Mecanismo de Reputação para Avaliação da Confiança dos Nós em Redes Ad Hoc Veiculares

Jackson Rodrigues da Silva
Universidade Regional Integrada do Alto Uruguai e das Missões
Departamento de Engenharias e Ciência da Computação
Santo Ângelo, RS - Brasil
jacksonrs1@hotmail.com

Carlos Oberdan Rolim
Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre - RS - Brasil
carlos.oberdan@inf.ufrgs.br

Resumo

As Redes Ad Hoc Veiculares (VANETs), são exemplos de redes móveis em ascensão que possuem diversos desafios a serem explorados. Entre eles, destaca-se as questões de segurança dos dados trocados pelos usuários. Assim, este trabalho aborda a proposta de um mecanismo de reputação para atestar a confiabilidade dos usuários em uma Rede Ad Hoc Veicular que utiliza um protocolo de roteamento Geocast para o encaminhamento das mensagens. Espera-se que o seu desenvolvimento contribua para elevar o nível de segurança e confiabilidade das informações transmitidas pelos membros da rede.

1. Introdução

Através do progresso tecnológico da comunicação sem fio, as pessoas ganharam maior comodidade e flexibilidade para se comunicar. Esta conexão entre eles fez com que fosse necessário o uso de tecnologias que permitissem a troca de dados entre si, por exemplo, a utilização das Redes *Ad Hoc* Móveis (MANETs), que realiza a comunicação entre os dispositivos sem necessitar de uma infraestrutura de rede predefinida [3].

Estendendo-se das MANETs, as Redes *Ad Hoc* Veiculares surgiram com o objetivo de melhorar as condições do tráfego veicular, proporcionando maior segurança e eficiência na comunicação entres os nós móveis da rede [15]. Estas redes, como qualquer outra, estão suscetível a ataques de membros maliciosos, consequentemente faz-se necessário o desenvolvimento de recursos que acrescentem mais segurança às informações transmitidas.

Diante desse cenário, o presente trabalho apresentará as etapas iniciais da construção de um mecanismo de reputação, cujo objetivo é realizar a avaliação da confiança dos nós em uma rede veicular. Como contribuição, espera-se melhorar o nível de segurança e confiabilidade dos dados trocados pelos veículos.

O trabalho está organizado da seguinte forma: a Seção 2 apresenta um breve Referencial Teórico a respeito das VANETs; a Seção 3 descreve os Problemas relacionados a segurança em tais rede; a Seção 4 demonstra a Justificativa utilizada como motivação para o desenvolvimento do trabalho; a Seção 5 traz alguns dos trabalhos correlatos encontrados na literatura; a Seção 6 apresenta os aspectos iniciais do mecanismo proposto; e, por fim o artigo é concluído na Seção 7.

2. Referencial Teórico

2.1. VANETs

Nas VANETs, os veículos são responsáveis por realizar a troca de informações sobre o ambiente em que se encontram. Tais informações, possibilitam aos condutores reagirem antecipadamente a eventos inesperados evitando acidentes e provendo maior segurança no trânsito [21]. As Redes *Ad Hoc* Veiculares possuem características especiais que as distinguem de outras redes móveis, sendo as mais importantes: auto-organização, alta mobilidade, comunicação distribuída e padrão de estrada restrito. Nesse tipo de rede, a comunicação entre os nodos pode ser feita através de di-

ferentes formas de roteamento, como por exemplo, Unicast, Broadcast ou através de Geocast (Figura 1).

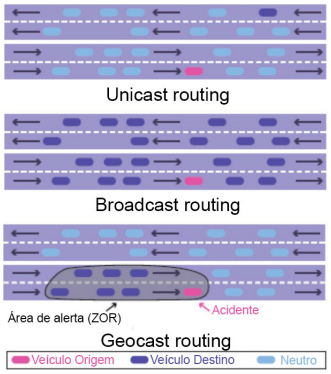

Figura 1. Diferentes cenários de comunicação em VANETs [14].

2.2. Geocast

O protocolo Geocast (Figura 2), fornece uma comunicação sem fio *Multi-Hop* em um ambiente móvel para um conjunto de nós sem necessitar de uma infraestrutura [18]. Os nodos são previamente especificados em uma determinada zona de relevância (ZOR). Os veículos fora dessa área não são alertados para evitar reações desnecessárias e precipitadas [1].

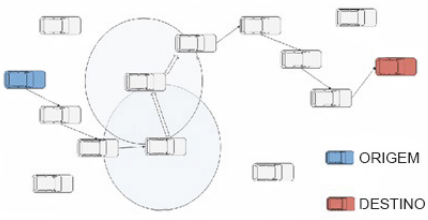

Figura 2. Exemplo do Protocolo de Roteamento Geocast.

2.3. Gerenciamento da Confiança

Em [6], é apresentado métodos que tem como objetivo minimizar a ação dos membros maliciosos, privilegiando aqueles que possuem um comportamento correto e que colaboram com a rede. Entre esses métodos, o sistema de reputação é o que chama mais atenção por ser considerado um dos mais eficientes.

3. Problema

As Redes Tolerantes a Atrasos e Desconexões (DTNs) geralmente são submetidas a condições de carência de recursos, principalmente no que tange a comunicação. Nas VANETs, por exemplo, devido à alta mobilidade dos nós na rede, os usuários sofrem constantes desconexões.

O sucesso da aplicação para esse tipo de rede depende especialmente da colaboração de todos os veículos em busca do benefício coletivo. Contudo, a existência de um ou mais membros agindo de forma maliciosa, é um risco iminente.

Então, visar à redução de membros com comportamentos maliciosos e como consequência, aumentar a segurança das Redes *Ad Hoc* Veiculares, com soluções que motivem a honestidade e a cooperação de seus membros torna-se indispensável [4].

4. Justificativa

As Redes *Ad Hoc* Veiculares tornaram-se uma abordagem muito promissora em Sistemas de Transportes Inteligentes (ITS) e se encontram em ascensão. Segundo [9], a necessidade de aumentar a segurança em ruas e estradas melhorando também o tráfego veicular, é um dos principais estímulos para o uso dessa abordagem.

Ao contrário das VANETs, as Redes *Ad Hoc* Móveis possuem como características: nós estáveis por um maior período de tempo e deslocamento em baixa velocidade, que faz com que os sistemas de reputação existentes para esse tipo de contexto não se adequem em ambientes veiculares [20].

Sistemas distribuídos como VANETs, MANETs e P2P, que não existe uma coordenação geral, são suscetíveis a diversos tipos de ataques. A redução desses ataques é muito importante para as resoluções dos problemas que requerem a cooperação e honestidade coletiva, sendo apresentado em [10], que a detecção da ação dos nós maliciosos tornou-se um dos problemas de segurança mais difíceis em Redes *Ad Hoc* Veiculares.

Logo, a criação de soluções para esses cenários se mostram necessárias. Portanto, este trabalho é uma forma de contribuir com a segurança em redes veiculares, desenvolvendo um mecanismo de reputação que fará o uso de técnicas para detecção e isolamento de usuários mal intencionados.

5. Trabalhos Relacionados

A seguir serão apresentadas as iniciativas relacionadas ao presente trabalho.

Em [15], os autores realizaram um trabalho para aumentar a segurança das decisões tomadas pelos veículos sobre

eventos ocorridos em aplicações LDW (*Local Danger Warning Application*), utilizando um esquema baseado em votação. O sistema desenvolvido melhora a segurança nas redes veiculares de maneira efetiva por meio da utilização de um mecanismo de votação. Entretanto, não é possível verificar no trabalho o quanto este mecanismo aumenta o processamento e o *overhead* das transmissões.

O sistema de reputação DTT (*Dynamic Trust-Token*) [20] proposto pelos autores, possui como objetivo a detecção de alterações nas mensagens transmitidas pela rede, realizando o isolamento dos nós maliciosos de forma que estes não interfiram em transmissões futuras. O mecanismo define a reputação instantaneamente, por utilizar o comportamento dos veículos em tempo de execução. Este trabalho realiza o tratamento apenas dos usuários que violam a integridade das mensagens e não avalia aqueles que propagam informações falsas pela rede.

O mecanismo de reputação VARS (*Vehicle Ad Hoc Network Reputation System*) [4], analisa a relação de confiança individual entre os nós. Desta forma, cada veículo é capaz de adicionar a sua opinião referente as mensagens recebidas e transmitidas pela rede. Na avaliação do sistema, os autores relatam apenas que as simulações realizadas mostraram um grau satisfatório de detecção de membros maliciosos.

O sistema de reputação RMDTV (*Reputation Mechanism for Delay Tolerant Vehicular Networks*) [16], faz a qualificação das informações em corretas ou falsas pelos membros da rede, emitindo mensagens para atestar a confiabilidade do evento informado.

No trabalho de [10] é proposto um sistema que permite avaliar a confiabilidade da mensagem recebida de acordo com a reputação do emissor de origem. Para representar o grau da sua confiança é utilizado uma pontuação numérica. A avaliação foi realizada através de simulações, utilizando como métrica a robustez do sistema em relação aos ataques sofridos pela rede.

5.1. Considerações dos Trabalhos Relacionados

Nos trabalhos analisados, em sua maioria a consulta da reputação é descentralizada, ou seja, não possui uma unidade central que contenha a reputação dos membros da rede. Em [10], a base de reputação utilizada para consultas é centralizada, utilizando servidores de reputação que possuem informações sobre os nós da rede e são os responsáveis por disseminá-los. Já em [20] a base de reputação é local, pois cada nó da rede mantém históricos de avaliações geradas a partir das experiências obtidas com outros membros da rede.

Em relação ao problema de usuários mal intencionados que propagam mensagens e alertas falsos pela rede, apenas a proposta de [20] não trata deste problema, pois avalia apenas a integridade da informação contida nas mensagens transmitidas.

6. Proposta

Inicialmente, está sendo projetado um mecanismo de reputação com o objetivo de identificar as ações realizadas por membros maliciosos. O sistema proposto deverá fazer o descarte das mensagens desses membros, elevando o nível de confiabilidade dos dados recebidos durante a interação dos usuários em uma Rede *Ad Hoc* Veicular.

Este mecanismo será implementado no simulador *ONE* [2] e realizará o gerenciamento das opiniões dos membros, utilizando estas como referência em conexões e transmissões futuras. O armazenamento das opiniões será local (reputação direta) e cada usuário terá uma lista com a reputação obtida dos contatos anteriores, sendo classificados em: Confiável, Malicioso e Neutro/Desconhecido.

A lista vai ser atualizada quando um nó realizar a conexão com outro membro e que este seja considerado confiável por ele, fazendo então a troca de informações sobre a reputação dos seus contatos anteriores (reputação indireta).

Desta forma, a lista com a classificação dos membros será transmitida pela rede, criando grupos de confiança e descartando as mensagens geradas por usuários mal intencionados (Figura 3). Com isso, obterá o condicionamento da rede para disseminação de informações verdadeiras.

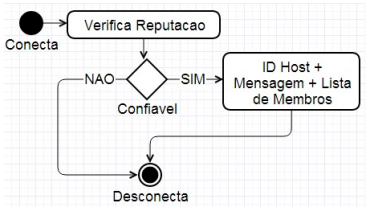

Figura 3. Diagrama UML de Atividades do Recebimento do Evento por um Membro.

O sistema de reputação proposto terá incorporado um modelo de movimento WDM (*Working Day Movement*) [5], fazendo uso de uma aplicação LDW (*Local Danger Warning*) [13] para disseminar os eventos de risco detectados pelos sensores dos veículos. Essas informações serão retransmitidas por nós confiáveis até que atinja um tempo limite (*Threshold*), ou até que seja criada uma revogação do alerta, sinalizando o fim do evento.

O protocolo de roteamento Geocast foi definido para as transmissões das mensagens, pois em aplicações LDW a referência geográfica é muito importante, tendo em vista que os alertas gerados podem ser totalmente irrelevantes para os nós que trafegam no sentido oposto da rodovia.

Para realizar os cálculos de confiança, serão usados os trabalhos de [8] e [12], que consistem em utilizar as informações obtidas em contatos anteriores para o cálculo de uma reputação (direta e indireta) média dos nós, sendo posteriormente definido como métrica para a análise da confiabilidade.

A reputação do remetente da mensagem somente será atribuída após o receptor verificar a veracidade da ocorrência do evento que lhe foi transmitido (Figura 4).

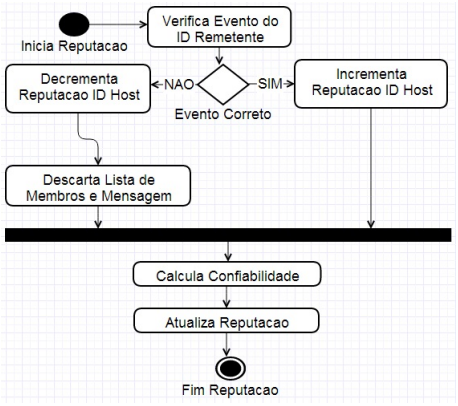

Figura 4. Diagrama UML de Atividades da Reputação do Membro.

7. Conclusão

Atualmente, as VANETs se transformaram em uma grande área de pesquisa, tanto pela comunidade acadêmica quanto pelas grandes indústrias automotivas. Por este motivo, a necessidade de recursos e soluções que tragam confiabilidade para o sistema sem afetar seu desempenho, tornou-se um de seus grandes desafios.

Esse trabalho apresentou as etapas iniciais de uma pesquisa direcionada para análise da confiança dos nós em uma Rede *Ad Hoc* Veicular com vistas a melhorar a credibilidade aos dados transmitidos aos usuários da rede. A solução proposta aborda uma aplicação LDW e possui como principal objetivo a identificação de membros maliciosos, fazendo o descarte de seus alertas por meio de um sistema de reputação.

Ao final de seu desenvolvimento espera-se comprovar a sua eficiência reduzindo o índice de erros das tomadas de decisões dos veículos. Assim, possibilitando elevar a taxa de entrega dos alertas sem afetar o desempenho da rede. Os próximos passos constitui-se então: codificar o mecanismo para posteriores simulações e realizar uma série de análises com base nos resultados obtidos, os quais indicarão a eficiência do mecanismo.

Referências

[1] Ahmed, M.H., Hassan, A., Rahman, Ma. *'Performance evaluation for Multicast transmissions in vanet"*, In: IEEE (CCECE), 2011.

[2] Ari Keranen, Jorg Ott, Teemu Karkkainen. *The ONE Simulator for DTN Protocol Evaluation"*, In: ICSTT, 2009.

[3] Daly, E. M. E Haahr M. *"Social Network Analysis for Routing in MANETs"*, In MobiHoc, 2007.

[4] Dotzer, F., Fischer, L. e Magiera, P. *"Vars: A VANETs reputation system"*, 2005.

[5] Ekman, F., Keranen, A., Karvo, J. e Ott, J. *"Working Day Movement Model"*, In: MobilityModels, 2008.

[6] Feldman, M. E Chuang, J. *"Overcoming freeriding behavior in P2P system"*, 2005.

[7] Fernandes, N., Moreira, M., Velloso, P. *"Ataques e Mecanismos de Segurança em Redes Ad Hoc"*, IN: (SBSeg), 2006.

[8] Igor Mateus A. and Crisluci Karina S. S. *"Projeto: Apostila Virtual - Noções Sobre Confiabilidade"*, In: (UFRN), 2012.

[9] Lee J., Chen W., e V. R. *"Vehicle Local Peer Group Based Multicasting Protocol for V2V Communications"*, 2008.

[10] Li Q., Keith M. Martin e Jie Zhang. *"A Reputation-based Announcement Scheme for VANETs"*, In: IEEE, 2012.

[11] Marwa A. and Imad M.*"A Survey of VANETs Routing Protocols"*, In: (ISSRJ), 2013.

[12] Mello, E. R *'Um modelo de confiança dinâmica em ambientes orientados a serviço"*, In: PhD thesis (UFSC), 2009.

[13] Mitropoulos,Karanasiou and A. Hinsberger *' Wireless Local Danger Warning: Cooperative foresighted driving using intervehicle communication"*, In: IEEE TIT, 2010.

[14] Nikhil D.Karande, Kushal K.Kulkarni. *'Efficient Routing Protocols For VANETs"*, In: (IJERT), 2013.

[15] Ostermaier B., Dotzer F., e Strassberger M. *"Enhancing the Security of LDW in VANETs - A Simulative Analysis of Voting Schemes"*, 2007.

[16] Paula, W.P., Oliveira, S., Nogueira, J.M. *"Um mecanismo de reputação para VDTNs"*, In: SBRC, 2010.

[17] Raya, M. e Hubaux, J. P. *'The security of VANETs"*, In: SASN, 2005.

[18] Salim A., Saadi B. *"Geocast Routing Protocols for VANETs: Survey and Geometry-Driven Scheme Proposal"*, 2013.

[19] Swamynathan, G., Zhao e Zheng. *"Globally Decoupled Reputations for Large Distributed Networks"*, 2007.

[20] Wang, Z., Chigan, C. *"Countermeasure uncooperative behaviors with dynamics trust-token in VANETs"*, In ICC, 2007.

[21] Yousefi, S., Mousavi, M.S., Fathy, M. *'VANETs: challenges and perspectives"*, 2006.