https://eventos.utfpr.edu.br//sicite/sicite2018

Ataque de negação de serviço utilizando GPS-spoofing em redes veiculares simuladas

Denial of service attack using GPS-spoofing in simulated vehicular networks

Paulo Ricardo Kenshun Nakaima
nakaima.prk@gmail.com
Universidade Tecnológica Federal do Paraná, Cornélio Procópio, Paraná, Brasil

Roberto Sadao Yokoyama
rsadao@gmail.com
Universidade Tecnológica Federal do Paraná, Cornélio Procópio, Paraná, Brasil

RESUMO

Este trabalho apresenta de forma geral conceitos básicos da área de VANET e o problema da falsificação de posicionamento contra uma aplicação de trânsito. Para isto utiliza o modelo generalista para implementar o cenário e o ataque de negação de serviço com *GPS spoofing*. Os resultados apontam que é necessário ao adversário o conhecimento prévio da densidade de veículos para o ataque ter efeito. Foi possível aumentar em 15% o tempo de viagem dos veículos.

PALAVRAS-CHAVE: Redes veiculares. GPS-spoofing. Ataque de negação de serviço.

ABSTRACT

This paper presents basic concepts of the VANET area and the problem of false position against a traffic application. For this it uses the generalist model to implement the scenario and the denial of service attack with GPS spoofing. The results indicate that it is necessary for the opponent to know the density of vehicles for the attack to take effect. It was possible to increase vehicle travel time by 15%.

KEYWORDS: VANET. GPS-spoofing. Denial of service.

Recebido: 31 ago. 2018.
Aprovado: 04 out. 2018.

INTRODUÇÃO

No campo de novas tecnologia de comunicação e da informação existe pesquisas direcionadas às redes veiculares, *Vehicular Ad Hoc Network* - Rede Veicular *Ad Hoc* (VANET), um tipo de rede principalmente não estruturada (*ad hoc*) e móvel a qual possibilita a comunicação entre veículos e veículos (V2V - *Vehicle to Vehicle*) e/ou veículos e infraestrutura (V2I - *Vehicle to Infrastructure*) (SAKIZ; SEN, 2017). Isto cria um novo paradigma para a concepção de aplicações de segurança no trânsito, assistência ao motorista e entretenimento ao usuário. Por exemplo, um carro equipado com sensores, sistema de geolocalização (GPS – *global positioning system*), antenas de comunicação de rádio frequência e computador de bordo (OBU - *Onboard unit*) pode coletar dados do veículo e compartilhá-los com seus vizinhos alertando-os sobre colisões, desaceleração, congestionamentos, por meio da troca de mensagens pela rede veicular. Por outro lado, a disseminação de sistemas computacionais e meios de comunicação veiculares, criam novos desafios relativos à segurança computacional que devem ser considerados visto o risco à vida de motoristas e passageiros, os quais tomarão decisões críticas baseadas nas informações geradas por esta tecnologia.

Uma vez que os benefícios obtidos com as redes veiculares estão intimamente ligados a troca de informações V2V ou V2I, o problema da falsificação do posicionamento do veículo deve ser considerado. Existe a possibilidade de infecção por malware em OBUs e RSUs já que estes possuem componentes de software. Além disto temos o ataque GPS *spoofing* o qual caracteriza-se pela injeção de posições falsas geradas por emuladores de GPS no nível da aplicação. Sendo as aplicações de segurança altamente dependentes da informação sobre o posicionamento dos veículos este tipo de ataque é um problema crítico (SAKIZ; SEN, 2017).

No padrão previsto para rede veicular assume-se a existência de mecanismos básicos de verificação de consistência de tempo e posição. Mensagens com o tempo anteriores a um determinado limite ou posteriores ao momento da verificação são descartadas. A posição será válida se estiver dentro do raio de comunicação do receptor. Os certificados digitais garantem apenas a autenticidade e integridade da mensagem, contudo não exclui a possibilidade de falsificação do conteúdo (KIM; KIM, 2017).

O problema principal abordado neste trabalho é ataque de falsificação de posicionamento (GPS *spoofing*) em aplicativos de trânsito em VANET. Implementou-se o cenário, o adversário e analisou-se os impactos para em trabalhos futuros implementar um mecanismo de detecção.

1 MÉTODOS

1.1 DESCRIÇÃO DAS FERRAMENTAS

Com o foco de implementar e avaliar a falsificação de mensagens em um ambiente de rede veicular utilizou-se os seguintes softwares:

a) SUMO (*Simulation of Urban Mobility* - Simulador de Mobilidade Urbana): é um simulador de tráfego urbano. Permite a modelação de sistemas de

tráfego, incluindo, veículos, transporte público e pedestres (SUMO, 2018);

b) OMNet++ (*Objective Modular Network Testbed*): é um simulador de redes orientado a objetos baseado em C++ (OMNET, 2018);

c) VEINS (*Vehicles in Network Simulation*): é um framework que possui um conjunto de modelos para simulação de redes veiculares. Reproduz o padrão WAVE (*Wireless Access in Vehicular Environments*) (VEINS, 2018).

1.2 IMPLEMENTAÇÃO DO CENÁRIO

Utilizou-se modelos generalistas de ambiente no qual veículos trafegam com a maior velocidade possível, não permitindo colisões. A comunicação de rádio simulada considera o enfraquecimento do sinal conforme a distância. Protocolo de disseminação de mensagem de salto único, contendo informações sobre identificação do emissor, posicionamento, velocidade. Outros parâmetros podem ser vistos na Tabela 1:

Tabela 1 – Parâmetros do cenário

Parâmetro	Valor
Dimensão do mapa	400 x 400 m
Vias	80
Congestionamento legítimo	1
Veículos	300
Cobertura do sinal OBU	~130 m
RSU	4
Cobertura do sinal RSU	~250 m

Fonte: Autoria própria.

Cada OBU possui uma aplicação de tráfego cuja função é gerar rotas alternativas quando notificada sobre congestionamento no trajeto. Para tanto utiliza-se o algoritmo de Dijkstra para encontrar o menor caminho desconsiderando a via congestionada. Os RSUs amplificam a cobertura do sinal para todo o cenário. Trabalhos que propõem o gerenciamento de tráfego com redes veiculares podem ser encontradas em Brennand et al. (2015), Souza et al. (2015).

1.3 IMPLEMENTAÇÃO DO ADVERSÁRIO

Um ataque de negação de serviço visa comprometer a disponibilidade de banda, processamento ou aplicação de forma parcial ou completamente. Dada a limitação do impacto que um atacante pode causar uma rede de computadores ou *zombies* pode ser usada para amplificar os efeitos. Esta rede pode ser controlada diretamente ou indiretamente para coordenar o ataque.

Neste sentido implementou-se um módulo responsável por definir a frequência da disseminação das mensagens e as vias alvo. A cada 5 segundos foi

enviado um comando de ataque com 18 localizações. Cada membro da rede *zombie* ficou encarregado de disseminar os alertas de congestionamentos ilegítimos. As escolhas das vias foram feitas conforme classificação relativa a densidade de veículos (estimativa de veículos por quilômetro) no cenário descrita na Tabela 3, sem esta seleção o ataque não tem efeito. Na Tabela 4 consta a seleção dos alvos:

Tabela 3 – Classificação de densidade

Classificação	Densidade
Alta	80
Moderada	41 a 79
Baixa	0 a 40

Fonte: Autoria própria.

Tabela 4 – Seleção das vias

Classificação	Quantidade vias
Alta	3
Moderada	9
Baixa	6

Fonte: Autoria própria.

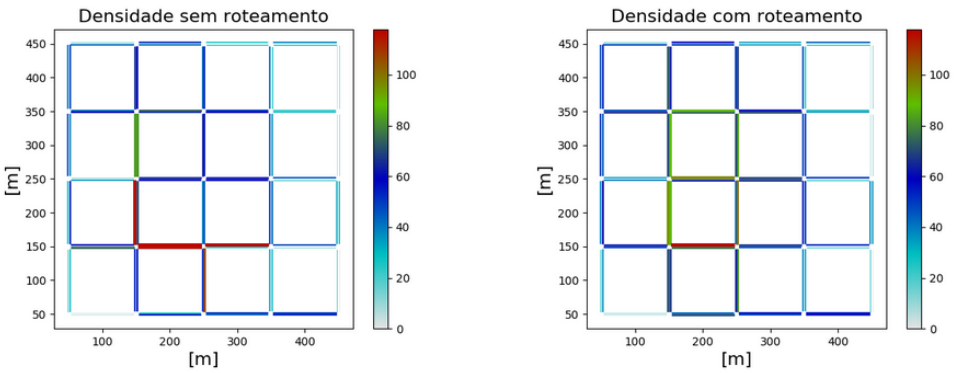
O alerta contém os seguintes campos: identificação, localização do emissor, tempo, localização do congestionamento. A segunda e a quarta informação foi falsificada.

2 RESULTADOS

As simulações foram realizadas três vezes. Primeiro sem roteamento e sem ataque (SR), a segunda com roteamento e sem ataque (CR), e a última com roteamento e com ataque (CA). Na Figura 1, as vias em vermelho significam que o trânsito está parado. A aplicação de tráfego consegue liberar 4 vias.

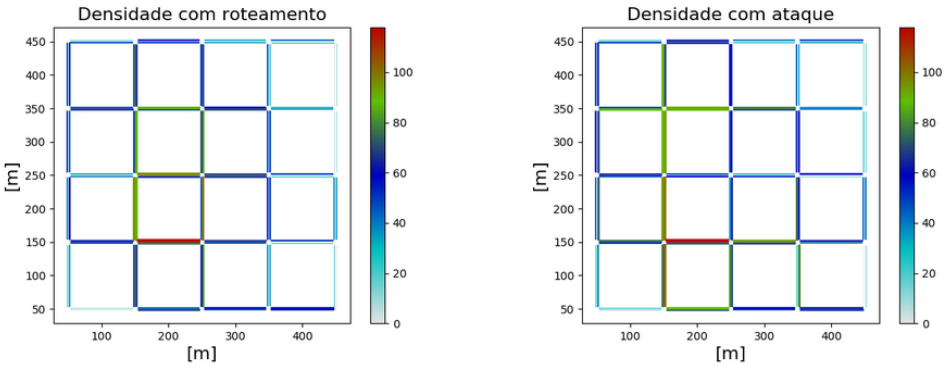
Na Figura 2 encontra-se o resultado do ataque, não foram criados novos congestionamentos e a aplicação de tráfego continua em operação. De 10 vias com densidade alta passa-se para 15.

Figura 1 – Comparação entre densidade



Fonte: Autoria própria.

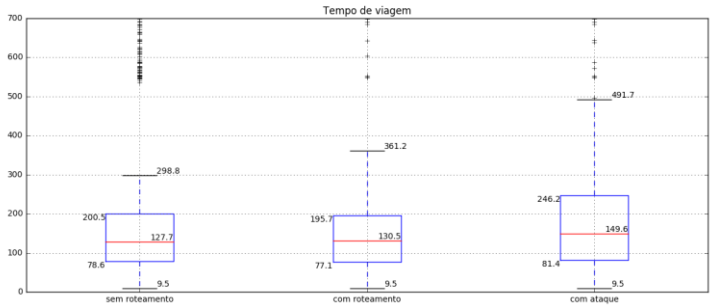
Figura 2 – Comparação entre densidade



Fonte: Autoria própria.

Na Figura 3 consta o gráfico para o tempo de viagem dos veículos nas três simulações. Os dados discrepantes são aqueles que não conseguiram chegar ao destino devido ao congestionamento sendo estes os resultados: SR: 60. CR: 8. CA: 10. A diferença entre a mediana foi de 2% comparando SR e CR e de 15% comparando CR e CA.

Figura 3 – Comparação tempo de viagem



Fonte: Autoria própria.

3 CONCLUSÃO

Diante dos resultados consideraremos alguns requisitos de segurança computacional.

Disponibilidade: Para afetar a disponibilidade da aplicação implantada por meio de *flooding* a saturação da banda deve ser muito alta ou completa, pois com uma única mensagem o usuário consegue desviar do congestionamento.

Controle de acesso e não repúdio: para este tipo de ataque o controle de acesso permitiria a identificação dos *zombies* e posterior notificação e correção do sistema de software do OBU.

Integridade: requisito crítico, o não cumprimento pode levar a prejuízos financeiros devido a congestionamentos causados intencionalmente.

A baixa efetividade do ataque (15%) pode ser explicada pelas características das rotas geradas para simulação, 75% delas estão abaixo de 479 metros diminuindo a quantidade de rotas alternativas. Além disto é necessário ao adversário o conhecimento da densidade de veículos da área atacada.

REFERÊNCIAS

BRENNAND, C. A. R. L. et al. An intelligent transportation system for detection and control of congested roads in urban centers. **IEEE Symposium on Computers and Communication,** 2015.

KIM, T.; KIM, H. Vehicle-to-vehicle message content plausibility check through low-power beaconing. **2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)**. Toronto: IEEE, 2017.

OMNET. 2018. Disponível em: <https://www.omnetpp.org/>. Acesso em: 29 ago. 2018

SAKIZ, Fatih; SEN, Sevil. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. **Ad Hoc Networks**, v. 61, jun. 2017.

SOUZA, A. M. et al. GARUDA: A New Geographical Accident Aware Solution to Reduce Urban Congestion.**IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing**. 2015.

SUMO. 2018. Disponível em: <http://sumo.dlr.de/>. Acesso em: 29 ago. 2018

VEINS. 2018. Disponível em: <http://veins.car2x.org/>. Acesso em: 29 ago. 2018

AGRADECIMENTOS

Os autores agradecem o apoio financeiro da Fundação Araucária FA - Paraná/Brasil.