Uma proposta para avaliação de confiança em redes VANETs

Eduardo Pandini[1], Fernando Menezes Matos[2], Aldri Santos[3], Adriano Fiorese[1]

[1]Departamento de Ciência da Computação (DCC)
Universidade do Estado de Santa Catarina (UDESC)
Caixa Postal 631 – 89.219-710 – Joinville – SC – Brasil

[2]Departamento de Sistemas de Computação (DSC)
Universidade Federal da Paraíba (UFPB)
João Pessoa - PB - Brasil

[3]Departamento de Ciência da Computação (DCC)
Universidade Federal de Minas Gerais (UFMG)
Belo Horizonte - MG - Brasil

pandiniedu@gmail.com, fernando@ci.ufpb.pbr

aldri@dcc.ufmg.br, adriano.fiorese@udesc.br

Abstract. *Information trust is a crucial factor for the execution of computational tasks and the security of systems and users. This feature is even more important when sensitive data, whether personal or from third parties, is involved. This importance can be observed in the dynamics of communication, whether capturing or disseminating events, in an ad hoc vehicular networks (VANET). Thus, one of the ways to model such trust is by means of the behavioral analysis of those involved in such a network, so that over time it is possible to correlate such analysis with some degree of reputation. In this case, this degree of reputation can be used as a mechanism to verify the information trust being transmitted indirectly, or, more directly, of the trust of the sender, bringing security to the system against vulnerabilities caused by malicious participants. Therefore, this article presents the development of a tool based on reputation principles to strengthen the security of systems and users of VANET networks.*

Resumo. *A confiabilidade a respeito das informações é fator crucial para a execução de tarefas computacionais e segurança de sistemas e usuários. Essa característica é ainda mais importante quando dados sensíveis, sejam pessoais ou de terceiros estejam envolvidos. É o que acontece na dinâmica de comunicação, seja de captura ou disseminação de eventos, em redes veiculares ad hoc (VANET). Assim, uma das formas de se modelar tal confiabilidade é por meio da análise comportamental dos envolvidos em tal rede, de forma que ao longo do tempo se consiga correlacionar tal análise com algum grau de reputação. Nesse caso, esse grau de reputação pode ser utilizado como mecanismo de verificação da confiabilidade seja da informação sendo transmitida de forma indireta, ou de forma mais direta, da confiabilidade do emissor, trazendo para o sistema segurança contra vulnerabilidades provocadas por participantes maliciosos. Sendo assim, este artigo apresenta o desenvolvimento de uma ferramenta fundamentada em princípios de reputação para fortalecer a segurança dos sistemas e usuários de redes VANET.*

1. Introdução

Uma rede VANET (Vehicular Ad-Hoc Networks) consiste em rede veicular para troca de informações entre veículos (V2V), tendo como foco principal transmitir rapidamente informações sobre acidentes, engarrafamentos ou qualquer situações que coloquem alguma vida em risco [Shrestha et al. 2020] e são a base para IoV (Internet of Vehicles) redes de veículos equipados com tecnologias, sensores e software capazes se realizar a conexão e troca de dados via internet.

VANET's contam com uma grande capacidade de aplicações, tanto para a segurança e comodidade dos motoristas quanto para auxilio na manutenção das rodovias. Desde a troca de mensagens sobre trânsito entre os motoristas, comunicação do estado das estradas para os órgãos gestores até mesmo a sincronização do movimento dos veículos em rodovias e comunicação de acidentes, VANETS apresentam um grande potencial para aprimorar a vida e a eficiência de motoristas e agentes de trânsito.

Contudo, por se tratar de um sistema embarcado, e que portanto não conta com muita capacidade de processamento e armazenagem, juntamente com as características únicas dos veículos, sendo alta mobilidade e implementação esparsa, tal qual se tratar de uma rede espontaneamente criada, fazendo com que as conexões sejam na maioria das vezes feitas com usuários desconhecidos, VANETS enfrentam o desafio de avaliar a credibilidade das mensagens transmitidas, assim como receios quanto a privacidade e segurança dos usuários. A segurança das redes VANET ainda é pouco desenvolvida. Falhas de segurança e ataques são extremamente perigosos em algumas situações. Por exemplo, na sincronização de veículos em uma rodovia um ataque a rede poderia causar um acidente ou alertar erroneamente uma autoridade sobre uma emergência nas vias.

A proposta deste trabalho é desenvolver uma abordagem fundamentada em reputação para ajudar a evitar tais ataques, baseada nas interações prévias e imediatas do usuário na rede.

O restante deste artigo está dividido da seguinte maneira: A Seção 2.1 discute termos e bases necessárias para o entendimento das redes VANET, e a Seção 2.2 os termos, bases e conceitos de confiança e segurança. A Seção 3 contem uma análise de trabalhos relacionados a redes VANET, sua segurança, assim como estudos utilizando confiança já realizados. A Seção 4 propõe um modelo de cálculo da confiança dos veículos envolvidos na rede VANET, assim como as ferramentas utilizadas para desenvolvimento e teste do modelo. A Seção 5 apresenta as considerações finais.

2. Referencial Teórico

Para compreensão da proposta apresentada vários conceitos são necessários e serão dessa forma apresentados.

2.1. Contextualização de VANET

Dispositivos minúsculos cada vez mais poderosos estão sendo desenvolvidos que podem ser incorporados em sistemas maiores e ainda possuírem capacidade de comunicação em rede. Este aparecimento de novos dispositivos também levou a muitas inovações em tecnologias de rede, que são referidas sob a categoria de Internet das Coisas (IoT) [Ashton et al. 2009].

Uma das subcategorias de IoT, MANET (Mobile Ad-Hoc Network) tenta criar a conexão de dispositivos moveis, tipicamente carregados por pessoas, para a criação de uma rede. Como apenas os dispositivos estão conectados e não há dispositivos de infraestrutura de gerenciamento, como roteadores ou torres telefônicas, essas redes são consideradas redes ad-hoc. [Lee and Atkison 2021]. Estas redes permitem a troca de dados entre todo e qualquer usuário na rede atualmente a seu redor. Redes MANET levaram a criação de uma nova categoria, voltada para a conexão de dispositivos movidos por veículos, chamada de VANET (Vehicular Ad-Hoc Network).

Existem dois tipos de entidades usadas em VANET - Veículos e unidades de beira de estrada (RSU). Os veículos são as entidades de comunicação em VANET. Estes veículos transmitem suas posições atuais por meio de mensagens de *beacon*, por exemplo. Existe um intervalo fixo durante o qual os veículos transmitem tais mensagens [Grover et al. 2013]. A VANET difere da MANET, pois fornece maior mobilidade de nós, redes de maior escala, topologia restrita geograficamente e fragmentação de rede frequente [Grover et al. 2013].

2.2. Contextualização de Confiança

Confiança se refere à segurança em termos de relacionamento que uma entidade VANET tem em outra entidade. Baseia-se na expectativa de que a outra entidade realizará uma ação acreditada/esperada/aceita. A confiança representa o grau em que uma entidade deve ser confiável e demonstrar um comportamento seguro durante qualquer interação com outras entidades.

O estabelecimento de confiança desempenha um papel fundamental na prevenção de ataques na VANET. As entidades envolvidas na defesa da rede contra tais ataques devem estabelecer confiança mútua para que a rede opere sem problemas. É um grande desafio, pois um nó receptor precisa garantir autenticidade e confiabilidade das mensagens recebidas antes de reagir a elas. Existem diversas fórmulas de realizar o cálculo de confiança dos usuários, e estes podem ser categorizados das seguintes formas:

- Cálculo de confiança global: Também chamada de confiança centralizada, a confiança dos usuários da rede é calculada por uma unidade central e distribuída entre os usuários para consulta.
- Cálculo de confiança local: Também chamada de confiança descentralizada, a confiança é calculada por cada usuário e é única para si.
- Cálculo proativo: O cálculo da confiança é realizado em intervalos pré-determinados de tempo.
- Cálculo reativo: O cálculo de confiança é realizado em situações pré-determinadas na rede.

Dadas as características da rede, assim como as características do cálculo de confiança, segundo [Grover et al. 2013] o estabelecimento deste cálculo deve respeitar as seguintes condições:

- Distribuído: A abordagem de gerenciamento de confiança deve ser distribuída para ser aplicável ao ambiente altamente dinâmico e distribuído de VANET. Todos os veículos devem ser capazes de avaliar seus vizinhos de forma independente.
- Dinâmico: O sistema deve reagir imediatamente, assim que evidências suficientes são encontradas. O sistema não deve apenas manter a gradação dos nós, mas

também deve ser flexível para reagir rapidamente a qualquer tipo de mau comportamento.

- Justo: O resultado do sistema de avaliação de confiança deve ser significativo. Enquanto não houver evidência de confiabilidade ou falta de confiabilidade dos veículos, o sistema permanece neutro. Apenas os veículos com mau comportamento devem ser detectados, ou seja, não deve haver quaisquer falsos positivos e falsos negativos.
- Adequadamente gerenciável: A análise de comportamento de todos os nós envolvidos no cálculo de confiança deve ser integrada. A avaliação deve tratar a perda de mensagens corretamente. Uma perda de pacote de um veículo honesto não deve atribuir uma classificação negativa pois a comunicação pode não ser estável.
- Qualidade Independente da Avaliação: A qualidade da avaliação deve ser independente de diferentes cenários de tráfego. As capacidades do sistema de avaliação podem ser diferentes devido a diferentes condições de tráfego. O sistema de avaliação deve trocar avaliações positivas locais apenas para melhorar a avaliação da comunidade local em termos de confiabilidade.
- Sem loop de distribuição de confiança: A troca de valores de confiança deve ser limitada a classificações locais. Apenas um sistema de reputação de um nível é necessário. Classificações de confiança local e cooperativa não devem ser enviadas para outros nós na rede pois os valores podem ser falsamente aumentados em loops.
- Desconhecimento da desconfiança dos membros: Ao trocar as classificações de confiança com os vizinhos, o usuário não deve estar ciente quando é classificado como não confiável. Por exemplo, se um atacante está forjando a posição de algum outro nó, ele não deve encontrar evidencia para provar que não é mais confiável, e portanto, poder mudar sua identidade para obter classificação neutra novamente.
- Escalável: É uma perspectiva importante no gerenciamento de confiança no meio VANET. Por exemplo, no cenário VANET de alta densidade, o número de veículos e informações podem ser muito grandes. Já considerando um cenário de baixa densidade, um só nó tem que tomar decisões muito rapidamente para situações críticas, e portanto tem que consultar ou aceitar informações de apenas um número pequeno de pares. O numero de consultas para a tomada de decisão pode ser inconsistente no cenário dinâmico de VANETS, e quando mal otimizado pode levar a tomadas de decisão incorretas, ou um tempo de resposta inviável. Um sistema de gestão de confiança eficiente garante que o número seja definido como um valor pequeno para levar em conta a escalabilidade.

3. Trabalhos relacionados

[Zhang et al. 2020] desenvolvem um método próprio chamado AATMS (anti-attack trust management scheme). O cálculo de confiança da ferramenta AATMS pode ser realizado remotamente, em uma unidade não relacionada ao veículo recebendo a mensagem, também conhecido como confiança global, ou localmente, no momento do recebimento da mensagem, também conhecido como confiança local. Resultados da simulação mostram que AATMS consegue eficientemente calcular a confiança e desconfiança de veículos até mesmo sob ataques maliciosos. Pode-se perceber deste trabalho as vantagens de um sistema de confiança global aliado com um sistema de confiança local.

[Pu 2021] desenvolve um método próprio, chamado Block MCDM para aplicação em VANETs, onde cada veículo avalia a credibilidade da mensagem recebida e gera o valor de confiança do veículo que fez o envio. Cada veículo periodicamente realiza o upload dos valores de confiança a uma RSU. Quando informações suficientes são recebidas, de diversos veículos, a própria RSU realiza o cálculo da confiança global, coloca essas informações em um bloco e os cunha na blockchain. Os testes mostram que o Thrust Block MCDM apresenta melhora na detecção de mensagens falsas e detecção de veículos maliciosos quando comparado ao modelo prévio de gerenciamento de confiança descentralizado. Além de apresentar uma melhora quando comparado aos métodos utilizados previamente, o uso de um sistema blockchain auxilia com o problema de armazenamento das informações da rede.

[Arif et al. 2019] fornecem uma ampla visão geral dos ITS (Intrusion detection systems, refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados) e da evolução do ITS para VANETs. Assim como os detalhes de VANETs, discute os ataques de privacidade e segurança em VANETs com suas aplicações e desafios. Aborda a eficácia de VANETs e computação em nuvem com arquitetura e questões relacionadas à privacidade e segurança. Também examina os protocolos de comunicação para cada camada de rede com os ataques relevantes ocorridos em cada camada. Também discute os benefícios potenciais das diferentes técnicas propostas relacionadas a VANETs, aplicação e desafios em detalhes. Ao final, fornece uma conclusão com algumas questões em aberto e emergentes em VANETs.

[Alladi et al. 2022] cataloga as principais contribuições relacionadas a requerimentos de segurança da utilização de blockchains em redes VANET, tais quais: Descentralização, transparência, resistência a ataques e auditabilidade pública.

[Yong-hao 2020] desenvolve um modelo de cálculo de confiança para Internet of Vehicles (IOV). O modelo utiliza as interações sociais do proprietário do veículo para definir o Trust inicial, avalia o Trust direto após avaliação de outro nó seguindo uma interação. Procura satisfazer a necessidade de uma tomada de decisão rápida limitando o comprimento do caminho quando avaliando a confiança. Os experimentos mostram que o modelo pode ajudar a estabelecer rotas estáveis e relacionamentos de Trust confiáveis entre veículos.

[Kim and Bae 2012] propõe um sistema de gerenciamento de reputação para redes VANETs, baseado em mau comportamento que é composto por três componentes: 1) detecção de mau comportamento; ii) re-disseminação de eventos e iii) algoritmos de remoção global de participantes em função do mau comportamento que detectam e filtram dados falsos.

[Malhi et al. 2020] O survey trata de 4 pontos: Ataques e sistemas de segurança em VANETs, análise comparativa de sistemas de segurança baseada nos mecanismos de criptografia utilizados, esquemas de gerenciamento de confiança baseados em características discretas e sistemas de detecção de intrusão e problemas em aberto que necessitam de maior consideração no futuro.

4. Uma Proposta Baseada em Análise Comportamental

O cálculo da confiança dos veículos na rede VANET será realizado utilizando fundamentos de confiança distribuída assim como global, e será baseado em 2 fatores básicos: a

idade do usuário na rede e suas interações prévias e imediatas, assim como o auxilio de uma base de comportamentos considerados maliciosos ou indesejados.

Como observado na Figura 1, o cálculo da confiança será realizado com a junção da observação imediata e o histórico da rede. Assim, todos os usuários participantes de uma transação terão seus coeficientes de confiança calculados, primeiramente fazendo sua própria avaliação do comportamento do usuário desejado, com base nos comportamentos esperados, e então juntamente com o histórico de comportamento prévio fornecido pela rede. Dados estes dois números, o novo coeficiente de confiança é calculado, disponibilizado ao usuário, para que este decida se irá ou não continuar a transação, e disponibilizado para o restante da rede, para consultas futuras.

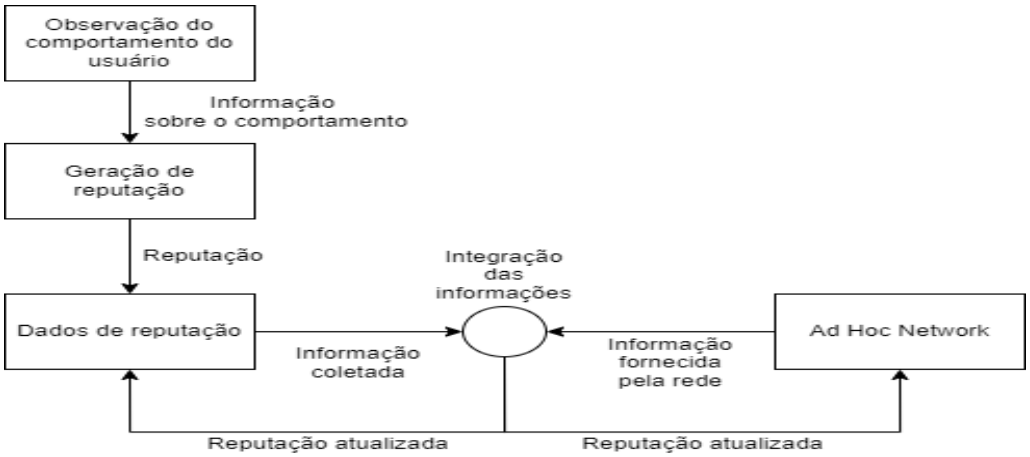

Figure 1. Arquitetura do cálculo de confiança

Exemplificando, supomos que $R(i, j)$ seja uma relação de confiança entre as entidades (veículos) i e j. Se a entidade i quiser alguma ação executada pela entidade j, e se j está executando com sucesso esta ação, j é uma entidade confiável para i. A entidade i aumentará o valor de confiança de j por seu bom comportamento. Por outro lado, caso j não esteja realizando a ação desejada, ou realize de forma errônea ou maliciosa, a entidade i reduz a confiança de j conforme a gravidade da infração. Do mesmo modo, se a ação requerida por i seja classificada como maliciosa segundo os comportamentos esperados, i terá sua reputação reduzida.

O histórico do usuário apresenta uma simples, porém efetiva maneira de realizar o cálculo da confiança, assim como a idade do usuário na rede, já que este indica que o usuário já está a uma quantidade de tempo apresentando comportamento no mínimo não malicioso.

A Equação 1 apresenta o cálculo da confiança do veículo j.

$$C_j = T_j + H_j \tag{1}$$

Nela, C_j representa o valor da confiança do veículo j. O termo T_j representa o tempo em que o veículo j está participando da VANET, e de acordo com a Equação 2 demonstra que quanto maior o tempo de participação maior o valor atribuído. Nesse caso,

o termo ts_j indica o tempo de atuação/permanência na VANET do veículo j, em meses. Também serve para a pontuação inicial de veículos que recém entraram na VANET e ainda não possuem um histórico de colaboração e portanto nenhum histórico de avaliações de comportamento. Os valores atribuídos ao tempo de participação na rede estão sujeitos a mudança de acordo com resultados de testes futuros.

$$T_j = \begin{cases} 0,1 \text{ se } ts_j < 1 \\ 0,2 \text{ se } 1 \leq ts_j < 2 \\ . \\ . \\ 0,9 \text{ se } 9 \leq ts_j < 10 \\ 1,0 \text{ se } ts_j \geq 10 \end{cases} \tag{2}$$

Por sua vez, a Equação 3 apresenta o termo H_j que representa o valor resultante da média móvel exponencialmente ponderada das n avaliações (A_i) de comportamento atribuídas ao veículo j de acordo com seu comportamento. Nesse caso, n corresponde ao número de sessões, i.e., participações ou iterações, de avaliação na VANET.

$$H_j = \frac{\sum_{i=1}^{n} A_i * i}{\sum_{i=1}^{n} i} \tag{3}$$

Para o teste do modelo representado pelas Equações 1, 2 e 3 estão sendo utilizados os softwares NS3, um simulador de redes, o software SUMO, um simulador de mobilidade urbana, especificamente com o módulo MINUET [Andrade et al. 2020], e o projeto Luxembourg SUMO Traffic (LuST) [Codecá et al. 2017] como cenário de mobilidade de tráfego real. O NS3 permite simulações mais próximas da realidade, já que contempla diversas características dos ambientes de redes, como interferência no meio.

5. Considerações Finais

Até o momento foi realizada uma revisão bibliográfica e atualmente está sendo realizada a modelagem para o cálculo da reputação. Nesse sentido, está se trabalhando com características que possam de alguma forma modelar comportamento dos participantes, como por exemplo, itinerários e frequência desses itinerários, de forma objetiva. Ainda, pretende-se adicionar características que modelem comportamentos subjetivos de forma a mesclar de forma equilibrada esses dois fatores de risco (objetivo e subjetivo).

Caso a proposta de avaliação gere resultados positivos, poderá ser uma ferramenta leve e eficiente de acrescentar mais segurança as redes VANET, e deste modo viabilizar sua utilização em cenários mais delicados, além de fornecer mais confiança para usuários da rede.

Referências

Alladi, T., Chamola, V., Sahu, N., Venkatesh, V., Goyal, A., and Guizani, M. (2022). A comprehensive survey on the applications of blockchain for securing vehicular networks. *IEEE Communications Surveys & Tutorials*.

Andrade, E., Veloso, K., Vasconcelos, N., Santos, A., and Matos, F. (2020). Cooperative monitoring and dissemination of urban events supported by dynamic clustering of vehicles. *Pervasive and Mobile Computing*, 67:101244.

Arif, M., Wang, G., Bhuiyan, M. Z. A., Wang, T., and Chen, J. (2019). A survey on security attacks in vanets: Communication, applications and challenges. *Vehicular Communications*, 19:100179.

Ashton, K. et al. (2009). That 'internet of things' thing. *RFID journal*, 22(7):97–114.

Codecá, L., Frank, R., Faye, S., and Engel, T. (2017). Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation. *IEEE Intelligent Transportation Systems Magazine*, 9(2):52–63.

Grover, J., Gaur, M., and Laxmi, V. (2013). *Trust Establishment Techniques in VANET*, pages 273–301. Springer Berlin Heidelberg.

Kim, C.-H. and Bae, I.-H. (2012). A Misbehavior-Based Reputation Management System for VANETs. In Park, J. J. J. H., Jeong, Y.-S., Park, S. O., and Chen, H.-C., editors, *Embedded and Multimedia Computing Technology and Service*, Lecture Notes in Electrical Engineering, pages 441–450, Dordrecht. Springer Netherlands.

Lee, M. and Atkison, T. (2021). Vanet applications: Past, present, and future. *Vehicular Communications*, 28:100310.

Malhi, A. K., Batra, S., and Pannu, H. S. (2020). Security of vehicular ad-hoc networks: A comprehensive survey. *Computers & Security*, 89:101664.

Pu, C. (2021). A novel blockchain-based trust management scheme for vehicular networks. In *2021 wireless telecommunications symposium (WTS)*, pages 1–6. IEEE.

Shrestha, R., Bajracharya, R., Shrestha, A. P., and Nam, S. Y. (2020). A new type of blockchain for secure message exchange in vanet. *Digital communications and networks*, 6(2):177–186.

Yong-hao, W. (2020). A trust management model for internet of vehicles. In *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, pages 136–140.

Zhang, J., Zheng, K., Zhang, D., and Yan, B. (2020). Aatms: An anti-attack trust management scheme in vanet. *IEEE Access*, 8:21077–21090.