Computer Networks 121 (2017) 152–172

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A game theory based trust model for Vehicular Ad hoc Networks (VANETs)

Muhammad Mohsin Mehdi, Imran Raza*, Syed Asad Hussain

Department of Computer Science, COMSATS Institute of Information Technology Lahore, Pakistan

ARTICLE INFO

Article history:
Received 12 July 2016
Revised 22 March 2017
Accepted 7 April 2017
Available online 13 April 2017

Keywords:
Game theory
Nash equilibrium
Trust
VANETs

ABSTRACT

Vehicular Ad hoc Networks (VANETs) facilitate road safety, transportation security, reliability and management. This paper presents a game theory based trust model for VANETs. The proposed model is based on an attacker and defender security game to identify and counter the attacker/malicious nodes. The parameters considered for attackers and defender's strategy are majority opinion, betweenness centrality, and node density. The outcome of the specific game is determined by the game matrix which contains the cost (payoff) values for possible action-reaction combination. Nash equilibrium when applied to calculate the best strategy for attacker and defender vehicles. The model is simulated in Network Simulator (ns2), and results show that the proposed model performs better than the schemes with random malicious nodes and existing game theory based approach in terms of throughput, retransmission attempts and data drop rate for different attacker and defender scenarios.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

In a highway scenario, Vehicular Ad-Hoc Networks (VANETs) consisting of high speed nodes need to log connection details providing road safety, transportation security, and reliability. The nodes communicate constantly and may share impersonated events such as false accidents, incorrect traffic conditions and false response from Road Side Units (RSUs). Therefore, the reliability of an event depends on the authenticity of a node and some reliable tagged nodes such as emergency vehicles which are reliable to report an event without any discrepancy. The authenticity of the node is calculated using majority opinion and betweenness centrality explained in detail in their respective sections. It is challenging to provide reliable communication in VANETs, especially in highway scenarios, as frequent addition and removal of nodes compromises the detection of malicious nodes. Therefore, VANETs need a robust approach to handle fast changing network topology to defend and react against an attack. The possibility of an attack is a checked exception and hence needs to be handled establishing trustworthy Intelligent Transportation System (ITS). The time critical nature of highway scenarios requires a node to verify the accuracy of the received information in real time. Different trust and reputation models [1] have been presented to classify inaccurate messages and malicious vehicles. Trust establishment schemes are available for peer-to-peer, sensors, and Mobile Ad-hoc Networks (MANETs) [1,2]. However, trust establishment in VANETs is challenging because of dynamic network topology, increase and variance of malicious nodes, and absence of a third party for network monitoring. The only possible communication with the infrastructure takes place with RSUs. Therefore, centralized systems are not suitable to establish trust in VANETs. Furthermore, high speed vehicles make it difficult to log quality of experience between them. The existing entity oriented trust models for VANETs are based on the verification of vehicles' identities and their legitimacy in the network [3–5]. In identity-based system, the trust metric is linked to the vehicle credentials and does not consider its trustworthiness. Other trust models are based on a data-oriented approach, where the vehicles are responsible for the trustworthiness of the information that it generates.

This paper presents a game theory based trust model for VANETs implementing a robust algorithm that calculates three parameters; majority opinion, betweenness centrality and node density. The proposed trust model verifies the information and messages to identify trusted nodes for reliable communication. This enables a node to have better understanding of the network and its surroundings to acknowledge both destructive and informative events. The proposed model modifies Ad-hoc On-demand Distance Vector (AODV) routing protocol [4] to maintain a log for every successful route. The proposed model is simulated using Network Simulator (ns2) [5] implementing both attacker and defender with a target i.e. an attack is always detected and deceived. In

* Corresponding author.
E-mail addresses: mohsin.mehdi@ciitlahore.edu.pk (M.M. Mehdi), iraza@ciitlahore.edu.pk (I. Raza), asadhussain@ciitlahore.edu.pk (S.A. Hussain).

http://dx.doi.org/10.1016/j.comnet.2017.04.024
1389-1286/© 2017 Elsevier B.V. All rights reserved.

the proposed model the majority opinion calculates the trust level based on event information for each communication cycle between nodes. The trust level is set high for certain vehicles such as police cars, and maintenance vehicles to report the trustworthiness of events successfully. The betweenness centrality calculates importance of a node based on the number of times it is accessed/chosen during a shortest path between two nodes. A node becomes central and important if it is accessed more frequently. The third parameter node density computes the number of nodes having similar speed and direction. The proposed model self-evolves with the changes in the network using majority opinion, betweenness centrality and node density. These three parameters are calculated for an attacker and defender scenario, categorizing an attacker node. The proposed model follows game theoretic approach implementing Nash equilibrium to calculate best strategy for attacker and defender through a payoff matrix. The proposed model maintains communication details in the form of a text file using node memory. The log size of a simulation scenario implementing dynamically changing 100 nodes is not more than 300 KB, and this does not affect battery usage.

The proposed model does not result in any routing complexity. The rest of the article is organized as follows: Section 2 enlists our contributions. Section 3 briefly reviews the existing trust models. Section 4 describes the proposed game theoretic trust model. Section 5 presents the performance evaluation and simulation results. Section 6 concludes the paper.

2. Our contributions

The proposed model dynamically calculates majority opinion, betweenness centrality and node density to identify an attack. Our contribution can be summarized as follows:

1. We have introduced a game theoretical approach for VANETs that allows the normal nodes, tagged as defenders, to intelligently monitor the network for reliability.
2. Unlike traditional security measures in VANETs, the proposed algorithm allows the defender nodes to avoid attacker nodes with the help of Centrality Measure C_m, Trust Level E_p and Node Density N_D.
3. We have used the information provided by service vehicles and RSUs to identify the status of an event for calculating the trust level of the corresponding node.
4. Our algorithm intelligently identifies both attacker and defender to deploy suitable strategies.
5. The proposed algorithm is validated against various performance parameters and real time simulation scenarios. The simulation results show that although with initial success the attacker nodes can affect the communication between nodes. But due to dynamic nature of the algorithm, defender nodes eventually neutralize a malicious activity. The comparison graphs show that the defender node performs better with its best strategy while neutralizing an attacker node with best strategy.
6. We have compared the simulation results of the proposed model with another scheme [18]. The comparative results show that the proposed scheme performs better in different network scenarios.

3. Related work

VANETs have scarce resources in terms of battery timings, memory and trivial connectivity [6]. That is why complex security algorithms are very difficult to implement. Some conventional methods like Key Management Schemes are resource intensive. Cryptography techniques cause a huge amount of communication and computation overhead. Due to this, game theory based approach was introduced to use minimum resources of attacker and defender nodes. Most Game theory based trust calculation approaches for security are based on experience and recommendations. Hence message authenticity is not a requirement. Game theory based schemes for VANETs focus on nonrepudiation of messages by evaluating quality and unrealistic information from nodes. Light weight self-organized trust (LSOT) model discussed in [8] is self-organized and have super nodes as tagged nodes to calculate trust. LSOT have trust-certification and recommendation based evaluation. LSOT have high robustness against collusion attack than other models. Maximum Local Trust(MLT) algorithm[8] identifies trustworthy recommenders in terms of recommendation-based evaluation. This model fails in the absence of service nodes. A security review in [7] evaluates reliable communication techniques implementing complex message authentication. These techniques demand more resources in terms of time and memory, therefore, their implementation in VANETs is more challenging. Authors have mentioned these problems and referenced that these techniques are still in process of improvement. In [9], authors proposed a scheme for reliable communication, floating trust certificates of each node in the network. These trust certificates have different verification parameters like acknowledgement packets and recommendation tags from other nodes. These parameters are recorded over certain period with certain number of communication links. In [10], authors have reviewed security and privacy techniques for VANETs. They proposed a technique based on experience and communication reliability provided by RSUs. The dependency on RSUs or other maintenance vehicles has limited the scope of VANET security. A complete survey of six well known security schemes is given in [11]. Each of these techniques has provided a separate mechanism, method or an algorithm for calculating trust for reliable communication between the nodes. Some of these techniques use cryptographic techniques for message security but are unable to identify the attackers. These techniques also result in more battery consumption. One of these techniques used RSUs and public keys resulting in deadlock due to huge amount of communication attempts. Other techniques have used fuzzy set classifiers and reputation based trust calculation. All these techniques have their own advantages and disadvantages. Some techniques for message reliability in VANETs are based on bad mouthing, balloting and collusion. Authors in [12] proposed a technique which collects recommendations based on such word of mouth parameters. The other parameters are certain time slots based on number of interactions, compatibility of information and closeness between the nodes. The simulation results are based on small area hence it can be concluded that these parameters may create deadlock in larger areas due to possibility of communication timeout. A rather comprehensive technique for trust calculation has been introduced in [13]. It calculates the trust based on energy, communication and data. All these trust values are calculated based on the experiences shared by nodes among themselves. Similarly, a location awareness routing protocol has been presented in [14]. This technique is more related to location based privacy and message authenticity of underwater WSN. In [15], authors proposed a reputation based trust calculation scheme for service oriented social networks. The proposed scheme cannot cater speed of nodes and hence cannot be applied in VANETs. A Bayesian network based trust management for WSN, MANETs and P2P networks has been proposed in [16] and [17]. The application of Bayesian Network comes with other complexities such as communication deadlock or time overlay. None of these techniques have mentioned the possibilities of having this model applied in VANETs. Authors in [18] propose two parameters for calculating trust for game theory approach for VANET security. First parameter is betweenness centrality and second is the use of service vehicles. Also, this paper presents detailed analysis of all network possibilities. We have selected and simulated this paper for comparative analysis.

Download English Version:

https://daneshyari.com/en/article/4954731

Download Persian Version:

https://daneshyari.com/article/4954731

Daneshyari.com