Um Sistema de Detecção de Ataques de Negação de Serviço Distribu´ıdo em Redes Veiculares Utilizando Aprendizado de Máquina

Davi Sell Iahn[1], Michelle Silva Wangham, Dra[1], Anita Maria da Rocha Fernandes, Dra[1]

[1]Computação Aplicada – Universidade do Vale do Itajaí (UNIVALI)
Santa Catarina – SC – Brasil

daviahn@gmail.com, {wangham,anita.fernandes}@univali.br

Abstract. *Vehicular ad hoc networks (VANETs) consist of a set of nodes composed by devices present in vehicles and along the roads, that communicate with each other. VANET applications offer more entertainment, comfort, safety and other benefits to drivers and passengers. However, like any wireless network, they present security challenges for vehicular applications. Currently, one of the major security challenges in VANETs is to handle the distributed denial-of-service (DDoS) attacks that affect the data and network availability. The main purpose of this work is to detect DDoS attacks in VANETs using machine learning. The proposed solution uses a VANET hybrid architecture in fog computing and using Support Vector Machine (SVM).*

1. Introdução

Uma rede *ad hoc* veicular (*Vehicular Ad Hoc Network* – VANET) é uma rede móvel que permite aos ve´ıculos se comunicarem uns com os outros, tendo o objetivo de melhorar a segurança nas rodovias através da troca de alertas entre veículos da vizinhança ou oferecer serviços usuários da estrada. As redes veiculares são uma variação das redes móveis, porém, possuem algumas diferenças, tais como alterações muito rápidas em sua topologia à medida em que os ve´ıculos se movimentam. Alguns requisitos das redes veiculares, como informações de contexto de rede, reconhecimento de localização e baixa latência, podem ser providos por uma plataforma de computação em névoa (*Fog Computing*) [Bonomi et al. 2012].

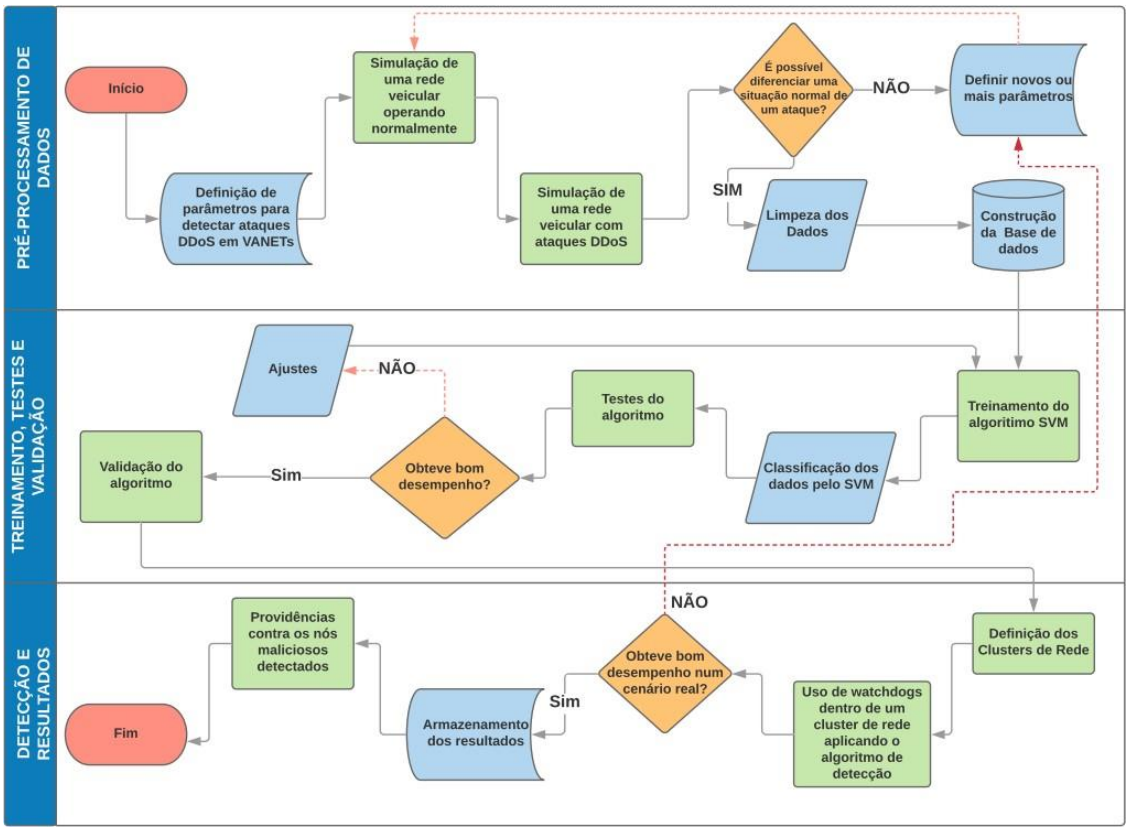
Uma das principais preocupações hoje nas redes VANETs são as questões ligadas a segurança destas redes. Diversos tipos de ataques são conhecidos, sendo os ataques de negação de serviço distribuídos (*Distributed Denial of Service* – DDoS) um dos mais drásticos e mais difíceis de se combater [Erritali and El Ouahidi 2013]. As contramedidas de ataques DDoS, como assinatura digital e criptografia, podem ser usadas como a primeira linha de defesa para reduzir as possibilidades de ataques. No entanto, apenas medidas de prevenção contra intrusões não são suficientes porque, à medida que os sistemas se tornam mais complexos, aumentam-se as vulnerabilidades. Ataques de DDoS podem ser melhor tratados quando técnicas de detecção são adicionadas [Pathre et al. 2013].

Variadas técnicas são utilizadas para tratar detecção de intrusão em VANETs. Ataques maliciosos contra as redes veiculares podem ser detectados utilizando aprendizagem de máquina baseada em anomalias [Grover et al. 2011]. Os algoritmos de aprendizagem de máquina têm como objetivo a determinação de limites de decisão que produzam

uma separação ótima entre classes por meio da minimização dos erros. Um dos algoritmos de aprendizagem de máquina utilizado para detecção de anomalias em redes sem fio é máquina de vetores de suporte (*Support Vector Machine* – SVM). O SVM consiste em uma técnica computacional de aprendizado para problemas de reconhecimento de padrão, introduzida por meio da teoria estat´ıstica de aprendizagem [Wahab et al. 2016]. Este trabalho visa contribuir com a área de segurança em redes veiculares, em especial, para a detecção de ataques de DDoS por meio da aprendizagem de SVM.

2. Solução Proposta

Os ataques de inundação são um dos mais comuns e um dos mais drásticos ataques de DDoS. No momento de um ataque de inundação de pacotes, os nós maliciosos geram tráfego a ponto de esgotar recursos de rede, como largura de banda, processamento, energia e outras m´ıdias semelhantes. O objetivo geral deste trabalho é detectar tais ataques em redes veiculares *ad-hoc* através de um sistema de detecção de anomalias utilizando aprendizagem de máquina. O fluxo geral da solução proposta é mostrado na figura abaixo:



A etapa de pré-processamento de dados inicia com a definição dos parâmetros que serão utilizados que podem diferenciar uma rede com ataques de DDoS e uma rede com atividade normal. Estes parâmetros são avaliados por uma simulação de uma rede veicular com e sem ataques DDoS. Realizada a simulação, os dados são coletados, normalizados e armazenados para uso futuro. Na etapa seguinte os dados são utilizados para treinar o algoritmo SVM. Após testes realizados, é analisado o desempenho do algoritmo a fim de valida-lo para uso. Na sequência é realizada a etapa em que inicia a simulação de um ambiente real com ve´ıculos sofrendo ataques de DDoS, onde sera´ utilizado o algoritmo

SVM. O próximo passo é segmentar a rede em *clusters*, e dentro de cada *cluster* terão nós responsáveis pela filtragem e análise dos pacotes da rede. Estes nós filtradores de pacotes também serão os responsáveis por aplicar o algoritmo SVM treinado para detectar, através de anomalias, tais nós maliciosos realizando ataques de DDoS.

A solução proposta também utilizará um ambiente com computação em névoa para satisfazer alguns requisitos das redes veiculares. Para as simulações serão utilizados alguns modelos de ameaças pré definidos, tendo tanto simples ataques (iniciando de um nó malicioso para vários) quanto situações de conluio.

3. Considerações Finais

Um dos desafios em redes veiculares é a inserção de novos sistemas que possam torná-las mais seguras e confiáveis, sem adicionar riscos no comprometimento de seu desempenho. A principal contribuição deste trabalho será fornecer um sistema de detecção que possibilitará a detecção de nós maliciosos cometendo ataques de DDoS em redes veiculares. Como prova de conceito, o sistema está sendo desenvolvido para demonstrar sua viabilidade técnica bem como permitir a realização de testes que considerará um estudo de caso para mostrar sua aplicabilidade em um cenário real através de simulações. Com estas simulações, também poderão ser analisados os possíveis impactos do uso deste sistema em relação à entrega das mensagens, ao número de colisões de mensagens e aos atrasos no recebimento de mensagens.

References

Bonomi, F., Milito, R., Zhu, J., and Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pages 13–16. ACM.

Erritali, M. and El Ouahidi, B. (2013). A survey on vanet intrusion detection systems. In *Proceedings of the 2013 International Conference on Systems, Control, Signal Processing and Informatics*, pages 16–19.

Grover, J., Prajapati, N. K., Laxmi, V., and Gaur, M. S. (2011). Machine learning approach for multiple misbehavior detection in vanet. In *International Conference on Advances in Computing and Communications*, pages 644–653. Springer.

Pathre, A., Agrawal, C., and Jain, A. (2013). Identification of malicious vehicle in vanet environment from ddos attack. *Journal of Global Research in Computer Science*, 4(5).

Wahab, O. A., Mourad, A., Otrok, H., and Bentahar, J. (2016). Ceap: Svm-based intelligent detection model for clustered vehicular ad hoc networks. *Expert Systems with Applications*, 50:40–54.