Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 965 – 972

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks

Uzma Khan[a,*], Shikha Agrawal[a], Sanjay Silakari[a]

[a]*University Institute of Technology, RGPV, Bhopal (M.P.) 462036, India*

Abstract

VANETs enable wireless communication among vehicles and vehicle to infrastructure. Its main objective is to render safety, comfort and convenience on the road. VANET is different from ad-hoc networks due to its unique characteristics. However, because of lack of infrastructure and centralized administration, it becomes vulnerable to misbehaviors. This greatly threatens different aspects of VANET's security. VANET being such a useful network must provide adequate security measures for secure communication. The proposed algorithm DMN-Detection of Malicious Nodes in VANETs improves DMV Algorithm in terms of effective selection of verifiers for detection of malicious nodes and hence improves the network performance.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: Malicious; Misbehaviour; Detection; Security;Performance; Vehicular Ad-Hoc Networks (VANETs).

1. Introduction

Traditional wired networks have mechanism for protection by various means of defence like gateways, firewalls etc. However, wireless networks are susceptible to security attacks targeting almost the entire network from any direction. Therefore, VANETs being an Ad-hoc Network are at risk of various misbehaviours like tampering of messages, eavesdropping, spamming, masquerading etc because of lack of centralized administration [1, 5, 21]. Security

* Corresponding author. Tel.: +91 8878881518.
E-mail addresses:uzma.khancs@gmail.com, shikha@rgtu.net, ssilakari@yahoo.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.01.006

of VANETs has been identified as one of the major challenge[8]. VANETs applications support real time communication and deals with life critical information. In order to do it correctly and effectively, it must follow the security requirements such as integrity, confidentiality, privacy, non repudiation and authentication to protect against attackers and malicious vehicular nodes [3, 22, 23].

Different misbehavior detection schemes have been proposed by researchers in order to identify the attackers responsible for misconducts in VANETs. Detection of such malicious nodes and abnormal activities in the network is very significant in order to devise precautionary measures for it. This paper proposes a node centric detection scheme called DMN (Detection of Malicious Nodes) which effectively detects malicious nodes that drop and duplicate packets in the network using monitoring approach. Nodes are being monitored by the verifiers which qualify the selection threshold. Thus, instead of selecting all the trustworthy nodes, only the most suitable nodes perform the job of monitoring other node's behavior. This helps to utilize the network resources properly which is generally overlooked by the researchers in their detection schemes. This, in turn improves the network performance which is one of the major requirement of security schemes for complex networks like VANETs.

The paper is organized as follows: Section 2 discusses the various node-centric and data-centric techniques for detecting misbehavior and malicious nodes in VANETs. Section 3 presents the DMN algorithm in detail. Performance evaluation and its comparative analysis are discussed in Section 4. Conclusion and Future work are stated in Section 5.

2. Related Work

Number of schemes has been proposed to detect misbehavior and malicious nodes in Vehicular Ad-hoc Networks. The misbehavior detection schemes can be broadly classified into following two types: Node-centric and Data-centric misbehavior detection schemes.

2.1. Node Centric Misbehavior Detection Schemes

Node-centric techniques need to distinguish among different nodes using authentication. Security credentials, digital signatures, etc are used to authenticate the node transferring the message. Such schemes emphasis on the nodes transmitting the messages rather than the data transferred.

In the research work [9, 10], Gosh et al. have proposed a robust scheme to detect malicious vehicles for Post Crash Notification application. They have considered the possibility of the fake position information of the vehicle in the PCN along with the false crash alert in [10]. Kim et al.[6] have proposed a novel Misbehavior Based Reputation Management Scheme (MBRMS) which includes three components a) Misbehavior detection b) Event rebroadcast and c) Global eviction algorithms for the detection and filtration of false information in vehicular ad-hoc networks. Daeinabi et al.[3] have proposed a detection algorithm called DMV to discover malicious nodes through observations that duplicates or drops received packets and isolates such vehicles from honest nodes. Vehicles are tagged using a distrust value and are monitored by the allocated verifier nodes. Wahab et al.[16] have used Quality of Service-Optimized Link State Routing (QoS-OLSR) clustering algorithm to detect malicious vehicles in (VANET) using Dempster–Shafer based cooperative watchdog model. This method maintains stability and quality of service with increase in detection probability and decreases the number of selfish nodes and false negatives. Kadam et al. have presented a new approach[14] for not solely the detection of malicious vehicles attack, additionally their prevention from the VANET. It is an improvement of the Detection of Malicious Vehicles (DMV) algorithm [3]. This approach reduced the impact of black hole attack within VANET and is more efficient and secure compared to DMV.

2.2 Data Centric Misbehavior Detection Schemes

Data-centric approach inspects the data transmitted among nodes to detect misbehaviors. It is primarily concerned with linking between messages than identities of the individual nodes. The information disseminated by the nodes in the network is analyzed and compared with the information received by the other nodes, in order to