View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

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.

© 2016 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

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.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

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

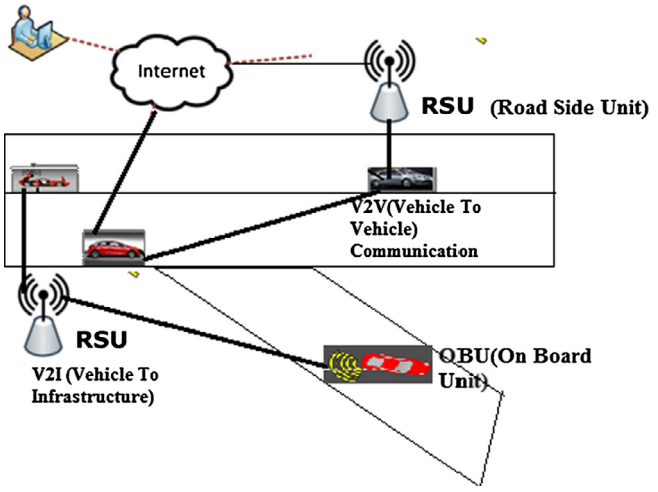

Figure 1. Vehicular ad hoc networks.

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

nation node openly broadcasts a route request (RREQ) message to the neighboring nodes and awaits route reply (RREP) message from any of the nodes which has detected a path to the destination. The AODV protocol suffers from a major drawback that the source node is unaware of which node receives the transmitted request packet and sends a reply. Because ad-hoc networks are absence of a fixed framework, there is no fixed line of infrastructure, therefore AODV is vulnerable and susceptible to the attacks.

The vehicular ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network. The attacks mainly include passive eavesdropping and leakage of secret information, Gray Hole, Black Hole, Worm Hole, and denial of service. The focus of this research paper is to detect and prevent Black Hole Attack.

In Black Hole Attack, the source node broadcasts route request (RREQ) to the nearby nodes in search for the shortest possible route to the destination. The intermediate nodes that receive the RREQ message transmit to the neighboring nodes till they find a route to the destination. Meanwhile, one of the intermediate nodes may be a malicious node and it transmits a false route reply (RREP) message to the source node. The source node transmits all the message packets to this malicious node, thus never transmitting them to the intended receiver. In the meantime, the source also rejects other RREP messages that contain a genuine path to the destination.

Black Hole Attack in VANET is diagrammatically explained in Fig. 2. Source node A broadcasts an RREQ message to discover a route for sending packets to destination node F. Node A broadcasts RREQ to its neighboring nodes B, M and C. However, malicious node M sends an RREP message immediately without even having a route to destination node F.

After receiving a false RREP, source node selects the route received from the malicious node and also ignores any forthcoming RREP messages from genuine nodes. By repeating this process, an intruder node can successfully capture other routes as well as message packets in the network by forcing most of the network traffic to flow through itself. If a malicious node intercepts the transmitted RREQ message and sends a fake RREP message, there is no inherent mechanism in AODV to detect whether the received RREQ is from a genuine node or from a malicious node.

This research focuses on Black Hole Attack, where the legitimate data packets are absorbed by a malicious node, thus causing the information to be lost. The malicious node can occur due to an intentionally node misbehaving or due to a damaged or corrupted node interface. A Black Hole Attack comes across as denial of service, with a malicious node falsely claiming to possess route information to the destination.

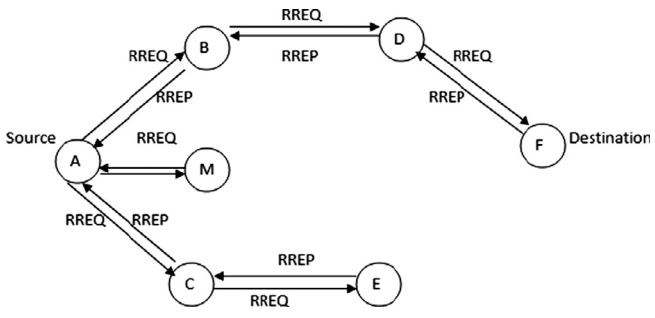

Figure 2. Black Hole Attack in VANET.

4. Proposed solution to detect and prevent Black Hole Attack

To prevent Black Hole Attack, the following mechanism is proposed and explained in Fig. 3. The source node uses additional information known as pseudo reply packet (PRREP). The source node stores the information about all the incoming packets in a look-up table designated as RREP_T. This table stores the PRREP sequences, arranged in ascending order using PUSH and POP operations. Any abnormality in the table sequences is considered to be a PRREP sequence received from a malicious node and is discarded by the source. Furthermore, the table is periodically updated, with all the PRREP sequences stores for a set duration defined by STR_dur. A header H_node attached to each message received from different nodes, assigns a priority to the PRREP message and is considered in that order by the source node. The priority is calculated based on the sequence number, and the shortest sequence number is given the highest priority. Node having abnormal sequence number is considered as a malicious node and source broadcast this message in network.

Proposed Algorithm

```
Pseudo Reply Packet (PRREP) {
t0 = get (current time value)
t1 = t0 + STR_Dur
while (CURRENT_TIME <= t1) {
Store P.Dest_Seq_No and P.NODE_ID In
RREP_Tab table
}
while (RREP_Tab is not empty) {
if (Dest_Seq_No >>>= Src_Seq_No) {
Mali_Node=Node_Id
discard entry from M_ table
}
}
select Packet q for Node_Id having
highest value of Dest_Seq_No
ReceiveReply(Packet q)
}
```

5. Experiment setup for implementation of proposed algorithm

The various network traffic scenarios are simulated in an environment without Black Hole Attack and a new algorithm is proposed to detect and prevent the Black Hole Attack in AODV and DSR routing protocol in VANET using NCTUns (*National Chiao Tung University Network Simulator*) [16,17] is used for simulation of VANET routing protocols, that serves both as an open end network simulator as well as an emulator. Embedded with GUI environment, NCTUns requires, Fedora to be operated. NCTUns provides many advantages over other network simulators.

The freeway mobility model is adopted to simulate vehicle movements on a highway. This model can simulate a bidirectional multi-lane highway that gets the highway route from an input map. The proposed algorithm is implemented and tested on NCTUns and the results are compared with AODV, DSR and B-AODV (AODV with Black Hole Attack) using various simulation parameters.

Testing scenario conditions of VANET in NCTUns:

1. A vehicular ad-hoc network is considered for study.
2. The Lane Width for vehicles is taken as 30 m.
3. The initial average distance between two nodes is supposed to be 500 m.

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

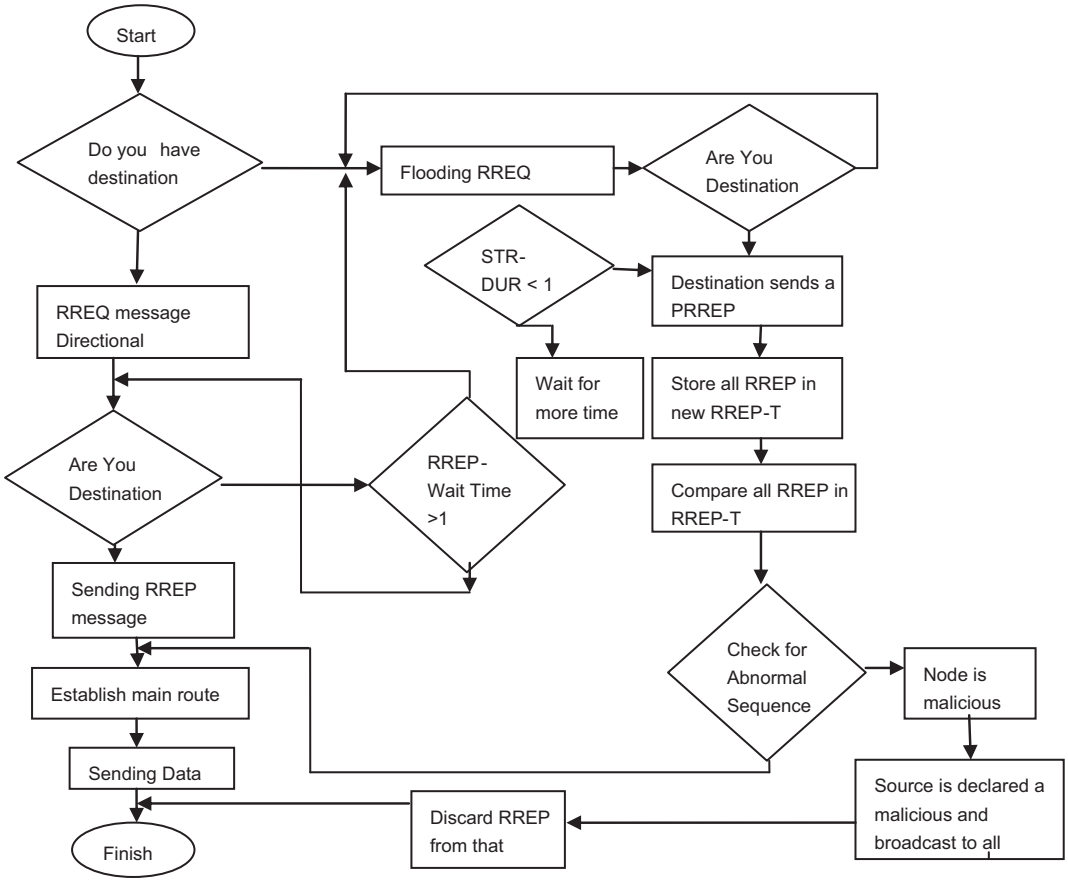

Figure 3. Flow chart of proposed algorithm.

4. Average simulation time is supposed to be 100 s.
5. The RTS threshold is set at 3000 bytes.

The simulated nodes are based on PHY/MAC networks. The vehicular network scenario is implemented using the Car Agent application. The simulation environment consists of 18 nodes on 4-lane road spread over an area of 1200 m.

The average speed 50 m/s with maximum deceleration 1–20 m per Second Square in each scenario. Table 1 shows the physical layer and channel model specification of simulation environment.

5.1. Performance metrics

Various performance measurement and analysis metrics exist that evaluate the protocol efficiency and performance in different traffic scenario in VANET environment. This work focuses on throughput, packet loss and collision rate parameters to investigate the performance of VANET routing protocols [18].

Table 1
Simulation environment parameters.

Parameter	Setting
Frequency (MHz)	24
Fading var	10
RiceanK	10
Tx antenna height (m)	1.5
System loss	1.0
Trans power (dbm)	3.0
Average building height (m)	10
Street width (m)	30
Average building distance (m)	80
Path loss exponent	2.0
Shadowing standard deviation	4.0
Close in distance (m)	1.0
Rx antenna height (m)	1.5

(a) Packet loss

Packet loss is obtained by subtracting the number of packets received at Access Point from the total number of packets transmitted.

$$\text{Packets losts} = \sum \text{Packets transmited} - \sum \text{Packets received}$$

$$\text{Packet loss ratio} = \frac{(\text{Packets losts} * 100)}{\Sigma \text{Packets transmitted}}$$

(b) Throughput

It is defined as the time average of the number of bits that can be transmitted by each node to its destination is called the per-node throughput. The sum of per-node throughput over all the nodes in a network is called the throughput of the network. The throughput is obtained by dividing the total number of packets received by the total time taken for simulation

$$\text{Throughput} = \frac{(\text{received packets} * \text{packet size})}{\text{simulation time}}$$

Throughput of the network is inversely proportional to the average delay between source and destination. Throughput of the network can also be estimated as follows:

$$\text{Throughput } (T_h) = \frac{ETT \cdot (n+1) \cdot L}{nR}$$

where R is transmission range, n is number of neighbors in the direction of destination node and ETT (Expected Transmission Time) is used to maximize the throughput of the path by measuring

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

the link capacities and would increase the overall performance of the network. ETT is defined as

$$\mathrm{ETT} = \frac{S}{L(1-p)}$$

where S is the size of a packet and L is the bandwidth of the link and p is the probability to deliver a packet successfully.

(c) Collision

A significant number of packets collide with the neighboring packets due to limited availability of communication bandwidth or congestion. This metric is defined as the ratio of the unsuccessful transmissions from the vehicle to the total number of sent packets over CCH.

$$\mathrm{CR\ (Collision\ Rate)} = \frac{\text{Unsucessfull Transmission}}{\sum \text{ Total number of sent packet}}$$

5.2. Different traffic scenarios used

The first VANET scenario depicts a highway area, and is represented using a simple single-hop scenario. Two cases under consideration for this study are the highway scenario and a city scenario. The simulation is carried out for different number of nodes (vehicles) travelling at variable speeds. These scenarios can be easily designed NCTUns-5 "draw topology" feature. The Car Agent mobility model allows nodes to follow roads just as in a real-time environment and additionally enables them to be aware of neighboring vehicles, traffic signals and varying traffic light status.

Highway scenario:

Fig. 4 illustrates the highway scenario with 10 cars with speed 90 km/h through NCTUns simulator and Table 2 describes the input parameters variation pattern and distribution pattern for highway scenario.

City scenario:

Fig. 5 illustrates the scenario with 20 cars with speed 60 km/h through NCTUns simulator and Table 3 depicts input parameters for city scenario.

5.3. Result analysis

A number of simulations were carried out in order to compared the performance of various protocols. The following results compared the performance characteristics of DSR and AODV in a simulated environment which is free of Black Hole Attacks. The practical networks contain a significant number of malicious nodes, and their effects need to be countered. The experiments were conducted without taking into consideration Black Hole Attacks and with Black Hole Attack in network. The results are exhibited in following figures.

City scenario:

The graphs in Figs. 6, 7, 9 and 10 shows the AODV and DSR protocol suffer from increased call drop rates and collision rates as the node density increases. Finally, the results in Figs. 8 and 11 emphasize that the throughput is better for proposed algorithm as the number of packet drop is higher as compared to AODV, DSR and B-AODV (AODV with Black Hole Attack). The protocols are analyzed and compared with respect to throughput, call drop and packet collision. The proposed algorithm shows somewhat better performance for all the three parameters in comparison to DSR, AODV protocol. Now we implement to enhance the security mechanism of AODV. The results are summarized in Table 4.

Table 5 gives comparative study of various algorithms, with proposed algorithm with low overhead and it is efficient for single and cooperative attacks. The solution does not add any control message to existing AODV neither it needs to even regenerate any control messages. So, there are minimum chances of rise in Normalized Routing Overhead i.e. in the ratio of number of control packets to data transmissions in a simulation.

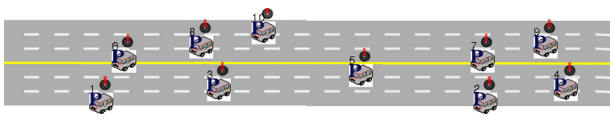

Figure 4. Highway scenario with 10 nodes with 60–90 km/h speed drawn using NCTUns -5.0.

Table 2
Input parameters for highway scenario.

Parameter	Setting
Total number of nodes	10
Max. node speed	60 km/h, 90 km/h
Packet type	UDP
Simulation time	100 s

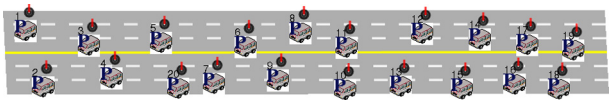

Figure 5. City scenario with 20 nodes with 20–60 km/h speed had drawn using NCTUns-5.

Table 3
Input parameters for city scenario.

Parameter	Setting
Total number of nodes	20
No. of radio obstacles	4
Attenuation provided	20 dBm
Max. node speed	20 km/h, 40 km/h
Packet type	UDP
Simulation time	100

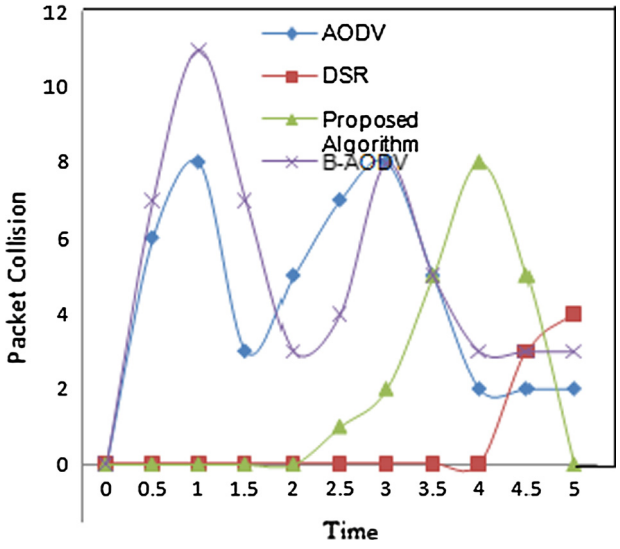

Figure 6. Packet collision rate vs. time (s) plot of highway scenario (vehicle density 10).

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

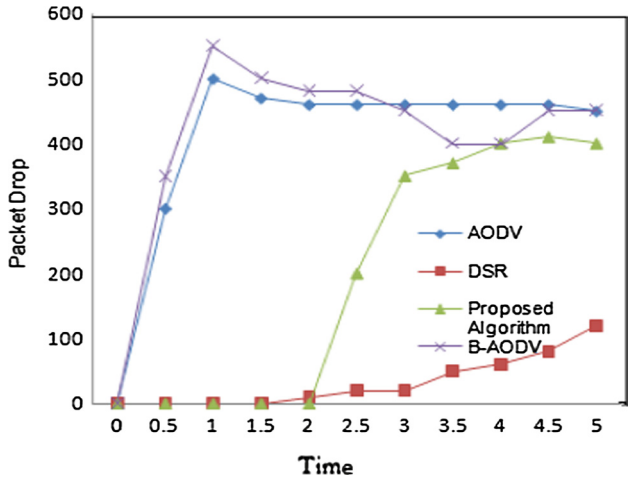

Figure 7. Packet drop vs. time (s) plot of highway scenario (vehicle density 10).

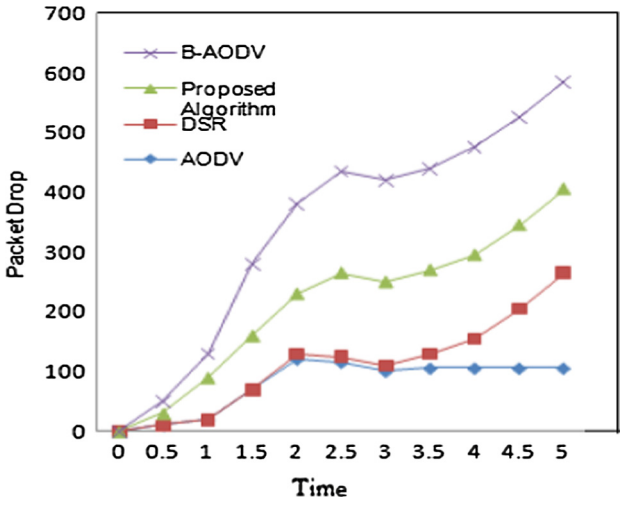

Figure 10. Packet drop vs. time in sec plot of city scenario.

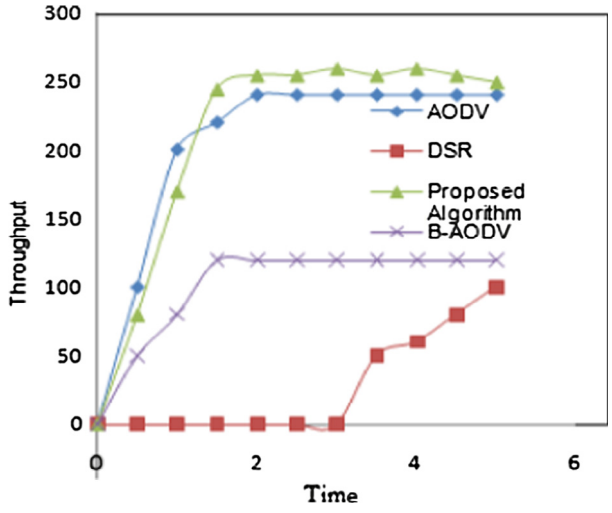

Figure 8. Throughput in kb/s vs. time in sec plot of highway scenario (car density 10).

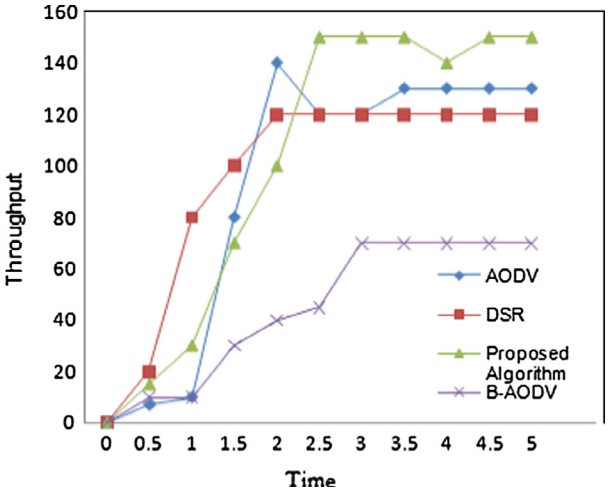

Figure 11. Throughput in kb/s vs. time in sec plot of city scenario.

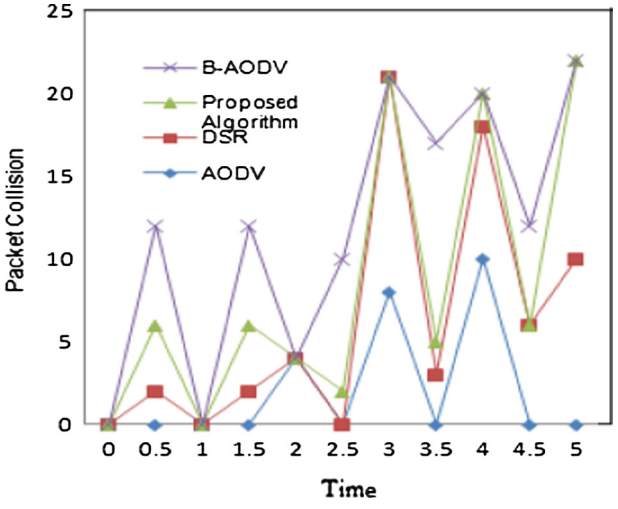

Figure 9. Packet collision rate vs. time in sec plot of city scenario.

6. Conclusion and future work

Routing protocols in VANET are more susceptible to attacks. Hence, there is a requirement for a novel supervisory algorithm. A new algorithm is proposed and implemented for VANET routing scenarios to take evasive action against the Black Hole Attack. This paper discusses the performance of DSR and AODV routing protocols for city and highway scenarios, for VANET and proposed a novel algorithm to examine 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. As VANET architectures are characterized by frequent topology changes, a precise description, control and monitoring of the timing of routing update is very important. The NCTUns simulation for these two protocols reveals that proposed algorithm is much better than AODV, DSR and B-AODV in comparison, with reference to parameters such as throughput, call drop and collision rate. Proposed algorithm adapts faster to dynamic network conditions with the help of various control messages.

The future aim would be to make the network completely immune to Black Hole Attacks using AODV routing protocol.

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

Table 4
Simulation highway and city scenario.

		Basic AODV	DSR	B-AODV	Proposed algorithm
Packet collisions	Scenario 1 (highway scenario)	8	4	11	7
	Scenario 2 (city scenario)	10	22	22	22
Packets dropped	Scenario 1 (highway scenario)	500	100	550	410
	Scenario 2 (city scenario)	100	230	550	400
Throughput (KB/s)	Scenario 1 (highway scenario)	230	100	120	255
	Scenario 2 (city scenario)	140	120	70	150

Table 5
Comparative analysis on algorithm performance.

Techniques	Overhead	Black Hole Attack	Cooperative Black Hole	Collision rate
Sanzgiri et al. [8] introduced Authenticated Routing protocol for ad hoc Networks (ARAN). It is based on cryptographic public-key certificates	High	Yes	No	High
Shurman et al. [11] proposed a novel mechanism which reduces overhead but group attack was not considered	Low	Yes	No	Low
Dokurer et al. [12] resolved group attack problem with a solution to ignore the first route reply but, this method was susceptible to Black Hole Attacks	–	Yes	Yes	High
In the proposed algorithm, overhead has been reduced and security of network for single and group attack is also been improved	Low	Yes	Yes	Low

References

[1] Chlamtac, Conti M, Liu J. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks; 2003. p. 13–64.
[2] Zeadally Sherali et al. Vehicular ad hoc networks (vanets): status, results, and challenges. Telecommun Syst 2012;50(4):217–41.
[3] Paul B et al. VANET routing protocols: pros and cons. Int J Comput Appl 2011;20(3):28–34. April.
[4] Perkin Charles E. Ad hoc on demand distance vector (AODV) routing. Internet draft, draft-ietf-manetaodv-02.txt, November 1988.
[5] Dembla Dr Deepak, Tyagi Ms Parul. A taxonomy of security attacks and issues in vehicular ad-hoc networks (VANETs). Int J Comput Appl 2014;91(7):22–7 [Published by Foundation of Computer Science, New York, USA].
[6] Hong X, Xu K, Gerla M. Scalable routing protocols for mobile ad hoc networks. Kluwer Wireless Networks 2002;16:11.
[7] Yi S, Naldurg P, Kravets R. Security-aware ad hoc routing for wireless networks. In: Proc. 2nd ACM symp. mobile Ad Hoc networking and computing (Mobihoc″01), Long Beach, CA, October. 2001. p. 299–302.
[8] Sanzgiri Kimaya, Dahill B. A secure routing protocol for Ad hoc networks. In: 10th IEEE international conference on network protocols (ICNP″ 02). 2002. p. 78–87. Nov.
[9] Hu YC, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc networks. Ad Hoc Networks J 2003;1:175–92.
[10] Yih-Chun, Perrig Adrian, Johnson David B. Ariadne: a secure on- demand routing protocol for AdHoc networks. In: MobiCom'02 proceedings of the 8th annual international conference on mobile computing and networking. 2002. p. 12–23.
[11] Shurman MA, Yoo SM, Park S. Black hole attack in mobile Ad Hoc networks. In: ACM Southeast Regional Conference. 2004. p. 96–7.
[12] Dokurer Semih, Erten YM, Acar Can Erkin. Performance analysis of ad-hoc networks under black hole attacks. In: Southeast con. proceedings. IEEE; 2007. p. 148–53.
[13] Raj Payal N, Swadas Prashant B. DPRAODV: a dynamic learning system against black hole Attack in AODV based manet. Int J Comput Sci Issues 2009;2:54–9.
[14] Kurosawa Satoshi et al. Detecting black hole attack on AODV-based mobile Ad Hoc networks by dynamic learning method. Int J Network Security 2007;5 (3):338–46. Nov.
[15] Mistry NH, Jinwala DC, Zaveri MA. MOSAODV: solution to secure AODV against black hole attack. (IJCNS) Int J Comput Network Security 2009;1(3). December.
[16] Wang Shie-Yuan, Lin Chih-Che. NCTUns 5.0: a network simulator for IEEE 802.11(p) and 1609 wireless vehicular network researches. In: Vehicular technology conference, VTC 2008-Fall. IEEE 68th. 2008. p. 1–2. Sept.
[17] Dembla Dr Deepak, Tyagi Ms Parul. Performance analysis and quality-of-service monitoring of protected and unprotected TCP networks using NCTUns simulator. In: Proc. IEEE CSNT 2015, April-4–6, 2015. Gwalior: Organized by-Machine Intelligence Research Labs, IEEE Madhya Pradesh Subsection; 2015.
[18] Elboukhari Mohamed, Azizi Abdelmalek. Impact analysis of black hole attacks on mobile Ad Hoc networks performance. Int J Grid Comput Appl (IJGCA) 2015;6(1). June.

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