Um Sistema de Reputação para Minimizar Ataques de Nós Maliciosos em Redes Veiculares

Claudio P. Fernandes[1], Michelle Wangham[1]

[1]Programa de Mestrado em Computação Aplicada – Universidade do Vale do Itajaí (UNIVALI)

euclaudio@redes.ufsm.br, wangham@univali.br

Abstract. *This paper aims to design a decentralized reputation system, in the aspect of data management, appropriate to vehicular ad hoc networks (VANETs). This system should be able to handle a large number of mobile and fixed network architecture in a vehicle, and should be able to respond effectively to the needs of communication between the vehicles of an application of local danger warning (LDW). The system proposed aims to calculate the confidence of nodes since only a few previous trust relationships exist.*

1. Introdução

As redes veiculares, do inglês *Vehicular Ad Hoc Network* (VANET), são formadas por sistemas de comunicação entre veículos e entre veículos e estações base estacionárias que fazem parte de um ambiente de trânsito. As VANETs têm atraído muita atenção ao longo dos últimos anos e tem como objetivo melhorar as condições de circulação dos tráfegos urbanos e rodoviários de forma segura e eficiente.

A segurança computacional pode ser considerada um fator crítico em qualquer tipo de rede, entretanto em redes veiculares, devido as suas características e limitações, trata-se de uma questão ainda mais delicada. Nestas redes, nos quais os nós trocam informações entre si, existe sempre o risco de algum dos participantes da rede agir de modo egoísta, ou seja, condicionar seu comportamento de acordo com seus interesses pessoais, em detrimento do interesse geral. Para prover segurança às VANETs e minimizar as conseqüências de comportamentos maliciosos, tornam-se necessárias soluções que motivem a cooperação e honestidade dos nós (PAULA et al, 2010).

Sistemas distribuídos nos quais não existem uma coordenação geral, como as VANETs, estão sujeitos a diversos tipos de ataques. A transmissão de dados fraudulentos sobre congestionamento das estradas ou posições dos veículos são exemplos dos possíveis ataques. Nestas redes, não há garantia de que nós anteriormente honestos não serão corrompidos no futuro. Um dos problemas mais difíceis nas VANETs é detectar e tratar ataques de nós maliciosos (GOLLE et al, 2004).

Procurando minimizar a ação de nós maliciosos, alguns métodos surgiram com o objetivo de privilegiar os nós que tenham um comportamento correto na rede, dentre estes, destacam-se os que utilizam sistemas de reputação. Um sistema de reputação tem por finalidade gerenciar as opiniões sobre os comportamentos dos nós. Essas opiniões são acertadas para formar a reputação que serve como referência para que usuários possam identificar quais nós podem oferecer recursos confiáveis, determinando dessa maneira a confiança do nó. Este trabalho tem como objetivo desenvolver um sistema de reputação combinado a um modelo de confiança que vise evitar ou minimizar ataques de nós maliciosos em redes veiculares.

2. Solução Proposta

O sistema de reputação proposto é descentralizado[1], no aspecto do gerenciamento de dados, apropriado às redes veiculares de forma não prejudicar as funcionalidades, segurança e desempenho das aplicações que se executam nestas redes. Este sistema deve ser capaz de lidar com um grande número de dispositivos móveis e fixos em uma arquitetura de redes veiculares e deve ser capaz de responder de forma eficaz as necessidades da comunicação entre os veículos de uma Aplicação de Alerta de Perigo Local (*Local Danger Warning* - LDW) focada para rodovias.

Em uma Aplicação de Alerta de Perigo Local (LDW), (OSTEMAIER et al., 2007) eventos de risco detectados pelos sensores dos veículos geram mensagens de aviso que são disseminadas pela rede (em *broadcast*), como por exemplo, a presença de óleo na via. A cada evento detectado é gerado um alerta informando sua condição. Cada receptor desses dados atua como roteador da mensagem, aumentando assim o alcance deste aviso. Além disso, em uma aplicação LDW os nós avaliam o conteúdo dos alertas recebidos. Toda vez que a aplicação considerar suficiente as evidências de um evento, esta fará uso da interface com o motorista para comunicá-lo da existência do problema, de forma que este motorista possa reagir àquela situação da maneira mais segura possível.

O sistema de reputação proposto visa calcular a confiança dos nós considerando que somente poucos relacionamentos de confiança prévios existem, o que exige o cálculo da confiança de nós desconhecidos. Para cada relação é atribuído um peso o qual indica o quão forte é a relação em questão. O sistema está baseado em métodos estatísticos para cálculo de confiança e será integrado à aplicação LDW visando tratar o problema dos nós maliciosos. O sistema faz uso de uma estratégia investigativa e otimista. Cada nó membro da rede possui (1) uma base de reputação local individual obtida através de experiências com outros nós, (2) uma lista preta contendo os nós maliciosos já identificados na rodovia e uma base com opiniões providas pelas estações bases estacionárias (EBE) por onde este nó passou recentemente.

Pretende-se avaliar os possíveis impactos do sistema de reputação proposto em uma aplicação de alerta de perigo local (LDW) para rodovias através de simulações de forma a verificar as suas funcionalidades, segurança e desempenho. O uso de simulação mostra-se atraente por permitir o controle sobre o ambiente e por consumir menos recursos. Utilizando simuladores de redes e de tráfego bidirecionalmente acoplados o impacto do uso deste sistema de reputação será avaliado considerando o overhead computacional, a latência da rede, a densidade dos nós da rede e a mobilidade dos nós da rede. Alguns ataques também serão simulados para analisar a eficácia do sistema de reputação proposto.

Referências

Golle, P.; Greene, D.; and Staddon, J (2004) “Detecting and correcting malicious data in VANETs,” in: Proceedings of the first ACM workshop on Vehicular ad hoc networks VANET’04.

Paula, W., Oliveira, S.; Nogueira, J.M. (2010) “Um mecanismo de reputação para redes veiculares tolerantes a atrasos e desconexões**".** In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Gramado. SBRC,2010, p.545-550.

Ostermaier B.; Dotzer F.; e Strassberger M.. (2007) “Enhancing the security of local danger warnings in VANETs - a simulative analysis of voting schemes”. In Proceedings of ARES’07.

[1] Não existe uma base de reputação centralizada.