International Journal of Engineering & Technology, 7 (3.16) (2018) 76-80

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Performance Analysis of ECDSA Based SE-AODV Routing Protocol In VANETS

Deepak[1], Rajkumar[2]

[1]Research Scholar, UIET, M.D. University, Rohtak, Haryana
[2]Director, MRKIET, Rewari, Haryana
**Corresponding author E-mail: deepakrohilla007@yahoo.co.in*

Abstract

Vehicular ad hoc networks is an emerging area for researchers to provide intelligent transportation system to the society. It is due to the wide area of applications of VANETs interest is developed among the people from different countries to be a part of it. Therefore many projects had been started and also presently working to implement VANETs in real world scenario. The main challenge in its implementation is to provide a secure mechanism against the various attacks and threats that have the capability to bring the network performance significantly down. In this paper to overcome different types of authentication based attacks in VANETs an ECDSA based secure routing protocol SE-AODV is proposed with security features incorporated in already existing AODV routing protocol. The performance of SE-AODV is evaluated and compared with original AODV and AODV with black hole attack (BH-AODV). The SE-AODV shows better performance with the parameters used for comparison with the variation in vehicle density, speed of vehicles and simulation time.

Keywords: *AODV;* BH-AODV; ECDSA; NS3; SE-AODV; *VANETs.*

1. Introduction

Vehicular ad hoc networks (VANETs) is a temporally network that comprises of vehicles, road side infrastructures and a central management unit[1]. These vehicles may communicate for a very small fraction of time to share important information regarding the traffic, road assistance, map sharing, weather related information and many entertainment based media files[2]. For participating in VANET a vehicle must have on board unit (OBU)[3] that operates in a dedicated short range communication (DSRC) channel[4]. Depending on the type of communication a vehicle adapts for sharing information among other participants in the network, VANET is classifies three modes of communications namely vehicle to vehicle (V2V)[5], vehicle to roadside infrastructure (V2I) and hybrid communication that is combination of both V2V and V2I[6]. The Institute of Electrical and Electronics Engineers (IEEE) standardizes the VANET communication using IEEE 802.11p [7] and IEEE 1609 standards[8]. Several routing protocols have been designed for enhancing the effectiveness of communication in VANET due to faster changing topology[9].
In this paper the various attacks in VANET are discussed with review on security related work. Further a secure routing protocol that works on the elliptic curve digital signature algorithm is proposed and its performance with existing protocols is compared.

2. Attacks In VANET

An attack is that phenomenon that restricts normal processing or working to degrade the performance of the network. Many different attack are identified in VANET that influences the routing performance of the protocols, security of data and damage to resources. Some of the VANET attacks are discussed below:

(i) Black Hole Attack: In this attack a malicious vehicle shows itself active in the network and receives messages as a next hop to further broadcast the message to other relaying vehicles or to the destination. But it keeps the packet with itself and continuously losses the transmitted packets thus degrading the network performance [10].
(ii) Worm Hole Attack: This attack a vehicle behaves normal in the beginning as the black hole vehicle. After generating trust in the network receives packets for further relaying to destination. It keeps them to itself and continuously tunnels them to some other node in spite of sending them towards the destination [11].
(iii) Grey Hole Attack: This attack is different from the above two attacks. In this attack a vehicle behaves normally as well as malicious in different intervals and it becomes difficult for the network to find this vehicle [12].
(iv) Sink Hole Attack: The malicious vehicle uses multiple IDs and hides it personal identification. It shows that it is the only vehicle near to the sender vehicle that is most relying. The sender sends the message to this ID which is fake and communicated messages starts losing [13].
(v) Message Spoofing Attack: In this attack a message received by the relaying vehicle is tempered or changed before further communicating it to the destination vehicle. Such attack incorporates wrong or false information [10].
(vi) Denial of Service Attack: If a vehicle starts in cooperating with sending unnecessary messages so as to occupy larger bandwidth assigned for communication is said to be following the denial of service attack.[14]

3. Security Requirements and Related Work In Vanets

Some of the attacks are discussed in the earlier section that degrades the network performance in one or the other way. Apart from these attacks many other aspects are present in VANET that requires security to the message integrity and authentication of participating vehicles. A large number of methods are proposed and adapted by the VANET society to make the network security enabled and attack free. There are many areas which require security features like authentication, data verification, non-repudiation, accountability and many others. Some of security related work done previously is presented in this section.

Hau Hu et.al [15] presented a trust based framework named it VTust that works with the dynamic characteristics of VANET. Also the digital signature scheme is incorporated to overcome the impact of possible attacks on the reputation system which is the basic block in the framework that builds trust related files and updates them at specific intervals. This reputation system is handled by a Trust Authority. Multisignature scheme proposed by C.Gentry [16] was used in this work.

R. Sugumar et al. [17] presented an authentication based scheme that works on cluster mechanism to counter the effects of man in the middle attack and replay attacks. The proposed scheme works with many CAs that can authenticate vehicles with the centralised update data based on the developed trust degree. The public key infrastructure is used to digitally sign before encryption at source and decryption at the destination.

Chengzhe Lai [18] proposed a secure downloading scheme based on incentives for reliable communication named it SIRC. This proposed scheme works in 3 steps; 1. Selection of proxy vehicle 2. Cooperative downloading 3. Cooperative forwarding. Attacks like injection, free riding, refusal, Denial of service, black and grey hole are considered while designing this secure scheme for VANETs.

Parul Tyagi et al. [19] designed a secure algorithm SE-AODV based on elliptic curve cryptography to cope with authentication based attacks as public key infrastructure was used along with assigning and verification of digital signatures. Performance of proposed scheme is compared with AODV and B-AODV in NCTUns and results are quite effective.

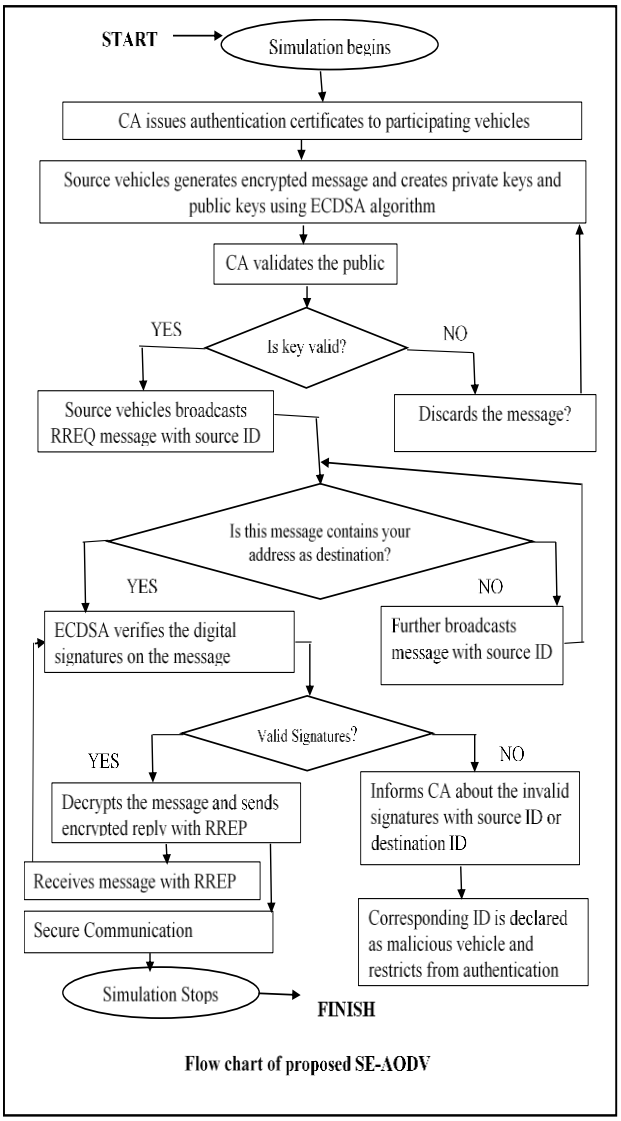
Joon-Sang et al. [20] considered one way hash chain method perfect for securing VANET by adopting and incentive based scheme with it. The performance is evaluated specifically for advertising application using PKI and CA against attacks. Also the proposed scheme is mathematically analysed. This work was funded by Korean government.

4. Problem Statement

VANETs are becoming popular among the peoples from different geographical areas because of its basic and entertainment related applications. Security to such an important network becomes primary issue to protect the information secure from different attacks. Even a small and slow attack is dangerous in this as the communicating nodes are vehicles carrying life with them [21]. So in this work we propose a solution to such attacks with a proposed algorithm that not only restricts the attacks and keeps the integrity of the messages but also enhances the performance of the network.

5. Proposed SE-AODV Routing Protocol

The proposed routing protocol is named as Secure ECDSA based AODV (SE-AODV) which uses elliptic curve technology for providing security to the vehicular ad hoc networks. This scheme uses ECDSA algorithm for generating public keys and digital signatures. Also a validation scheme for public keys is introduced to minimize the scope of any type of attack before assigning digital signatures. The verification of digital signature is also performed using the ECDSA algorithm. The flow chart and steps involved in this algorithm are as under:



Flow chart of proposed SE-AODV

Step I: Issues authentication certificate to all participating vehicles.

Step II: Generate cryptographic keys (public and private) for secure information sharing.

Step III: Authenticates the public key before broadcast of message.

Step IV: Generates digital signatures and send with encrypted message with route request.

Step V: Validates digital signatures before decryption and discards the message if found invalid.

Step VI: Declares that vehicle as malicious and restricts it at Step I.

6. Simulation Set Up

The VANET scenario is designed in NS3 using IEEE 802.11p and GPS accuracy feature. A synthetic highway model with dimensions of **250m*3000m** is considered for evaluating the performance of SE-AODV with normal AODV and black hole attack implemented AODV i.e. BH-AODV with different other parameters listed in Table 1.

Table 1. Simulation Set Up

Parameters	Value
Platform	Linux (Ubuntu 16.04 LTS)
Network Simulator	NS 3.28
IEEE standard	IEEE 802.11p
Path loss Model	Two ray ground

Mobility Model	Random Way Point
Transmission Power	10dBm
Transmission maximum delay	10 ms
Date rate	2048bps
GPS accuracy	40ns
Routing Protocols	SE-AODV (proposed)
No. of Vehicles	20, 40, 60, 80, 100, 120
Speed of Vehicles (m/s)	14, 17, 20, 23, 26
Simulation Time (seconds)	20, 40, 60, 80, 100, 120
Simulation Area	250m*3000m

7. Results and Discussions

The performance evaluation and comparison of SE-AODV with AODV and AODV has been done on the basis of variation in vehicle density, speed of vehicles and simulation time. For the analysis on the basis of variation in number of vehicles the speed of vehicles is kept 20 m/s and simulation time of 20 seconds is taken. The number of vehicles are limited to 60 and speed of vehicle to 20 m/s for the comparison on the basis of variation in speed of vehicles. The number of vehicles are restricted to 60 and simulation time offered is 40 seconds for the comparison on the basis of speed of vehicles. Goodput, E2E delay, Packet delivery ratio (PDR) and Packet loss ratio (PLR) are the parameters on the basis of which performance evaluation and comparison is done.

7.1 Comparison of Average Goodput

The average goodput for SE-AODV, AODV and BH-AODV is calculated and compared on the variation of number of vehicles (Fig.1), speed of vehicles (Fig.2), and simulation time (Fig.3). As shown in Fig. 1 the obtained average goodput is higher than the compared protocols except for the case of 80 vehicles. Where the performance of BH-AODV is effected with the black hole attack and is far below from the latter two protocols. SE-AODV shows significant rise as the vehicle density increases.

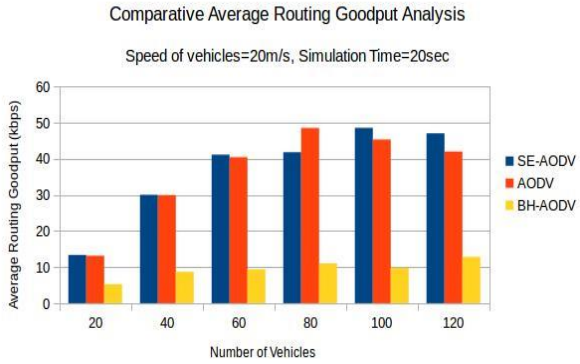


Fig.1 Comparison of average goodput with variation in number of vehicles

The variation in speed of vehicles for average goodput is shown in Fig.2 which showa that maximum goodput is achieved with a speed of 23 m/s for SE-AODV while it is 14m/s speed that provides highesh goodput for AODV. The designed protocol provides better results with the increase in speed of vehicles. It is very less with BH-AODV and decreases with the increase in speed of vehicles.

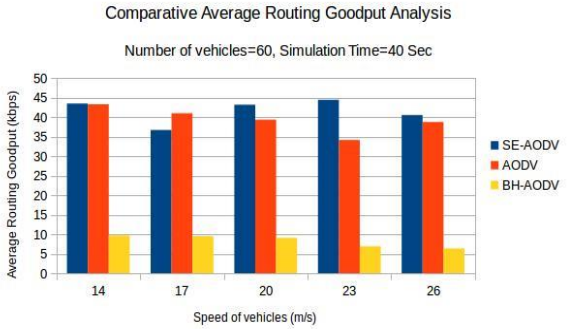


Fig.2 Comparison of average goodput with variation in speed of vehicles

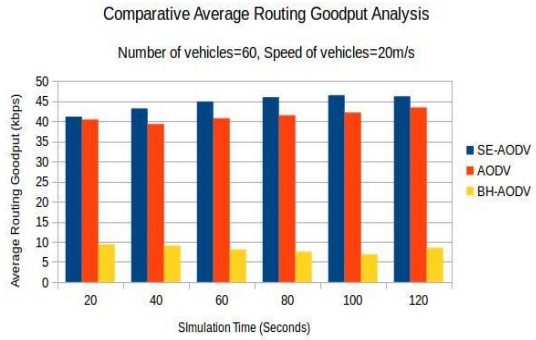


Fig.3 Comparison of average goodput with variation in simulation time

Fig. 3 shows the average goodput with variation in simulation time. The number of vehicles are 60 and simulation time is 40 seconds, if we decrease the simulation time the goodput decreases and increases with the increase in simulation time. It is also important to note that SE-AODV performs better with all the simulation time than AODV. While goodput continues to degrade with the simulation time as the black hole vehicle is getting more time for losing more packets.

7.2 Comparison Of Average End To End Delay

The average end to end delay is shown in Fig 4 for variation in number of vehicles.

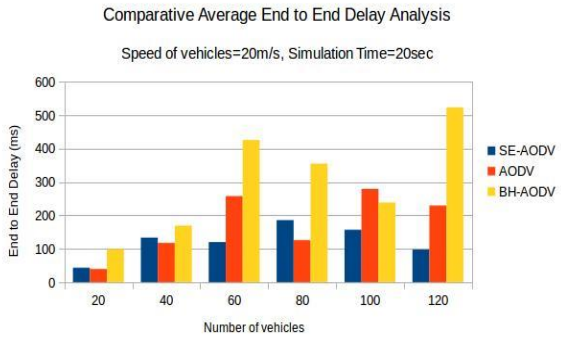


Fig.4 Comparison of average end to end delay with variation in number of vehicles

SE-AODV provides lesser delay to AODV with high density of vehicles ranging from 100 to 120 in this simulation scenario. The BH-AODV has the highest delay among all protocols in low, medium and high density. As the number of vehicles are increasing it becomes difficult to identify the black hole vehicle.But if we consider the vehicle density and simulation time consistent and varies the vehicle speed from low to high. As seen from Fig 5 the SE-AODV provides least delay in all speed ranges while the delay of AODV is higher than SE-AODV and lower than BH-AODV in all speed variation simulations. Similar results has been observed when the simulation time is varied to compare the delay among

the three protocols. But for 120 seconds the BH-AODV is providing delay above 800ms while for the same simulation time the AODV is providing delay near to 500 ms and SE-AODV shows 300ms delay which is very less and good for a secure routing protocol. Fig. 6 is showing the comparative results of end to end delay with variation in simulation time.

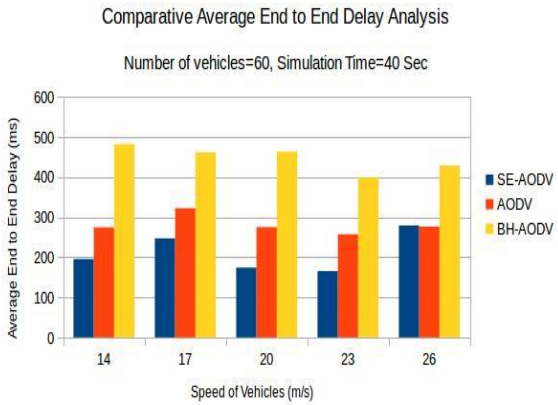


Fig.5 Comparison of average end to end delay with variation in speed of vehicles

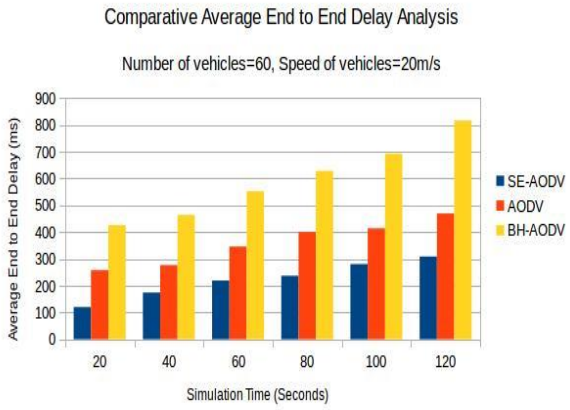


Fig.6 Comparison Of Average End To End Delay With Variation In Simulation Time

7.3 Comparison of Packet Delivery Ratio

The Packet delivery ratio (PDR) for SE-AODV, AODV and BH-AODV is compared with the variation number of vehicles shown in Fig.7, variation in speed of vehicles shown in Fig.8 and variation in simulation time shown in Fig.9.

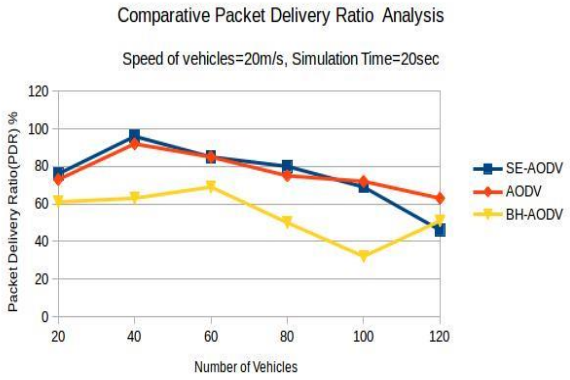


Fig.7 Comparison of PDR with variation in number of vehicles

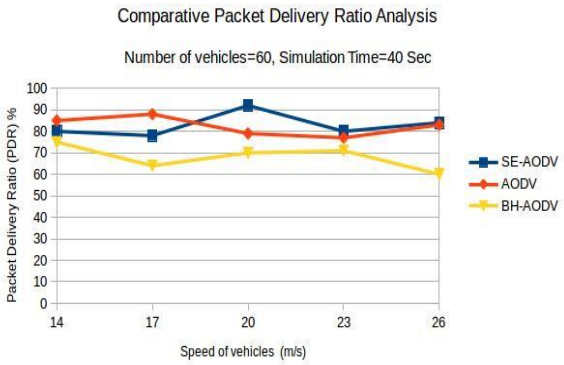


Fig.8 Comparison of PDR with variation in speed of vehicles

From Fig. 7 the simulation results shows that the PDR decreases with the increase in number of vehicles, but is should increase as the participant increases. This decrease is due to limited simulation time 20 second that is not enough for the large number of vehicles to participate fully. Although the SE-AODV show higher PDR upto 80 vehicles but then it falls for 100 and 120 vehicles. The BH-AODV has the least PDR in every range of vehicles. The performance of SE-AODV with slow speed as 14 m/s and 17 m/s is slightly less than AODV while for faster speed 20 m/s, 23 m/s and 26 m/s it is the highest among the three protocols. The secure SE-AODV provides the highest PDR with a vehicle speed of 20 m/s as shown in Fig. 8. The secure algorithm proves to best when the simulation time is varied for 60 vehicles case with a speed of 20 m/s as shown in Fig. 9. BH-AODV has the least PDR in all three variations.

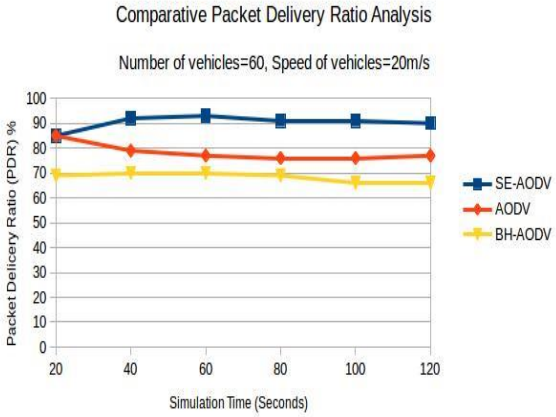


Fig.9 Comparison of PDR with variation in simulation time

7.4 Comparison of Packet Loss Ratio

The comparison of packet loss ratio for the secure SE-AODV with AODV and BH-AODV is presented in Fig. 10 with variation in number of vehicle, Fig. 11 with variation in speed of vehicles and Fig. 12 with variation in simulation time.

The results from Fig. 10 shows that the PDR is least for SE-AODV in all types of vehicle density and maximum for BH-AODV in all vehicle densities as compared to rest two protocols. The black hole attack keeps the packets with itself and does not forward further towards destination thus resulting in a packet loss.

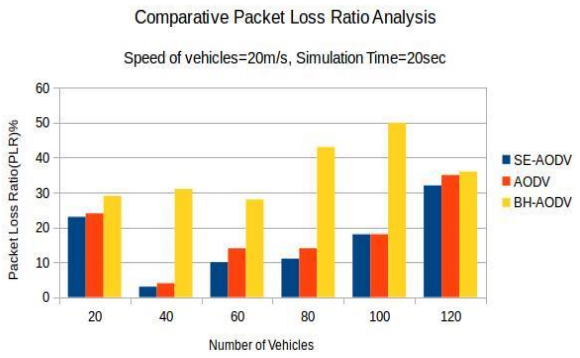


Fig.10 Comparison of PLR with variation in number of vehicles

The PLR comparison is shown in Fig. 11 with the variation in speed of vehicles. The results shows the best performance of SE-AODV at a speed of 20 m/s. However as compare to all three protocols the SE-AODV provides least PDR on or above the vehicle speed 20 m/s. The PLR for BH-AODV is highest in all vehicle speeds.

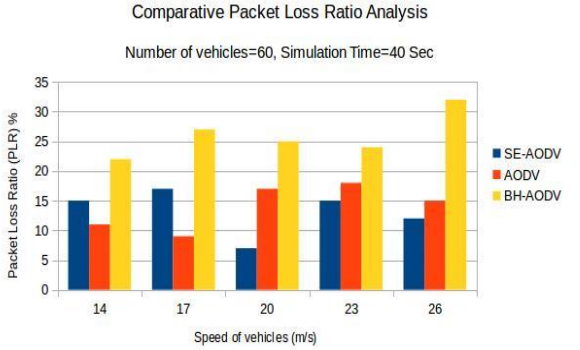


Fig.11 Comparison of PLR with variation in speed of vehicles

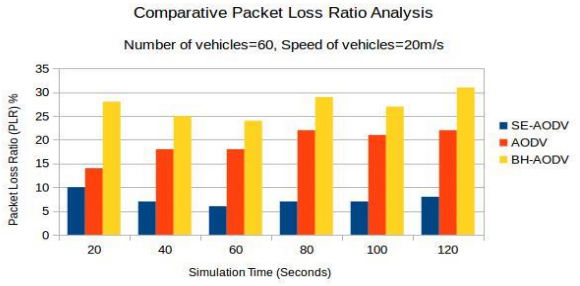


Fig.12 Comparison of PLR with variation in simulation time

The simulation time variation for PLR is shown in Fig. 12 which shows the results of proposed SE-AODV are consistent and less than AODV and BH-AODV. With the increase in simulation time the PLR increases for AODV and BH-AODV.

8. Conclusion

The secure elliptic curve digital signature algorithm based AODV (SE-AODV) is designed to cope with different threats and attacks of VANETs. It is secure and resistant for many authentication based attacks. It is based on PKI and digital signatures to ensure high security to the data and routing packets. The performance SE-AODV is analyzed and compared to AODV and BH-AODV in a vehicular scenario. The comparative results proves that SE-AODV is better than AODV and BH-AODV with providing higher goodput, higher PDR, lower PLR and least delay with all three analysis done with the variation in vehicle density, variation in speed of vehicles and variation in simulation time.

9. Future Scope

In this work we focused the comparison of proposed SE-AODV with AODV and BH-AODV only while in future these results can be compared with other existing VANET routing protocols. Also the simulation can be extended to a realistic scenario using real geographical map extracted from different available tools.

References

[1] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan, (2012), "Vehicular Ad Hoc Networks (VANETS): Status, Results, and challenges", Telecommunication Systems, Vol.50, no. 4, pp. 217,241.

[2] Connected vehicles: The future of transportation; official website: https://www.its.dot.gov/ (last visit: 11.03.2018).

[3] Xiaomin Ma; Jinsong Zhang; Xiaoyan Yin; Trivedi, K.S, (2012), "Design and Analysis of a Robust Broadcast Scheme for VANET Safety-Related Services", IEEE Transactions on Vehicular Technology. vol.61, no.1, pp.46, 61.

[4] Sumra, I.A.; Ahmad, I.; Hasbullah, H.; bin Ab Manan, J.-L. (2011) "Classes of attacks in VANET", Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International , vol. no. pp.1,5, 24-26.

[5] Nzouonta, J.; Rajgure, N.; Guiling Wang; Borcea, C (2009), "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information", IEEE Transactions on Vehicular Technology. vol.58, no.7, pp.3609, 3626.

[6] W. Liang, Z. Li, H. Zhang, Y. Sun, and R. Bie (2014), "Vehicular ad hoc networks: Architectures, research issues, challenges and trends". https://link.springer.com/chapter/10.1007/978-3-319-07782-6_10 (last visit: 11.03.2018).

[7] Awerbuch, Baruch, and Amitabh Mishra. "Introduction to Ad Hoc Networks." http://www.cs.jhu.edu/~cs647/intro_adhoc. (last visit 12.04.2018)

[8] Shie-Yuan Wang, Chih-Che Lin, Wei-Jyun Hong and Kuang-Che Liu (2011), "On the performances of forwarding multihop unicast traffic in WBSS-based 802.11(p)/1609 networks", Computer Networks. Volume 55, Issue 11, Pages 2592-2607.

[9] Gadkari, Mushtak Y., and Nitin B. Sambre, (2012), "VANET: Routing Protocols, Security Issues and Simulation Tools", IOSR Journal of Computer Engineering, vol.3, no.3, pp. 28, 38.

[10] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan, (2012), "Vehicular Ad Hoc Networks (VANETS): Status, Results, and challenges. Telecommunication Systems", Vol.50, no. 4, pp. 217-241.

[11] Fatih Sakiz and Sevil Sen (2017), "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV", Ad Hoc Networks.Vol. 61, pp. 33-50

[12] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil and Anis Laouiti (2017), "VANET security, challenges and solutions: A survey", Vehicular Communications,Vol. 7 pp. 7-20

[13] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, Alejandro Quintero(2014), "VANET security surveys. Computer Communications" vol. 44, pp. 1-13.

[14] Bassem Mokhtar and Mohamed Azab (2015), "Survey on security issues in Vehicular Ad hoc Networks", Alexandria Engineering Journal. https://doi.org/10.1016/j.aej.2015.07.011 pp 1115-1126.

[15] Hau Hu, Rongxing Lu and Zonghua Zhang (2016), "VTrust: A robust trust framework for relay selection in hybrid vehicular communications",IEEE Global Communications Conference (GLOBECOM). DOI 10.1109/GLOCOM.2015.7417027

[16] C. Gentry and Z. Ramzan (2006), "Identity-based aggregate signatures", Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA,April24-26, 2006, Proceedings, pp. 257–273,

[17] R. Sugumar, A.Rengarajan and C.Jayakumar (2016), "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)", Wireless Netw.DOI 10.1007/s11276-016-1336-6

[18] Chengzhe Lai, Kuan Zhang, Nan Cheng, Hui Li and Xuemin Shen (2016), "SIRC: A Secure Incentive Scheme for Reliable Cooperative Downloading in Highway VANETs", IEEE transactions on intelligent transportation systems. pp 1-16

[19] Parul Tyagi, Deepak Dembla (2018), "Advanced secured outing Algorithm of Vehicular ad hoc Network", Wireless Pers Commun. Springer. https://doi.org/10.1007/s11277-018-5824-0

[20] Joon-Sang Park and Seung Jun Beak (2012), "Securing one-way hash chain based incentive mechanism for vehicular ad hoc networks", Peer-to-Peer Netw. Appl.. DOI 10.1007/s12083-012-0178-y

[21] Suguo Du, Xiaolong Li, Junbo Du, Haojin Zhu (2012), "An attack-and-defence game for security assessment in vehicular ad hoc networks", Peer-to-Peer Netw. Appl. DOI 10.1007/s12083-012-0127-9