_{xy}, com aquela oriunda da competência que nó y possui, T^{Skill}_{xy} (Equação 5). Para valores de $T^I_{xy} > 0$, os valores de T_{xy} variam na faixa $]0, 1]$, conforme os valores de T^I_{xy} (Equação 2) e T^{Skill}_{xy} (Equação 4).

$$T_{xy} = \frac{T^I_{xy} + T^{Skill}_{xy}}{2} \quad (5)$$

Por exemplo, considere que um nó x avalia a confiança sobre um nó y, T_{xy}, cuja competência atribuída é de *cuidador* e ambos possuem um único interesse - *saúde*. Empregando-se uma taxonomia de competências em saúde baseada em [Carminati et al. 2016] e [Mohammad and Hirst 2012] e o interesse descrito, o resultado da T^{Skill}_{xy} será equivalente à similaridade, Sim_s, da competência do nó y, s_y. A $Sim_s(s_y)$, correspondente a $Sim_s(cuidador)$, terá o valor 0,28, ou seja, $T^{Skill}_{xy} = 0{,}28$. A T^I_{xy} (Equação 1), terá o valor 1, visto que o nó avaliador e avaliado possuem apenas *saúde* como interesse comum, único interesse de ambos. Logo, aplica-se a Equação 5 e obtém-se a $T_{xy} = 0{,}64$. No entanto, caso o nó y tenha a competência *outras*, $Sim_s = 0$, ou seja, ele

não possui qualquer competência em atividades de saúde, $T_{xy}^{Skill} = 0$. Como $T_{xy}^{I} = 1$, o valor da confiança de x em y, T_{xy}, será de 0,5.

4.2. Módulo Gestão de Eventos Críticos

Neste módulo, o componente *Monitoração* verifica a condição de saúde da pessoa ao receber seu status de saúde. Um dispositivo médico que a pessoa porta junto ao seu corpo é responsável por identificar um evento crítico e informar ao STEALTH. O componente *Dados Sensíveis* obtém os dados sensíveis da pessoa em situação emergencial e garante sua disseminação apenas nessas condições. O componente *Disponibilidade* verifica a pessoa adequada para se disseminar os dados sensíveis, garantindo que seja aquela com a competência mais elevada em saúde. O componente *Disseminação* coordena a disseminação dos dados sensíveis ao receber esses dados e a identificação da pessoa adequada. Essa disseminação ocorre por meio de mensagens de alerta somente às pessoas que pertençam à comunidade de saúde do nó e na medida de sua competência em saúde.

Algoritmo 2: Gestão de Eventos Críticos

```
1  for each node d ∈ D do
2      procedure HANDLEEMERGENCYEVENT( )
3          neighid ← GetHigherScoreNeighbor( )
4          neighskill ← GetNeighborSkill (neighid)
5          criticaldata ← GetCriticalData (neighskill)
6          SendAlert(neighid, criticaldata)
7          SendStopAnnounce( )
8      end procedure
9      procedure RECEIVEALERT (id, criticaldata)
10         SendAckAlert( )
11     end procedure
12     procedure RECEIVESTOPANNOUCE (Id)
13         NeighborList ← RemoveNeighbor(Id)
14     end procedure
```

Os nós pertencentes às CoI formadas com interesse em saúde apoiam os nós que representam as pessoas em situação emergencial, como descrito no Algoritmo 2. Desta forma, ao ocorrer um evento crítico com um determinado nó, ele verifica o nó vizinho com a confiança mais elevada (*l*.2) e obtém o dado sensível apropriado (*l*.3-4). Em seguida, envia uma mensagem de alerta para o nó selecionado (*l*.5) com seu dado sensível. Além disso, ele anuncia por *broadcast* a interrupção de sua operação (*l*.6). Ao receber uma mensagem de alerta, o nó confirma seu recebimento (*l*.9). Quando um nó percebe que outro nó anuncia a interrupção de sua operação, ele exclui esse nó da sua lista de vizinhos (*l*.11). Isso impede que um nó em situação emergencial venha a ser selecionado para receber dados sensíveis de outros nós.

4.3. Funcionamento

Esta seção ilustra o funcionamento do sistema STEALTH em um ambiente urbano e demonstra sua contribuição na disseminação controlada dos dados sensíveis de uma pessoa em situação emergencial, a fim de que ela possa receber um primeiro atendimento. Considere uma área urbana onde seis pessoas deslocam-se a pé pelas ruas: uma enfermeira, um paciente, um executivo, um policial, um bombeiro e um médico. Cada

uma delas possui uma profissão ou habilidade para executar determinadas tarefas no seu dia-a-dia. O paciente é uma pessoa que eventualmente precisa de atendimento emergencial. O médicos são profissionais que detém o maior conhecimento em saúde, enquanto um policial, por exemplo, possui condições de prestar primeiros socorros.

Todas essas pessoas possuem um interesse em comum em saúde e não mantêm relações entre si. A enfermeira, o policial, o bombeiro e o médico possuem interesse em saúde por conta da sua profissão. O executivo se interessa por saúde, por exemplo, a fim de ajudar pessoas necessitadas. As pessoas portam dispositivos móvel, *smartphones*, para se conectarem em redes. O STEALTH roda nesses *smartphones*, estando configurado para operar. Além disso, o paciente porta um dispositivo junto ao seu corpo para verificar sua pressão arterial, por exemplo, e reportar a um aplicativo instalado em seu *smartpphone*. Esse aplicativo comunica-se com o STEALTH para informar os valores de pressão arterial medidos e sua normalidade para esse paciente.

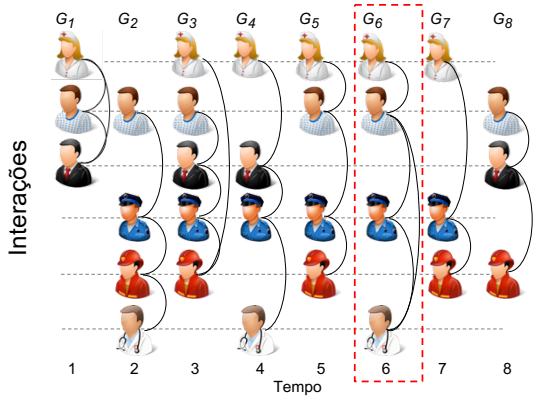

Figura 2. Interações no tempo

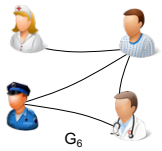

Figura 3. Grafo da rede em t_6

Tabela 1. Medição da confiança

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

As interações entre pessoas ao longo do tempo $t = \{1, 2, ..., 8\}$, resultantes da sua mobilidade, são ilustradas na Figura 2, quando seus dispositivos estabelecem redes *ad hoc* para trocarem dados entre si. Assume-se que o paciente entra em situação emergencial em t_6. Nesse instante, o seu dispositivo interage com os de outras pessoas, como ilustra o grafo G_6 (Figura 3), e cada um deles forma sua própria comunidade de saúde. O dispositivo do paciente mede a confiança dos demais e os insere na sua lista de vizinhos com os valores de confiança exibidos na Tabela 1. Ao ocorrer o evento crítico, o STEALTH rodando no *smartphone* do paciente identifica o médico como a pessoa com o maior valor de confiança na sua comunidade de saúde e, assim, dissemina seus dados sensíveis a ele.

5. Avaliação do STEALTH

Esta seção apresenta a metodologia de avaliação aplicada para analisar o desempenho do sistema STEALTH. Ele foi implementado no simulador NS-3, versão 3.28, instalado no sistema operacional Debian, versão 9.1. O cenário de uso do STEALTH é composto por 100 dispositivos (nós) móveis representando o comportamento de movimentação de usuários em um ambiente urbano. Esses usuários portam equipamentos sem fio - *smartphones* - e deslocam-se em uma área de 400m x 430m da Cidade de Estocolmo (Suécia) com velocidades entre 0,5m/s e 2,0m/s [Helgason et al. 2014]. Os nós estabelecem redes *ad hoc* através de transmissão usando o padrão IEEE 802.11a e o protocolo de

transporte UDP. O raio de alcance dos nós é de 50m, para permitir a formação de comunidades de interesses ao seu redor e na medida em que se movimentam. Além disso, eles são configurados randomicamente com aspectos sociais, isto é, a cada rodada de simulação eles possuem uma única competência e um conjunto de interesses, com um mínimo de um e máximo cinco interesses. A Tabela 2 lista a distribuição dos aspectos. A classe *node* do NS-3 foi modificada para incorporar os atributos sociais de confiança aos nós.

Tabela 2. Distribuição dos aspectos sociais atribuídos aos nós

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

Tabela 3. Métricas de avaliação de desempenho

Descrição	**Equação**
Número Médio de Comunidades de Interesse em Saúde (N_C) computa a média do somatório de todas as comunidades de saúde formadas por um nó ao longo de todas as execuções (N_S).	$N_C = \sum_{i=1}^{N_S} \sum_{j=1}^{t_s} \frac{C_{xy}}{t_s \times N_S}$
Taxa de Sucesso no Acesso aos Dados (TS) indica a taxa de sucesso na entrega dos dados à pessoa adequada, sendo a razão entre o total de acessos com sucesso aos dados sensíveis (A_{Sucess}) e o total de vezes em que os dados sensíveis estiveram disponíveis para acesso (A_{Disp}).	$TS = \frac{A_{Success}}{A_{Disp}} \times 100$
Taxa de Sucesso no Acesso aos Dados por Competência (TS_{Skill}) equivale à métrica TS computada pela razão entre o acesso de cada competência individualmente (A_{Skill}) e o total de acessos com sucesso ($A_{Success}$), diante das competências vistas na Tabela 2.	$TS_{Skill} = \frac{A_{Skill}}{A_{Success}} \times 100$
Taxa de Dados Não Acessados (TN_a) corresponde ao porcentual de dados que não foram acessados nas situações emergenciais.	$TN_a = 100 - TS$
Tempo Médio de Acesso aos Dados Sensíveis (MTA) computa o tempo médio de acesso aos dados sensíveis de um determinado nó para todas as simulações realizadas. Ele corresponde ao somatório da razão entre as diferenças entre o momento em que os dados foram acessados (t_r) e o momento da sua disseminação (t_s) e o total de execuções (N_S).	$MTA = \sum_{i=1}^{N_S} \frac{ta_i - td_i}{N_S}$

Os nós em simulação foram enumerados de 1 a 100 e a avaliação do comportamento do sistema foi realizada através de três deles - 37, 52 e 70. Eles apresentam a mesma configuração em todas as simulações realizadas, enquanto os demais nós são configurados randomicamente a cada rodada de simulação. O tempo de simulação é de 900s e os nós selecionados entram em situação emergencial apenas aos 890s de simulação, permitindo observar seus comportamentos em grande parte da simulação. Assume-se que todos os nós apresentam um comportamento honesto e há mecanismos de segurança para validação das suas identidades e proteção na transmissão dos dados. Assume-se, também, que a identificação de um evento crítico acontece por um dispositivo que as pessoas portam junto ao seu corpo, e que informa ao STEALTH. Os resultados exibidos correspondem à média de 35 simulações e um intervalo de confiança de 95%. As métricas empregadas na avaliação de desempenho do sistema STEALTH são detalhadas na Tabela 3 e foram definidas especificamente para essa finalidade. A análise da disponibilidade dos dados provida pelo STEALTH leva em conta a evolução das comunidades de inte-

resse em saúde ao longo do tempo e a métrica N_C. A análise da confiabilidade do serviço de disseminação dos dados é mensurada através das métricas TS, TN_a, MTA e TS_{Skill}.

5.1. Disponibilidade

A análise da disponibilidade verifica a prontidão do sistema para disseminar com sucesso e de maneira controlada os dados sensíveis das pessoas em situação emergencial. A Figura 4 demonstra esse comportamento ao sintetizar o número médio de comunidades de interesse em saúde (N_C) estabelecidas ao longo do tempo. O nó 37 estabeleceu, em média, 12 comunidades distintas ao longo de cada rodada de simulação. Isso caracteriza a dinamicidade das redes locais estabelecidas, especialmente da sua topologia. A mobilidade dos nós através de caminhos distintos, associada aos aspectos sociais - interesses - atribuídos a eles, impactou na formação dessas comunidades. O nó 70 estabeleceu uma quantidade ainda maior de comunidades, $N_C = 28$, o que aumenta a disponibilidade para disseminação de seus dados em situações emergenciais.

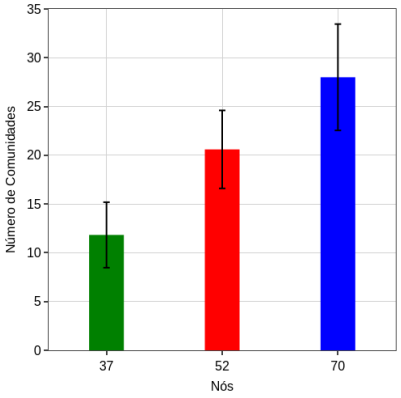

Figura 4. Número médio de comunidades

A Figura 5 apresenta os gráficos da dinamicidade das comunidades de saúde dos nós 37, 52 e 70 estabelecidas pelo STEALTH e seu tamanho ao longo do tempo em uma rodada específica de simulação. Os resultados mostram que o STEALTH acompanhou a dinamicidade das redes locais criadas, especialmente diante da mobilidade dos nós. Ele conseguiu verificar as mudanças nas vizinhanças dos nós e ajustou suas comunidades de interesse em saúde, a fim de mantê-las atualizadas. O nó 37 manteve comunidades de saúde em 63,93% do tempo de simulação em que esteve ativo. Durante esse período de tempo, o sistema esteve pronto para disseminar seus dados sensíveis, pois identificou nós que poderiam auxiliá-lo. Porém, ao entrar em situação emergencial, aos 890s, não havia vizinhos ao seu redor, não estabelecendo assim uma comunidade. Logo, não disseminou seus dados sensíveis. O nó 52 manteve um comportamento distinto e estabeleceu comunidades por 97,22% do tempo, até que entrou em situação emergencial. Neste instante, conforme representado na figura, ele possuía sete vizinhos, mas dois deles pertenciam à sua comunidade de saúde, o nó 13 e 41. Como o nó 13 possuía a competência mais elevada em saúde, cuidador, o nó 52 disseminou seus dados para ele. Por fim, constata-se que o nó 70 foi aquele que manteve comunidades de saúde por mais tempo, 98,8%. Ao entrar em situação emergencial, ele tinha 4 vizinhos, mas apenas um deles com interesse em saúde - nó 96, para o qual seus dados sensíveis foram disseminados. Esse comportamento é corroborado pela Figura 4, onde o nó 37 estabeleceu o menor N_C, 12, enquanto o nó 70 apresentou o maior valor entre todos os nós, 28.

5.2. Confiabilidade

A análise da confiabilidade verifica a capacidade do sistema em disseminar com sucesso e de maneira controlada os dados sensíveis das pessoas em situação emergencial. O comportamento dos nós selecionados - 37, 52 e 70 - demonstra essa situação. O nó 52 foi bem-sucedido (TS) em 80% das situações emergenciais ao longo das simulações,

quando seus dados disseminados foram acessados com sucesso. O agrupamento dos nós em comunidades de interesse impacta diretamente na TS, pois garante a disseminação dos dados sensíveis de um nó em situação emergencial apenas a um outro nó dentre aqueles que pertençam à sua comunidade de interesse em saúde. A importância do emprego das CoI para controlar a disseminação dos dados sensíveis dos nós é constatada pelos dados não acessados (TNa). Em 68,57% das situações emergenciais, os dados sensíveis do nó 37 não foram acessados por outros nós. Isso ocorreu devido à falta de uma comunidade de saúde durante as situações emergenciais ou a sua conexão com os outros nós foi interrompida por conta da sua mobilidade. O nó 70 não foi tão bem-sucedido como o nó 52, apesar de ter estabelecido um maior número de comunidades, como visto na Figura 4. Isso se deve ao instante em que ele entrou em situação emergencial, quando não existia vizinhos na sua comunidade de saúde para os quais pudesse disseminar seus dados.

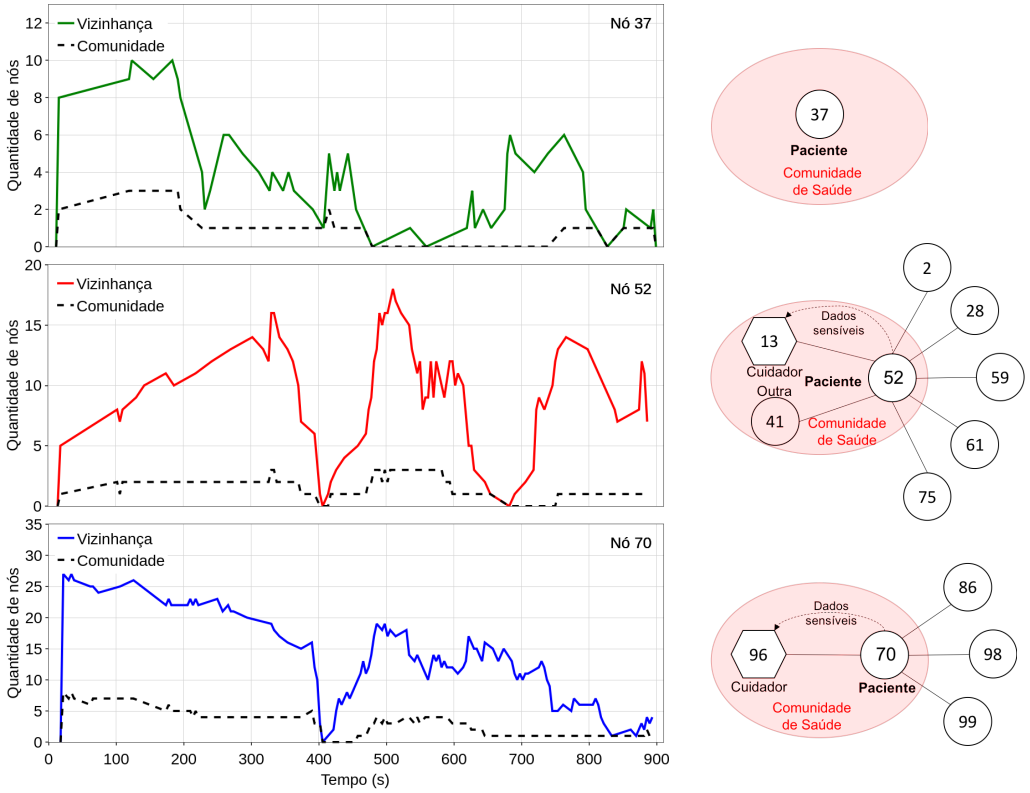

Figura 5. Dinamicidade da comunidade de saúde e tamanho ao longo do tempo

O tempo médio de acesso aos dados sensíveis (MTA) representa o custo em relação ao tempo para que os dados sensíveis disseminados por um nó em situação emergencial sejam acessados. Ele é impactado diretamente pela dinamicidade das redes locais estabelecidas, cuja topologia se modifica com a mobilidade dos nós. A Tabela 4 sumariza os resultados obtidos, onde se constata que eles atendem à latência máxima de 125ms estabelecida pela IEEE para entrega de alertas médicos [Association et al. 2012]. Enquanto os dados sensíveis do nó 52 foram acessados mais rapidamente que os dos demais ($MTA < 1ms$), os do nó 37 foram acessados, em média, após 95ms de sua disseminação. O emprego das comunidades de interesse contribui para o processo de tomada de decisão de verificação do nó adequado e reduz o tempo de acesso aos dados disseminados.

Tabela 4. 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 5. Controle de disseminação

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

Os dados sensíveis dos nós em situação emergencial foram disseminados somente aos nós pertencentes às suas comunidades de saúde e diante das competências previstas na Tabela 2. O emprego de interesses e competências, associados à formação de comunidades de interesse, além de possibilitar avaliar a confiança dos nós, permite controlar a disseminação dos seus dados sensíveis. Isso ocorre em uma condição *Zero-Knowledge*, visto que as comunidades de saúde são recriadas periodicamente e desconsideram interações anteriores entre os nós da rede. O sucesso no acesso aos dados por competência (TS_{Skill}) indica a prevalência das competências nas comunidades estabelecidas, como se observa na Tabela 5, onde 21,48% do total de dados disseminados foram para nós com outras competências. 30,03% desses dados foram acessados por nós com competência de *médico*. Isso indica que em 30,03% das situações emergenciais, o STEALTH detectou a presença de pelo menos um médico na comunidade de saúde disponível.

6. Conclusão

Este trabalho apresentou STEALTH, um sistema para disseminar dados sensíveis de saúde de maneira controlada em redes locais dinâmicas sem fio. Ele estabelece agrupamentos virtuais levando em conta comunidades de interesses e aplica confiança social a fim de permitir os dispositivos decidirem de maneira robusta num dado momento sobre a disseminação de dados em situação emergencial. Simulações avaliaram a eficácia do STEALTH e os resultados mostraram sua capacidade de assegurar a disseminação de dados sensíveis. O STEALTH obteve uma confiabilidade de até 80% no acesso aos dados disseminados e uma latência máxima de 95ms, e uma disponibilidade de até 98,8%. Como trabalhos futuros, serão investigadas questões associadas a unicidade dos identificadores dos nós e à autenticação mútua. Também será analisada a confiabilidade do sistema nas tomadas de decisões diante de múltiplas situações de emergência simultaneamente, e na presença de comportamento malicioso.

Agradecimento

Os autores agradecem o apoio do CNPq no projeto Universal No. 436649/2018-7.

Referências

Al-Hamadi, H. and Chen, R. (2017). Trust-Based Decision Making for Health IoT Systems. *IEEE Internet of Things Journal*, 4(5):1408–1419.

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.

Bao, F. and Chen, R. (2012). Trust Management for the Internet of Things and Its Application to Service Composition. In *WoWMoM 2012*, pages 1–6.

Bao, F., Chen, R., and Guo, J. (2013). Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems. In *ISADS 2013*, pages 1–7.

Carminati, B., Ferrari, E., and Guglielmi, M. (2016). Detection of Unspecified Emergencies for Controlled Information Sharing. *IEEE TDSC*, 13(6):630–643.

Cho, J.-H., Chan, K., and Adali, S. (2015). A Survey on Trust Modeling. *ACM Computing Surveys (CSUR)*, 48(2):28.

Coscia, M., Giannotti, F., and Pedreschi, D. (2011). A classification for community discovery methods in complex networks. *Statistical Analysis and Data Mining*, 4(5):512–546.

Feige, U., Fiat, A., and Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of cryptology*, 1(2):77–94.

Garyfalos, A. and Almeroth, K. C. (2008). Coupons: A Multilevel Incentive Scheme for Information Dissemination in Mobile Networks. *IEEE Transactions on Mobile Computing*, 7(6):792–804.

Helgason, Ó., Kouyoumdjieva, S. T., and Karlsson, G. (2014). Opportunistic Communication and Human Mobility. *IEEE Transactions on Mobile Computing*, 13(7):1597–1610.

Latré, B., Braem, B., Moerman, I., Blondia, C., and Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks*, 17(1):1–18.

Lima, M. N., dos Santos, A. L., and Pujolle, G. (2009). A Survey of Survivability in Mobile Ad Hoc Networks. *IEEE Communications Surveys and Tutorials*, 11(1):66–77.

Mohammad, S. and Hirst, G. (2012). Distributional Measures of Semantic Distance: A Survey. *CoRR*, abs/1203.1858.

Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., and Jamalipour, A. (2014). Wireless Body Area Networks: A Survey. *IEEE Communications surveys & tutorials*, 16(3):1658–1686.

Nogueira, M., Mannes, E., and Santos, A. (2012). Serviços Confiáveis em MANETs Baseado em Sistema de Quórum Tolerante à Má-conduta. In *Anais do XXX SBRC*, pages 305–318. SBC.

Resnik, P. (1999). Semantic Similarity in a Taxonomy: An Information-Based Measure and its Application to Problems of Ambiguity in Natural Language. *JAIR*, 11:95–130.

Rossetti, G. and Cazabet, R. (2018). Community Discovery in Dynamic Networks: a Survey. *ACM Computing Surveys (CSUR)*, 51(2):35.

Silverstein, J. (2019). Hundreds of millions of Facebook user records were exposed on Amazon cloud server. https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/. [Online]. Acessado em Abr. 2019.

Truong, N. B., Lee, H., Askwith, B., and Lee, G. M. (2017). Toward a Trust Evaluation Mechanism in the Social Internet of Things. *Sensors*, 17(6):1346.

Vasilomanolakis, E., Wolf, J. H., Böck, L., Karuppayah, S., and Mühlhäuser, M. (2017). I Trust my Zombies: A Trust-enabled Botnet. *CoRR*, abs/1712.03713.

Vivekavardhana, R. B. and Sudhindra, K. R. (2014). Survey of Trust Models in Wireless Sensor Networks. *IJAIST*, 31(31).

Williams, M., Nurse, J. R., and Creese, S. (2016). The Perfect Storm: The Privacy Paradox and the Internet-of-Things. In *ARES 2016*, pages 644–652. IEEE.

Wu, Z. and Palmer, M. (1994). Verbs semantics and lexical selection. In *ACM Proceedings of the 32nd annual meeting on Association for Computational Linguistics*, pages 133–138.