Egyptian Informatics Journal xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)

Parul Tyagi [a,*], Deepak Dembla [b]

[a] Dept of ECE, JECRC University, Jaipur 303905, India
[b] Dept of Computer Science, JECRC University, Jaipur 303905, India

ARTICLE INFO

Article history:
Received 23 December 2015
Revised 23 August 2016
Accepted 7 November 2016
Available online xxxx

Keywords:
Routing protocol
Mobile ad hoc network (MANET)
Vehicular ad hoc network (VANET)
Black Hole Attack
Malicious node
Throughput

ABSTRACT

Next-generation communication networks have become widely popular as *ad-hoc* networks, broadly categorized as the mobile nodes based on mobile *ad-hoc* networks (MANET) and the vehicular nodes based vehicular ad-hoc networks (VANET). VANET is aimed at maintaining safety to vehicle drivers by begin autonomous communication with the nearby vehicles. Each vehicle in the ad-hoc network performs as an intelligent mobile node characterized by high mobility and formation of dynamic networks. The ad-hoc networks are decentralized dynamic networks that need efficient and secure communication requirements due to the vehicles being persistently in motion. These networks are more susceptible to various attacks like Warm Hole attacks, denial of service attacks and Black Hole Attacks. The paper is a novel attempt to examine and investigate the security features of the routing protocols in VANET, applicability of AODV (Ad hoc On Demand) protocol to detect and tackle a particular category of network attacks, known as the Black Hole Attacks. A new algorithm is proposed to enhance the security mechanism of AODV protocol and to introduce a mechanism to detect Black Hole Attacks and to prevent the network from such attacks in which source node stores all route replies in a look up table. This table stores the sequences of all route reply, arranged in ascending order using PUSH and POP operations. The priority is calculated based on sequence number and discard the RREP having presumably very high destination sequence number. The result show that proposed algorithm for detection and prevention of Black Hole Attack increases security in Intelligent Transportation System (ITS) and reduces the effect of malicious node in the VANET. NCTUNs simulator is used in this research work.

1. Introduction

Vehicle to vehicle communication (V2V) and Intelligent Transportation Systems (ITS) have emerged as a reliable solution to a number of inconveniences faced by drivers and commuters on the road. Vehicular communication (VC) architecture utilizes a specific wireless communication frequency band known as the dedicated short-range communication (DSRC) band that enables wireless coverage to provide the wireless access in vehicular environments (WAVE). WAVE allows vehicles within specified vicinity to interact with the road side infrastructure (V2I communication) and also with other neighboring vehicles (V2V communication). These vehicles have lack of centralized controlling authority and form a distributed network, characterized by dynamic movement and self organization of nodes, leading to vehicular ad-hoc networks (VANET). Whereas the nodes in MANET cannot recharge their battery power, provisions exist for VANET nodes to recharge themselves at frequent intervals [1]. A pictorial display of a typical V2V and V2I communication scenario is shown in Fig. 1.

Two types of such units that provide V2V and V2I communications are the On Board Unit (OBU) inside the vehicles and the Road Side Unit (RSU) installed along the travel zones. Increasing number of car-manufacturers employ the VANET framework to incorporate more and more comfort and security applications of VANET. Due to high mobility of nodes, executing efficient data transmission in VANET needs appropriate communication protocol. VANET nodes traverse a fixed number of internet gateways at high speed to

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

* Corresponding author.
E-mail addresses: parultyagi.ece@jecrc.ac.in, tyagi.parul82@gmail.com (P. Tyagi), deepak.dembla@jecrcu.edu.in (D. Dembla).

http://dx.doi.org/10.1016/j.eij.2016.11.003
1110-8665/© 2016 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.

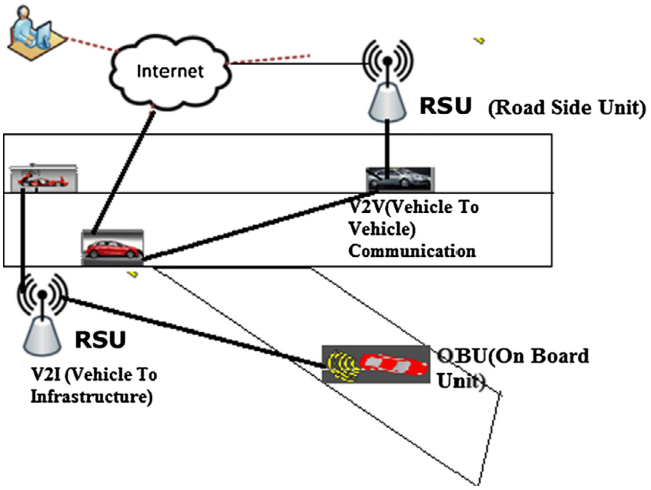
Internet
RSU (Road Side Unit)
V2V(Vehicle To Vehicle) Communication
RSU
V2I (Vehicle To Infrastructure)
OBU(On Board Unit)

Figure 1. Vehicular ad hoc networks.

forward data and then get disconnected from the network as they fall out of the wireless coverage range. Link reliability model is used to compute and predict the optimum probability of future status (formation and disruption of links among nodes) in wireless link [2].

VANET is susceptible to a number of attacks and malicious intrusions, and designing stronger routing protocols would contribute towards making the networks less prone to attacks. This paper presents an insight into the working and performance characteristics of two commonly used VANET protocols: DSR [3] and AODV [4]. The original version and implementation of the AODV protocol was centered on efficient routing of data packets, but had little consideration for security aspects and we have designed a algorithm to enhance the security mechanism of AODV protocol and to introduce a mechanism to detect Black Hole Attacks and to prevent the network from such attacks in which source node stores all route replies in a look up table. This table stores the sequences of all route reply, arranged in ascending order using PUSH and POP operations. The priority is calculated based on sequence number and discard the RREP having presumably very high destination sequence number.

2. Related work

Significant amount of research has analyzed the security aspects of routing protocols used in VANET described as follows:

Yi et al. [7] investigated Security-Aware Ad hoc Routing (SAR) protocol using trust values and relationships. The work yielded some results having varying percentages of message packets transmitted by unauthorized and malicious nodes, indicating flaws in the security aspects of ad-hoc network communication.

Sanzgiri et al. [8] introduced Authenticated Routing protocol for ad hoc Networks (ARAN). ARAN was viewed as a mechanism to resolve the security issues based on cryptographic public-key certificates. ARAN is as efficient as AODV in maintaining and discovering the route but ARAN uses larger packets which results overall higher routing overhead.

Hu et al. [9] proposed Secure Efficient Ad hoc Distance Vector Routing Protocol (SEAD), which was based on hash chain sequences to authenticate hop counts between nodes. The sequence numbers also enhanced the security features in Distance Sequence Distance Vector (DSDV) protocol. SEAD outperforms than DSDV in terms packet delivery ratio but it increase more overhead in network due to increase in number of routing advertisement.

Ariadne Perrig [10] proposed a algorithm based on Dynamic Source Routing (DSR) that shared the secret key between two nodes. Although these distributed and independent developments have provided an insight into analysis of network security features, still there is a lack of a standard protocol that characterizes secure VANET and could act as a benchmark against which further protocols could be designed.

Shurman et al. [11] proposed a novel mechanism where the source node was appended with computational capabilities to verify the authenticity of the node initiating the RREP messages. The node could now detect so many possible paths to the destination and compute the safest route to the destination. The method, though novel, resulted in routing delays extending from a few nanoseconds to several orders of magnitude. He studied only one node attack to be in the route but not considered group attack.

Dokurer et al. [12] resolved group attack problem with a solution to ignore the first route, in order to counter the Black Hole Attack under the assumption that the first RREP message might be from a malicious node. Though widely agreed upon, this method ignored the possibility of the second RREP message being received from a malicious node. Thus, the method was susceptible to Black Hole Attacks, lacking a mechanism to identify and delete attacker node from the network.

Raj and Swadas [13] suggested an enhanced model to detect Black Hole Attacks, where the source continuously monitors the RREP destination sequence number and compares it with a periodically updated threshold. A value higher than the threshold is suspected to have arrived from malicious node. The neighboring nodes are informed of the presence of the malicious node through an ALARM packet. The method again increased the routing overhead. DPRAODV increases PDR with minimum increase in Average-End-to-end Delay and normalized Routing Overhead.

Kurosawa et al. [14] proposed an anomaly detection scheme using dynamic training method in which the training data is renovated at regular time intervals and analyzes Black Hole Attack in the network which is one of the main attacks in ad hoc networks. In Black Hole Attack a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node.

Mistry et al. [15] proposed an algorithm to verify the authenticity of RREP destination sequence number by heuristically analyzing the predefined waiting period. A high sequence number marked the sender as malicious node. The node suffered from latency time in case there was no attack from any node; still the monitoring proofs had to be carried out, in order to decrease the redundant threshold and hence the routing overhead.

As observed from the above discussion, most of the methods and algorithms brought some novelty to the attack detection scheme, but also suffered from routing overhead issues on intermediate and source node. Here, we propose a new algorithm with the following objectives of minimizing the routing overhead, decreasing the latency time and designing a routing protocol for efficient processing.

3. Security aspects and issues in routing protocol in VANET

Ad-hoc routing protocols usually work based on either route discovery or route maintenance. A source node without routing information needs to establish a route towards the destination. When the node changes, certain link on the activated path may break, then the route maintenance process will be initiated. Ad-hoc On-Demand Distance Vector (AODV) [5,6] routing protocol is the most widely adopted topology based routing protocol used in VANET. A source node looking for a route to the desti-

Please cite this article in press as: Tyagi P, Dembla D. Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). Egyptian Informatics J (2016), http://dx.doi.org/10.1016/j.eij.2016.11.003