Comunicação Robusta para Disseminação de Eventos Dinâmicos em Redes Táticas Apoiada em Grafos Temporais

Diego Milhomem Schmitt[1], **Marcos Aurélio Carrero**[1], **Aldri Santos**[1]

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR
Caixa Postal 19.081 – 81.531.980 – Curitiba – PR – Brasil

{dmschmitt, macarrero, aldri}@inf.ufpr.br

Abstract. *Tactical Networks act in the diffusion of actions of command and control, frequent events disseminated among the diverse members of the network to carry out coordinated actions. Composed of devices with heterogeneous computational resources where the intermittent connections, scalability and application in environments without infrastructure characterize a dynamic structure susceptible to communication failures over time, preventing the realization of coordination tasks. This paper presents a mechanism to support the dissemination of events in Tactical Networks in order to guarantee a greater robustness in the synchronization of the actions of command and control in urban environments. The mechanism is based on Local Bridges of graphs to identify and select nodes in conditions to act in the dissemination of events according to the local dynamics of the network. Results show the robustness of the proposed mechanism to deal with the dynamicity of the structure and the devices, providing efficiency in the diffusion of actions in urban scenarios.*

Resumo. *As Redes Táticas atuam na difusão de ações de comando e controle, eventos frequentes disseminados entre os diversos integrantes da rede para execução de ações coordenadas. Compostas por dispositivos com recursos computacionais heterogêneos onde a intermitência das conexões, a escalabilidade e a aplicação em ambientes sem infraestrutura caracterizam uma estrutura dinâmica susceptível a falhas de comunicação ao longo do tempo, prejudicando a realização de atividades coordenadas. Este trabalho apresenta um mecanismo para apoiar a disseminação de eventos em Redes Táticas de modo a garantir uma maior robustez na sincronização das ações de comando e controle em ambientes urbanos. O mecanismo baseia-se em Pontes Locais de grafos para identificar e selecionar nós em condições de atuar na disseminação de eventos de acordo com a dinâmica local da rede. Resultados mostram a robustez do mecanismo para lidar com a dinamicidade da estrutura e dos dispositivos provendo eficiência na difusão de ações em cenários urbanos.*

1. Introdução

As Redes Táticas, formadas por um conjunto de dispositivos heterogêneos móveis que se comunicam por tecnologias sem fio, são empregadas em contextos desafiadores para comunicação em rede. A falta de infraestrutura impacta na efetividade da rede, o que limita sua operação em situações de desastres naturais, emergências urbanas e guerras, impactando na atuação rápida de órgãos de Segurança Pública [Verma et al. 2017]. Em ambientes urbanos, a difusão de eventos de comando e controle para coordenar ações

sincronizadas entre agentes de segurança, médicos e socorristas fica prejudicada principalmente pela intermitência de conexões, mobilidade dos dispositivos, obstáculos naturais, limitação de banda e a frequente troca de mensagens. Soluções dedicadas para esse contexto são necessárias para garantir a disseminação de eventos de maneira eficaz, minimizando o impacto das limitações de rede na atuação das entidades de Segurança Pública.

A dinâmica da infraestrutura da rede para disseminação de eventos críticos impõe mudanças em sua topologia. Soluções tradicionais de gerenciamento de rede cliente-servidor e *P2P* (*Peer-to-Peer*) falham ao lidar com a dinâmica da infraestrutura e intermitência de conexões [Casini et al. 2016]. Os eventos disseminados precisam ser atendidos por essa infraestrutura desorganizada, considerando restrições de tempo, cobertura de rede e localização. As redes *Ad Hoc* permitem o uso oportunístico das conexões em rede, possibilitando a comunicação numa rede dinâmica. A complexidade de situações críticas exige um serviço de disseminação de informação adaptativo e robusto [Lima et al. 2009] para garantir a confiabilidade das aplicações oferecidas pela rede. Os sistemas de recomendação associam os eventos com as relações entre os indivíduos, o comportamento coletivo, a localização e período onde ocorrem. Contudo, essas redes não são voltadas para ambientes com intensa intermitência onde há necessidade de robustez da rede.

A dinâmica nas Redes Táticas compreende duas perspectivas [Zhang et al. 2016]. A primeira abrange o comportamento dinâmico das entidades ou dispositivos, isto é, na mobilidade e na forma como trocam mensagens ou eventos. A segunda trata das alterações da topologia ao longo do tempo. A variação nas quantidades de dispositivos, conexões e difusão de informação caracterizam uma infraestrutura dinâmica, influenciando na escalabilidade da rede. A difusão de informação sofre com a dinâmica dos dispositivos e da estrutura, particularmente se a quantidade de dispositivos e eventos cresce. Logo, a disseminação de eventos em redes dinâmicas que necessitam executar ações com sincronismo se mantém um desafio, como as Redes Táticas empregadas em contextos Militares.

A dinâmica dos dispositivos é explorada por técnicas inspiradas nos modelos *Broadcast e P2P*. Entretanto, falham ao lidar com a mobilidade, escalabilidade e intermitência de conexões entre os dispositivos. Os trabalhos de [Holzhauer et al. 2016, Casini et al. 2016] expõem a dificuldade na comunicação ao considerar apenas o comportamento individual dos dispositivos numa rede dinâmica. É importante destacar que o comportamento dinâmico da infraestrutura influencia na comunicação [Mercer et al. 2016, Gao 2016]. Ao considerar uma infraestrutura global, existe a dificuldade em lidar com a dinâmica e o custo de manutenção. Por outro lado, partes da rede exercem influência na comunicação, cooperando para robustez nas comunicações e eficiência computacional. A abordagem proposta por [Macker 2016] ressalta a importância das estruturas locais no contexto de redes dinâmicas. As Pontes Locais são uma propriedade de grafos inferida inicialmente em redes sociais [Hwang et al. 2006]. Elas auxiliam em mecanismos de roteamento, eleição de líderes e mitigação falhas, uma vez que necessitam apenas de informação local da rede para identificar importantes partes estruturais. A fim de diminuir a complexidade computacional e de comunicação, o uso de Pontes Locais tem sido aplicado para identificar estruturas de uma rede de comunicação que possuam maior importância e robustez para Redes Táticas [Macker 2016].

Este trabalho propõe o mecanismo *SinERT* (**Sin**cronização Robusta de **E**ventos em **R**edes **T**áticas) para apoiar a disseminação e sincronização de eventos em Redes

Táticas, de modo que ações de comando e controle possam ser realizadas de maneira consistente e coordenadas ao longo do tempo. O mecanismo emprega a técnica *Pinning* [Li and Yang 2017] que possibilita a seleção de "pontos" para atuar no controle, contribuindo para a sincronização de uma rede. Isso permite que uma característica desejada para se manter os contatos entre os nós seja empregada para sincronização de eventos diante da mobilidade dos usuários em ambientes desorganizados e com restrições de mobilidade. Quanto mais densa a rede maior a possibilidade de sincronização de evento e à medida que a rede torna-se esparsa, há uma perda de comunicação entre os nós. Assume-se neste trabalho que o mecanismo incorpora a existência de segurança na comunicação dos dados. O mecanismo foi avaliado no simulador ONE de modo a mostrar a sua eficiência e eficácia em garantir a disseminação robusta de eventos de modo síncrono.

O restante do artigo está organizado da seguinte forma: a Seção 2 discute os trabalhos relacionados. A Seção 3 brevemente apresenta as questões sobre a disseminação de eventos em Redes Táticas. A Seção 4 descreve o mecanismo *SinERT* e detalha os seus componentes e funções. A Seção 5 apresenta uma avaliação do mecanismo e os resultados obtidos. A Seção 6 apresenta as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

A literatura apresenta vários mecanismos e técnicas para reduzir falhas decorrentes de conexões intermitentes e falhas de roteamento, de modo a garantir a robustez da comunicação para disseminação de eventos dinâmicos em Redes Táticas. Algumas técnicas se baseiam apenas na dinâmica dos dispositivos como a *Broadcast*, utilizada para tratar a mobilidade, redução no atraso de entrega de mensagens e o aproveitamento de banda. O trabalho proposto por [Grönkvist et al. 2016] utiliza o *Broadcast Cooperativo* para transmissão e retransmissão de pacotes com base num *framework* distribuído onde cada mensagem pode ser retransmitida de acordo com um agendamento. Embora seja eficiente para disseminar informação, não explora um ambiente onde há disrupções da rede, intermitência de conexões e exige que todos os nós trabalhem da mesma maneira. Outras propostas aplicam técnicas modernas como *Peer-to-peer* (P2P) para lidar com a intermitência das conexões entre os nós e sistemas de recomendação para disseminar eventos a indivíduos ou grupo de indivíduos que participam de uma rede social [Ogundele et al. 2017], [Purushotham and Kuo 2016].

A estratégia usada por BANDIT [Holzhauer et al. 2016] descreve um protótipo de serviço P2P de gerenciamento de informação distribuída para se adequar aos requisitos de conexões intermitentes, frequentes entrada e saída de dispositivos da rede, escalabilidade e ponto único de falha. O BANDIT aplica uma técnica para apoiar a disseminação de informação para quem de fato deve receber ou quer receber. Embora não utilize nenhuma informação sobre a estrutura da rede nem das relações entre as entidades para disseminar informação, precisa manter uma topologia para alcançar a gerência proposta.

Em contrapartida, outras técnicas utilizadas pelas Redes Táticas fazem uso da topologia e do relacionamento das entidades da rede para garantir a robustez nas comunicações. Por exemplo, os trabalhos propostos por [Mercer et al. 2016, Gao 2016] apresentam técnicas distintas para apoiar mudanças na dinâmica da infraestrutura e comunicação em rede. [Mercer et al. 2016] propõem a criação de grupos afins com estruturas em árvore para cada escopo de grupo com o objetivo de restringir a comunicação dentro do escopo

necessário. Contudo, a manutenção dessas estruturas torna-se inviável dentro de uma dinâmica mais desorganizada. [Gao 2016] propõe a predição de contatos para aumentar o desempenho nas comunicações entre os dispositivos. Embora relevante para um cenário onde haja uma dinâmica nas conexões, a necessidade do conhecimento da topologia inteira para estimar futuras conexões torna-se um limitador para seu uso em Redes Táticas, haja vista o custo e viabilidade de manter uma estrutura dinâmica.

A temporalidade da informação, a dinâmica do comportamento em grupo e a localização dos eventos nas Redes Sociais Baseadas em Eventos (EBSN, Event Based Social Networks) e Redes Sociais Baseadas em Localidade (LBSN, Local Bases Social Networks) [Ogundele et al. 2017] são características presentes nas Redes Táticas. Neste contexto, [Macker 2016] destaca a importância de observar as estruturas locais formadas numa rede, e como o relacionamento entre as entidades envolvidas pode influenciar na comunicação. Ele propôs o uso de Pontes Locais para identificar as entidades fundamentais para suportar a comunicação dentro de uma estrutura, bem como trouxe a aplicação de uma medida que necessita de informação restrita de parte da rede, ressaltando sua aplicabilidade num cenário de rede dinâmica.

3. Visão Geral da Disseminação de Eventos em Redes Dinâmicas

Esta seção apresenta os conceitos utilizados para compreender e fundamentar a proposta de garantia da disseminação de eventos em Redes Táticas. As redes móveis sem fio não estruturadas são preferencialmente destinadas para situações onde a infraestrutura de comunicação é precária ou inexistente. Situações de desastres naturais, emergências urbanas e guerras exemplificam cenários críticos de aplicação para essas redes [Reina et al. 2014]. Os sistemas complexos, como redes sociais, redes de transportes e redes de telecomunicação, mostram que as interações entre os elementos da rede estão relacionados com a topologia e suas as propriedades, sendo possível inferir sobre o comportamento das conexões entre os elementos [Martínez et al. 2017]. A teoria de controle aplicado a redes complexas mostra como exercer influência e alcançar sincronização a partir da seleção de indivíduos da rede [Li and Yang 2017].

A disseminação de eventos normalmente ocorre em redes baseadas em eventos. Exemplos dessas redes consistem nas Redes Sociais Baseadas em Eventos (EBSN)e Redes Sociais Baseadas em Localidade (LBSN) [Ogundele et al. 2017]. As principais características das ESBN compreendem criar, promover e compartilhar eventos com qualquer usuário da rede. Já nas LBSN os usuários compartilham atividades e localização. Ambas contribuem para organização, coordenação e participação de usuários em eventos promovendo informações detalhadas e consistentes para os usuários [Purushotham and Kuo 2016]. Nesse cenário, os sistemas de recomendação são amplamente empregados para apoiar os usuários dessas redes a encontrarem eventos ou locais de interesse. Um evento normalmente tem uma duração definida e também apresenta sazonalidade, por exemplo, um determinado dia da semana tem maior importância que os outros. Assim, a temporalidade é um requisito fundamental ao se recomendar um evento para um determinado grupo de usuários. Ainda, o aspecto social das relações entre os usuários ou indivíduos, comportamento em grupo e individual, em uma rede servem para filtrar e recomendar eventos com base nessas relações, aumentando a qualidade das recomendações. A localização é outro ponto ressaltado nesse contexto, usada para estabelecer preferências de eventos com base na proximidade e locais anteriormente visitados.

Todos esses aspectos dos eventos são importantes ao se considerar a garantia da disseminação em redes dinâmicas. Embora as Redes Táticas não sejam propriamente ditas redes sociais e estejam mais próximas de redes com caráter profissional, ainda assim trazem consigo as mesmas características de temporalidade, relações sociais e localização. Similarmente, esse comportamento também é observado em outros padrões de disseminação de informação como Limiar (*Threshold*), Cascata e Epidêmico [Zhang et al. 2016]. A dinâmica da estrutura ou topologia se relaciona com a localização e com as relações entre as entidades de uma rede ao longo do tempo. Já a dinâmica dos dispositivos está mais voltada para o comportamento individual e podem ou não estar relacionados com o grupo no qual está inserido. Logo, a dinâmica da estrutura possui maior interesse ao se considerar o contexto da disseminação de eventos, sendo também a essência desse trabalho.

3.1. Dinâmica das Conexões

Os estudos sobre predição de link fundamentam que a interação entre duas entidades de uma rede apresentam maiores chances de acontecer caso evidenciem características similares [Martínez et al. 2017]. O conceito de similaridade é muito amplo e varia de acordo com a abordagem da rede. Normalmente está relacionado à quantidade de caminhos ou conexões existentes entre duas entidades. A predição de link vem sendo aplicada em redes sociais, redes de entretenimento aprimoradas por sistemas de recomendação, pesquisas biológicas para prever interação entre proteínas e para prever grupos de colaboração científica. O trabalho de [Martínez et al. 2017] propõe uma taxonomia para classificar a predição de link composta por quatro principais categorias divididas em similaridade, probabilidade, algoritmos e procedimentos. Logo, esses estudos mostram a relevância do comportamento individual e coletivo das entidades de uma rede.

3.2. Controle Aplicado na Disseminação em Redes Complexas

As abordagens de controle centralizado de uma rede ou sistema em rede podem apresentar uma complexidade e um peso computacional muito grande. Isso normalmente ocorre quando há uma grande quantidade de dispositivos (nós) que possuem comportamento dinâmico. Manter uma estrutura centralizada de larga escala que muda com uma frequência muito alta pode ser uma tarefa custosa e também difícil. Numa rede ou sistema (em rede) isso pode acarretar em impactos de desempenho e até provocar um mau funcionamento dela como um todo. A descentralização do controle busca contornar essa característica atribuindo autonomia aos nós para gerenciar seu controle com base na visão total ou parcial da rede. Isso possibilita a gerência de uma grande quantidade de dispositivos minimizando o impacto do custo computacional frente às abordagens centralizadas.

O conceito de comportamento coletivo síncrono é tipicamente visto na natureza em sistemas bio-inspirados, como observado no voo dos vaga-lumes [Gielow et al. 2014, Gielow et al. 2015]. A observação desse comportamento serviu de inspiração e gerou aplicabilidade em áreas como telecomunicações, sistemas biológicos, reações químicas, entre outras [Li and Yang 2017]. Em redes onde há uma dificuldade de sincronizar informação surge a necessidade de adicionar controles que viabilizem tal tarefa. Em redes dinâmicas e escaláveis existe uma dificuldade natural em garantir uma sincronização global devido à demanda computacional relacionada à quantidade de dispositivos. Do ponto de vista de [Li and Yang 2017], ele classifica em dois tipos os métodos de controle usados para sincronizar em redes escaláveis: controle do tipo *Pinning*, totalmente controlado.

O controle *Pinning* se caracteriza por distribuir o controle para poucos ou uma porcentagem dos dispositivos da rede de modo que atuem localmente e possibilitem os outros dispositivos conectados a eles sincronizem, levando a uma sincronização total da rede. As estratégias mais comuns de seleção desses nós para controle podem ser classificadas em aleatória e seletiva [Tang et al. 2014]. A estratégia aleatória se baseia na escolha dos nós que farão o controle aplicando uma probabilidade uniforme na escolha para todos os nós. Já a estratégia seletiva escolhe um determinado número de nós com base em propriedades anteriormente estabelecidas. Medidas de centralidade de intermediação, grau de um nó e importância na estrutura, são exemplos de estratégias geralmente aplicadas para escolher os nós no processo de controle.

4. Disseminação Robusta para Sincronização de Ações

Esta seção descreve o modelo de rede tática e a proposta do mecanismo *SinERT* (**Sin**cronização Robusta de **E**ventos em **R**edes **T**áticas) para controle da disseminação de eventos dinâmicos. As Redes Táticas possuem dispositivos ou nós heterogêneos com recursos computacionais e de comunicação móveis, restritos neste trabalho a mobilidade terrestre. Nós da rede escolhidos pelo serviço de gerenciamento da infraestrutura controlam a disseminação dos eventos dinâmicos. A transmissão de informação ocorre por meio de comunicação sem fio. Mensagens de controle trocadas pelos nós mantém o gerenciamento da infraestrutura local de modo dinâmico. Os eventos de comando e controle (C2) e alerta enviados pelos nós na rede objetivam a execução de ações sincronizadas e consistentes num ambiente desorganizado e caótico. Os grafos temporais trabalham a dimensão do tempo e permitem compreender e representar a evolução de estrutura de uma rede dinâmica. A formação de Pontes Locais é utilizada como critério para identificar e classificar nós para atuarem no gerenciamento dos eventos. O *SinERT* aborda a sincronização de eventos dinâmicos em Redes Táticas e como as estruturas locais de uma rede influenciam na robustez da disseminação desses eventos.

4.1. Modelo da Rede

A Rede Tática é representada como um grafo temporal não direcionado $G = (V, E, T)$, onde V denota o conjunto de tuplas (n, t_i, t_f), n um nó do grafo, $(t_i, t_f) \in T$ respectivamente o tempo de início e fim do correspondente vértice no grafo G (com $t_i < t_f$). Denota-se $E = (n_i, n_j, t_i, t_f)$ o conjunto de ligações entre pares de dispositivos tal que $(n_i, n_j) \in V$ estão conectados por uma caminho de comprimento r se existir uma sequência de $r + 1$ nós distintos começando em n_i e terminado em n_j, de modo que os nós consecutivos são adjacentes. A observação de uma rede dinâmica num dado instante T (Snapshot Networks) é dada pelo grafo não direcionado $G_i = (V_i, E_i)$, onde $i \in T$, $V_i = \{v_1, v_2, v_3, \ldots, v_n\} \subseteq V$ denota o conjunto de vértices e $E_i \subseteq E$ o conjunto de arestas no instante t_i. Seja L_{n_i,n_j} o tamanho do menor caminho entre n_i e n_j, define-se os vizinhos de n_i com relação ao grafo G_i como o conjunto $L_i(n_i) = \{ n_j \mid L_{n_i,n_j} = 1\}$.

A interação entre as entidades ou dispositivos da rede respeita a característica de mobilidade da rede. As conexões realizadas de modo oportunísticas devem-se a constante evolução da topologia da rede motivada pela dinâmica da infraestrutura. O protocolo Wi-Fi 802.11 foi proposto para representar a camada física permitindo a mobilidade na rede. Desconexões entre os dispositivos das redes descrevem um padrão de comportamento já esperado, tendo em vista a falta de infraestrutura, barreiras naturais inerentes

dos cenários onde essas redes são empregadas. A dificuldade de estabelecer um caminho fim-a-fim inviabiliza os protocolos de encaminhamento de pacotes tradicionais em Redes Táticas [Moore et al. 2016]. Este trabalho utiliza um modelo de comunicação baseado em redes tolerantes a desconexões, porquanto são úteis em cenários sem caminho fim-a-fim, intermitência de conexões e atrasos significativos, características que degradam severamente a comunicação [Moore et al. 2016]. Além disso, o mecanismo também assume a existência de meios de codificação segura na comunicação de troca de dados na rede [Kurdziel 2014]. A Figura 1 ilustra um cenário de Rede Tática e as alterações da topologia ao longo do intervalo de tempo $T1, T2$ e $T3$.

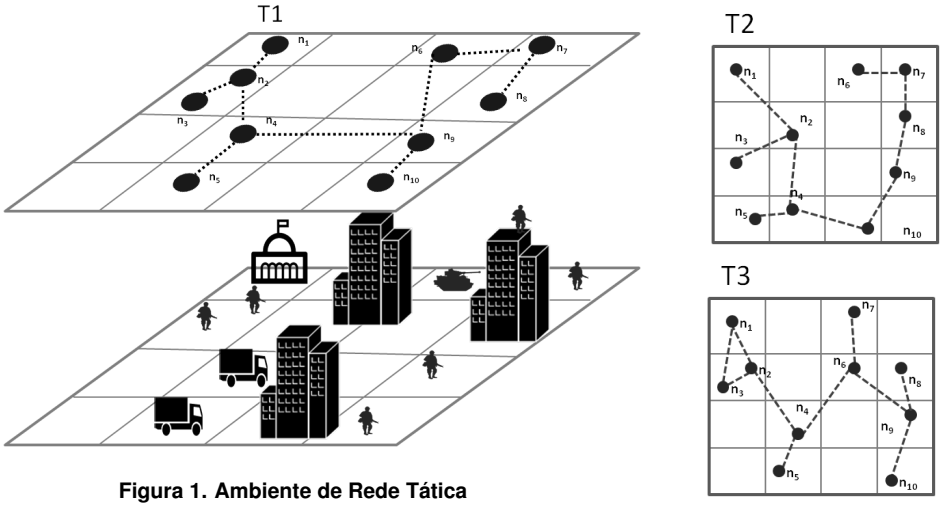

Figura 1. Ambiente de Rede Tática

As técnicas de disseminação de eventos em Redes Táticas que utilizam métodos locais são adequadas e promissoras [Macker 2016], principalmente onde há dinâmica da infraestrutura, das entidades ou dispositivos. Buscando uma classificação adequada para essas técnicas que tratam de comportamento local, o trabalho proposto por [Martínez et al. 2017] classifica como métodos de similaridade de abordagem local as estratégias que utilizam informação da estrutura de sua vizinhança. Dentre as vantagens desses métodos, tem-se a baixa complexidade e o alto paralelismo, apresentando ganhos em termos computacionais. A similaridade se fundamenta na atribuição de um valor para todas as entidades de uma rede, realizando uma classificação para tal.

$$SobreViz = |L(n) \cap L(v_i)| \ / \ (|L(n))| + |L(v_i)| - |L(n) \cap L(v_i)| - 2) \qquad (1)$$

As Pontes Locais, embora não mencionada por [Martínez et al. 2017], se enquadram nessa classificação trazendo uma perspectiva nova para inferir sobre as relações entre duas entidades vizinhas numa rede. As Pontes Locais (PL) são definidas com relação à sobreposição de vizinhança $(SobreViz)$ de uma aresta, dada pela Equação 1.

4.2. *SinERT*

O mecanismo *SinERT* oferece uma abordagem robusta no controle da disseminação de eventos em redes dinâmicas. Ele estabelece dois modos de operação dos dispositivos (nós) da Rede Tática: os nós que atuam na disseminação de eventos assumem o

papel de nó controlador e os demais o papel de nó simples. O conjunto de nós controladores, num dado instante t, onde $C_t = \{n_i \in V_t \mid n_i$ é controlador$\}$ caracteriza os nós responsáveis pelo encaminhamento, envio e descarte de eventos. O conjunto $S_t = V_t - C_t$ representa os demais nós com papel simples que apenas recebem e enviam eventos sem nenhum controle específico. Os nós $n_i \in C_t$ são selecionados com base na sua vizinhança $L_t(n_i)$ de acordo com sua importância estrutural na "fotografia"da rede G_i. Os nós em S_t estabelecem uma relação de associação com os nós em C_t de forma a manter o controle e robustez na rede.

4.2.1. Inicialização da Rede

Na inicialização da rede todos os nós são definidos como simples, então $C_t = \emptyset$ e $S_t = V_t$. Um serviço de rede separa as mensagens de controle e as encaminha para o serviço de gerenciamento da infraestrutura. Cada nó em S anuncia seus identificadores únicos (ID) para seus vizinhos permitindo que cada nó n_i construa uma lista local dos seus vizinhos $L(n_i)$. A Figura 2 ilustra essa etapa, onde num dado tempo t, cada nó pode calcular sua importância estrutural pela sobreposição de vizinhança, descrita pela equação 1, com base na sua lista de vizinhos. Essa informação é utilizada para classificar os nós com base nas Pontes Locais e posteriormente determinar a função de cada um na rede (visto na Figura 3). O Algoritmo 1 descreve a execução do cálculo da importância local para identificar o papel funcional do nó na rede.

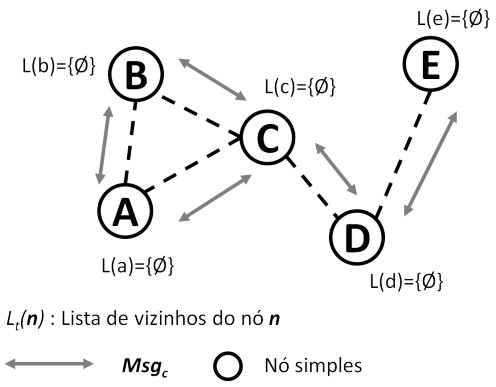

Figura 2. Inicio da rede

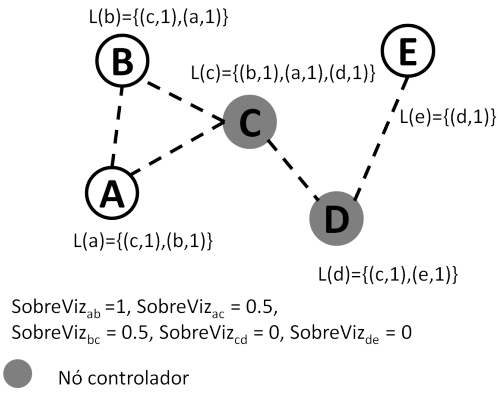

Figura 3. Função de cada nó

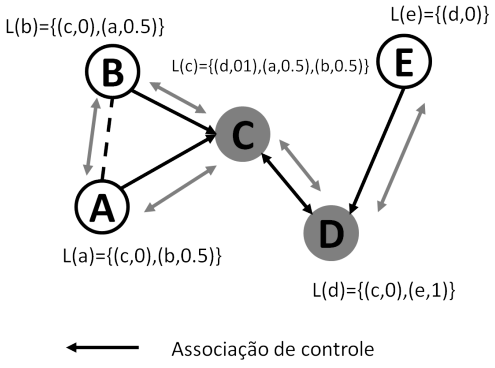

Figura 4. Estrutura local de controle

A igualdade, calculada como $PL \Leftrightarrow SobreViz = 0$, identifica um nó como participante de uma ponte local. Entretanto a maioria dos nós candidatos ao controle apresentam um valor de $SobreViz$ próximo de zero. Um parâmetro de controle $(Threshold)$ estabelece um limiar para definir os nós que pertencem à C. Cada nó n_i anuncia seu valor de $SobreViz$ para seus vizinhos e atualiza o papel deles na rede em sua lista $L(n_i)$. A lista de vizinhos é mantida ordenada pelo valor decrescente de $SobreViz$ de cada nó, de modo que as primeiras entradas da lista são nós de controle, ao passo que os últimos são nós com menor importância estrutural. Os nós simples decidem com quais controladores vizinhos irão se associar dependendo da configuração local da vizinhança (visto na Figura 4). Os nós de controle se associam respeitando suas vizinhanças.

Algoritmo 1: Identificação do Nó Controlador

```
   Input  : n_i ∈ V with node identifier (ID)
   Output: Each node n_i knows its controller
 1 Procedure CONTROL_ROLE()
 2     role[isControl](n_i) = FALSE ;
 3     L(n_i) ← {} ;
 4     knownNeighbors(n_i) ← {} ;
 5     controller(n_i) ← {} ;
 6     NeighList ← {} ;
 7     broadcast ('ANNOUNCEMENT',ID);                          // node announcement
 8     WAIT (Γ time units);
 9     send ('ACK_ANNOUNCEMENT', knownNeighbors(n_i), n_i);
10     WAIT (Δ time units);
11     send ('NEIGHBOR_LIST', L(n_i), n_i);                    // neighbor discovery
12     WAIT (Θ time units);
13     role[isControl](n_i) ← CALCULATE_NEIGHBORHOOD_OVERLEAP(L(n_i), Threshold) ;
14     if role[isControl](n_i) = TRUE then                     // node elected as controller
15         for n_i ∈ L(n_i) do
16             send ('ID_CONTROLLER', ID, n_i);
17         end
18     end
19 Procedure Receiving('ANNOUNCEMENT', ID) by n_i
20     knownNeighbors(n_i) ← knownNeighbors(n_i) ∪ {ID} ;
21 Procedure Receiving('ACK_ANNOUNCEMENT', ID) by n_i
22     L(n_i) ← L(n_i) ∪ {ID} ;
23 Procedure Receiving('ID_CONTROLLER', ID) by n_i
24     controller(n_i) ← controller(n_i) ∪ {ID}
25 Procedure Receiving('NEIGHBOR_LIST', NeighList) by n_i
26     L(v_i) ← L(v_i) ∪ NeighList
27 Procedure CALCULATE_NEIGHBORHOOD_OVERLEAP(NeighList, Threshold) // controller election
28     localBridge ⇐ ∞ ;
29     neighOverleap ⇐ ∞ ;
30     for L(v_i) ∈ NeighList do
31         neighOverleap = |L(n) ∩ L(v_i)|  /  (|L(n))| + |L(v_i)| − |L(n) ∩ L(v_i)| − 2 ;
32         if localBridge > neighOverleap then
33             localBridge ← neighOverleap ;
34         end
35     end
36     if Threshold > localBridge then
37         if |L(n)| > 1 then
38             return True;
39         end
40     end
```

Inicialmente, cada dispositivo envia a mensagem "ANNOUNCEMENT" para seus vizinhos informando seu identificador (ID) *(l.7)*. Cada dispositivo n_i que recebe a mensagem armazena as leituras de seus vizinhos $knownNeighbors$ *(l.19-20)*. Após certo período de tempo Γ, cada dispositivo n_i envia uma mensagem de `ACK` para os dispositivos conhecidos *(l.8-9)*. As mensagens de `ACK` recebidas pelos dispositivos são armazenadas

na estrutura de vizinhos conhecidos $L(n_i)$ *(l.21-22)*. Após certo período de tempo Δ os dispositivos enviam sua lista de vizinhos conhecidos $L(n_i)$ *(l.10-11)*. Após o envio da mensagem, os dispositivos armazenam a lista de vizinhos de seus vizinhos conhecidos durante um certo tempo Θ *(l.25-26)* . Quando o tempo expirar, os dispositivos executam a função "CALCULATE_NEIGHBORHOOD_OVERLEAP" *(l.12-13)*, que realiza o cálculo da importância local para identificar o nó que vai atuar no controle de disseminação de eventos, informando sua lista de vizinhos $L(n_i)$ e qual o limite $(threshold)$ definido pelo usuário. Os dispositivos selecionados com o papel de controle $isControl$ anunciam a decisão para seus vizinhos *(l.14-18)*.

4.2.2. Manutenção da Rede

A dinâmica da infraestrutura altera o controle inicialmente estabelecido. Cada fotografia $\mathcal{G}_k$ da rede descreve a topologia no instante k, revelando a necessidade de ajustar os papéis dos nós na rede. Portanto, os nós em V iniciam uma fase de manutenção. O conjunto $\mathcal{G}_k = \{G_1, G_2, G_3, \ldots, G_k\}$ representa a sequência ordenada dos grafos observados desde o período de observação t_1 até o tempo t_k. Entre esses instantes, uma fase de manutenção δ é estabelecida para que cada nó registre as alterações de sua vizinhança. Cada conexão perdida ou formada gera uma notificação para o serviço de gerenciamento da infraestrutura que atualiza $L(n)$ dos nós envolvidos. Nessa fase, mensagens de controle (Msg_c) são trocadas entre os nós vizinhos para atualizarem suas listas. Os nós utilizam as (Msg_c) para anunciar aos nós vizinhos suas listas de vizinhos, seu `ID` e $SobreViz$.

Dado um grafo $\mathcal{G}_k$, um nó n_i precisa recalcular sua importância na estrutura local se for observado que $L_t(n_i) \neq L_k(n_i)$ no instante $k = t + \delta$, onde δ representa a fase de manutenção. O valor de *SobreViz* dos nós afetados pela dinâmica na rede precisam ser atualizados. Os procedimentos do Algoritmo 1 são utilizados em cada nó, para que verifiquem se houve alteração em sua vizinhança e recalculem sua importância estrutural. Em seguida, anunciam a seus vizinhos seus papeis na rede para que as associações sejam atualizadas. A fase de manutenção reduz o impacto da dinâmica da rede no mecanismo de controle e evita que as alterações na vizinhança de um nó se propaguem para rede toda. O serviço de gerenciamento de eventos utiliza as informações atualizadas do serviço de gerenciamento da infraestrutura para encaminhar os eventos corretamente. A adaptabilidade do serviço de gerenciamento de infraestrutura contribui na garantia da robustez na disseminação de eventos. Dessa forma, o controle distribuído pela rede se mantém condizente em cada instante *t*, levando a rede a operar com eficiência.

4.2.3. Gerência de Eventos

A gerência de eventos trata as mensagens de eventos (Msg_{ev}), agindo nos identificadores de origem e destino, na comunidade, no tempo de vida e no tipo de evento. Nós em *C* fazem a gerência da disseminação da informação. Duas comunidades de Msg_{ev} são disseminadas pela rede. Msg_{ev} de *C2* geradas por unidades de controle são aquelas destinadas à coordenação de ações entre os agentes e devem ser difundidas por toda a rede. Msg_{ev} de alerta geradas por qualquer nó tem o objetivo de reportar uma situação particular sofrida ou observada. Uma abordagem de comunidades cria uma hierarquia de eventos dentro da rede e os classifica de acordo com a função operacional ou estratégica

de seus agentes. A gerência dos eventos compreende as atividades de encaminhamento dos eventos na rede com base na infraestrutura local, nos identificadores, na comunidade dos eventos e no tempo de vida do evento. Os nós controladores verificam o tempo de vida das mensagens e descartam os eventos expirados. Também alteram o destino das mensagens para serem os nós simples associados, evitando retransmissões. Encaminham eventos que não são da mesma comunidade apenas para os nós controladores.

A dinâmica presente em Redes Táticas exige constantes adaptações da rede. Quando um nó é identificado como potencial controlador para a rede, sua influência local permite que ele atue favorecendo a disseminação de eventos [Li and Yang 2017]. Fatores como desconexões constantes e escalabilidade podem levar a ruptura de uma rede quando atingem um determinado conjunto de nós [Zhang et al. 2016, Hwang et al. 2006]. As Pontes Locais determinam a influência local de um nó de uma rede e contribuem para manter a conectividade e ajudam em questões de encaminhamento de mensagens [Macker 2016, Hwang et al. 2006]. *SinERT* utiliza essa metodologia para identificar nós conforme o Algoritmo 1 com capacidade de exercer controle eficiente e eficaz. Para se adaptar à dinâmica da rede, a fase de manutenção trabalha de modo a garantir que o conjunto de controle *C* esteja sempre condizente com o estado atual *t* da rede em G_t. A gerência de eventos utiliza as informações sobre a infraestrutura local para disseminar eventos prioritariamente para nós que tenham maiores condição de difusão de informação.

5. Avaliação

Esta seção apresenta uma avaliação do mecanismo proposto para analisar sua eficácia e eficiência na garantia da disseminação robusta de eventos em Redes Táticas. O mecanismo proposto é comparado a um modelo probabilístico que maximiza a entrega de mensagens estimando futuras interações entre os nós da rede, baseado na proposta de [Gao 2016]. Ele também o paradigma de troca de mensagens "*carry-and-forward*" em redes WiFi. Todas as propostas foram implementados no simulador ONE (Opportunistic Network Environment simulator) versão 1.6 [Keränen et al. 2009], que atende aos requisitos para simular intermitência de conexões em redes dinâmicas [DTNRG 2018] e o paradigma "*carry-and-forward*" utilizado por [Gao 2016].

Os mecanismos foram avaliados num cenário que representa a cidade de Helsinki, como descrito em [Keränen et al. 2009]. Os nós respeitam as condições impostas pelo mapa da cidade e trafegam apenas pelas ruas e passagens. Apenas um conjunto de nós é responsável pela criação de eventos. Os demais nós participam apenas da disseminação dos eventos na rede. Um nó foi definido como responsável pela criação dos eventos de comando e controle em todos os cenários. Este nó representa a entidade central que coordena as ações realizadas pelos agentes. No cenário empregado, considerou-se um tempo inicial de 100 segundos para iniciar a rede e o mecanismo de controle. Em seguida, após 400 segundos, foi disseminado um evento na rede e realizadas as medições para verificar a robustez do mecanismo. A avaliação foi executada numa máquina com sistema operacional Ubuntu 16, 64bits, 3 CPUs e 6,5GB de memória *ram*.

As métricas aplicadas na avaliação da eficiência dos mecanismos são: **Tempo Médio para recebimento de um evento (**EMT_{ev}**)** e **a Quantidade de Nós que receberam um evento dentro de um dado tempo (**$NEC_{t,ev}$**)**. Elas permitem avaliar o desempenho da disseminação de um evento na rede. A métrica para avaliar a eficácia da proposta

mede a cobertura de um evento (NC_{ev}), isto é, a quantidade de nós que receberam um dado evento. Ambas $NEC_{t,ev}$ e EMT_{ev}, representadas nas Equações 2 e 3, possibilitam avaliar requistos funcionais da rede ao passo que NC_{ev} permite observar questões técnicas e limitações relativas ao funcionamento dos mecanismos de disseminação.

$$NEC_{t,ev} = |\{ V'_t \subseteq V_t |\ v_i \in V' recebeu\ o\ evento\ \textbf{\textit{ev}}\ at\acute{e}\ o\ tempo\ \textbf{\textit{t}}\}| \tag{2}$$

$$EMT_{ev} = \frac{\sum_{v_i} T(v_i)_{\textbf{ev}}}{|V'|},\ onde\ n_i \in V' |\ v_i\ recebeu\ o\ evento\ \textbf{\textit{ev}} \tag{3}$$

$$NC_{ev} = \frac{|\sum v_i|}{|V|},\ onde\ v_i \in V |\ v_i\ recebeu\ o\ evento\ \textbf{\textit{ev}} \tag{4}$$

5.1. Resultados

Os resultados desta seção foram colhidos a partir da simulação com os parâmetros definidos na seção anterior. Foi avaliada a disseminação de um evento gerado por um nó fixo, com o objetivo de representar uma estrutura de comando e controle em situações de emergências urbanas. O tempo útil de um evento, que representa a oportunidade de utilizar a informação disseminada, foi estabelecido em 1 min. Assim, considera-se que após esse tempo, mesmo que a mensagem chegue ao destino ele não é mais útil. O gráfico da Figura 5 descreve o desempenho da disseminação de um evento medidos em intervalos de 10 segundos, até o tempo de 60 segundos após o início de sua disseminação. Para isso, foi empregada a métrica de avaliação $NEC_{t,ev}$, para *t* = {10, 20, 30, 40, 50, 60}.

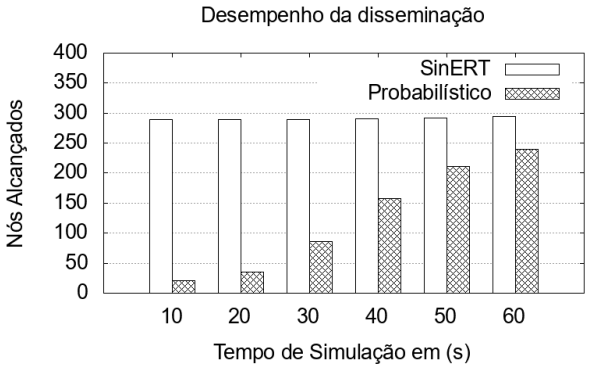

Figura 5. Robustez de disseminação obtida por evento num dado instante *t*

A quantidade de nós que recebem o evento logo nos primeiros segundos da rede é significantemente maior para o mecanismo proposto. O mecanismo probabilístico necessita de mais informações sobre a rede para estimar as probabilidades ao tentar difundir um evento. Isso impacta diretamente na rapidez da difusão do evento. Já *SinERT*, mantém um estrutura mais simplificada que demanda informação reduzida sobre a rede para disseminar o evento. O mecanismo probabilístico com o tempo vai ganhando desempenho e começa apresentar comportamento expressivo. Porém, para o cenário com emprego de eventos de curta duração em Redes Táticas, esse atraso pode inviabilizar sua aplicação.

O tempo de convergência, isto é, para sincronizar um evento na rede, avalia a eficácia das propostas simuladas, que é dado pelo tempo em que NC_{ev} atinge 100% ou o

Tabela 1. Tempo de Sincronização de um Evento na Rede Tática

Mecanismo	Tempo de Convergência	NC_{ev}
SinERT	149	100%
Probabilístico	206	100%

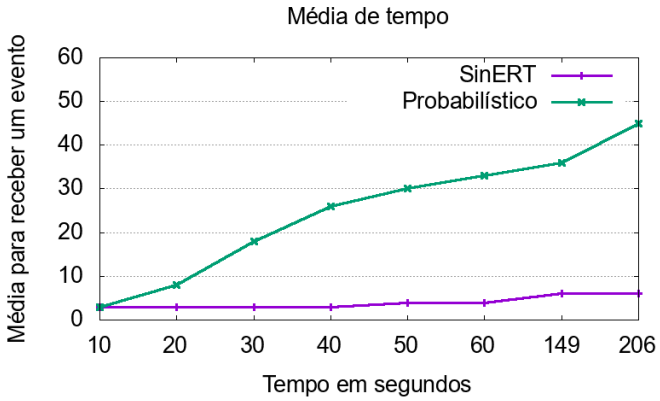

Figura 6. Tempo médio para um nó receber um evento ao longo do tempo

TTL do evento expira. A Tabela 1 mostra o tempo em segundos que um evento levou para ser disseminado por toda a rede. A proposta probabilística apresentou um tempo aproximadamente 38% maior em relação ao *SinERT*. A quantidade de nós aumenta a expectativa de entrega de mensagens, porém eleva o custo de manutenção e cálculo das probabilidades, degradando o desempenho frente a dinâmica da rede. A robustez em se adaptar a dinâmica imposta pela rede faz o *SinERT* mais adequado para cenários com dinâmica dos nós e conexões intermitentes. A Figura 6 mostra a evolução da EMT_{ev} ao longo do tempo. Nota-se que a influência do cálculo das probabilidades de contatos para estimar a entrega de um evento restringe o desempenho dessa abordagem. Percebe-se que há um aumento desse tempo em ambas as propostas até NC_{ev} alcançar 100%. Nós que sofrem mais intensamente pela dinâmica da infraestrutura demoram mais a receber o evento.

6. Conclusões

Este trabalho apresentou o mecanismo *SinERT* para apoiar a disseminação robusta de eventos em Redes Táticas. Utilizando informação de vizinhança entre os dispositivos conectados, foi possível aplicar a métrica de Pontes Locais para selecionar dinamicamente nós para exercer função de controle na disseminação. Grafos temporais foram a base para modelar Redes Táticas permitindo compreender e representar a dinâmica da rede. Métricas de eficiência e eficácia foram empregadas para avaliar a viabilidade do mecanismo proposto. Trabalhos futuros consistem em aplicar outros mecanismos para avaliação e mensurar o custo computacional, sobrecarga de rede decorrente dessa proposta e considerar cenários com redes densas e esparsas.

Referências

Casini, E., Benincasa, G., Morelli, A., Suri, N., and Breedy, M. (2016). An experimental evaluation of data distribution applications in tactical networks. In *Military Communications Conference (MILCOM)*, pages 1267–1272. IEEE.

DTNRG (2018). Delay-tolerant networking research group DTNRG. https://irtf.org/concluded/dtnrg. Último acesso em 02/07/2018.

Gao, W. (2016). Exploiting deployment information for social-aware contact prediction at the tactical edge. In *Military Communications Conference (MILCOM)*, pages 594–599. IEEE.

Gielow, F., Jakllari, G., Nogueira, M., and Santos, A. (2015). Data similarity aware dynamic node clustering in wireless sensor networks. *Ad Hoc Networks*, 24:29–45.

Gielow, F., Nogueira, M., and Santos, A. (2014). Data similarity aware dynamic nodes clustering for supporting management operations. In *Network Operations and Management Symposium (NOMS)*, pages 1–8. IEEE.

Grönkvist, J., Komulainen, A., Sterner, U., and Uppman, U. (2016). Dynamic scheduling for cooperative broadcasting in tactical ad hoc networks. In *Military Communications Conference (MILCOM)*, pages 1034–1040. IEEE.

Holzhauer, N. D., Milligan, J. R., and Soule, N. B. (2016). A hybrid P2P and pub/sub messaging system for decentralized Information Management. In *Military Communications Conference (MILCOM)*, pages 1016–1021. IEEE.

Hwang, W., Cho, Y.-r., Zhang, A., and Ramanathan, M. (2006). Bridging centrality: identifying bridging nodes in scale-free networks. In *The 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 20–23.

Keränen, A., Ott, J., and Kärkkäinen, T. (2009). The ONE Simulator for DTN Protocol Evaluation. In *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, New York, NY, USA. ICST.

Kurdziel, M. T. (2014). Cyber threat model for tactical radio networks. In *Wireless Sensing, Localization, and Processing IX*, volume 9103, page 910305. International Society for Optics and Photonics.

Li, X.-J. and Yang, G.-H. (2017). Graph theory-based pinning synchronization of stochastic complex dynamical networks. *IEEE transactions on neural networks and learning systems*, 28(2):427–437.

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.

Macker, J. P. (2016). An improved local bridging centrality model for distributed network analytics. In *Military Communications Conference (MILCOM)*, pages 600–605. IEEE.

Martínez, V., Berzal, F., and Cubero, J.-C. (2017). A survey of link prediction in complex networks. *ACM Computing Surveys (CSUR)*, 49(4):69.

Mercer, L., Kuperman, G., Hunter, A., and Proulx, B. (2016). Large scale over-the-air testing of group centric networking. In *Military Communications Conference (MILCOM)*, pages 1273–1278. IEEE.

Moore, S., Amin, R., Ripplinger, D., Mehta, D., and Cheng, B.-N. (2016). Performance evaluation of a disruption tolerant network proxy for tactical edge networks. In *Military Communications Conference (MILCOM)*, pages 964–969. IEEE.

Ogundele, T. J., Chow, C.-Y., and Zhang, J.-D. (2017). Eventrec: Personalized event recommendations for smart event-based social networks. In *International Conference on Smart Computing (SMARTCOMP)*, pages 1–8. IEEE.

Purushotham, S. and Kuo, C.-C. J. (2016). Personalized group recommender systems for location-and event-based social networks. *ACM Transactions on Spatial Algorithms and Systems (TSAS)*, 2(4):16.

Reina, D., Coca, J. M. L., Askalani, M., Toral, S., Barrero, F., Asimakopoulou, E., Sotiriadis, S., and Bessis, N. (2014). A survey on ad hoc networks for disaster scenarios. In *International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, pages 433–438. IEEE.

Tang, Y., Qian, F., Gao, H., and Kurths, J. (2014). Synchronization in complex networks and its application–a survey of recent advances and challenges. *Annual Reviews in Control*, 38(2):184–198.

Verma, S., Kawamoto, Y., Fadlullah, Z. M., Nishiyama, H., and Kato, N. (2017). A survey on network methodologies for real-time analytics of massive IoT data and open research issues. *IEEE Communications Surveys & Tutorials*, 19(3):1457–1477.

Zhang, Z.-K., Liu, C., Zhan, X.-X., Lu, X., Zhang, C.-X., and Zhang, Y.-C. (2016). Dynamics of information diffusion and its applications on complex networks. *Physics Reports*, 651:1–34.