THINK INDIA JOURNAL

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

Performance analysis of Session Initiation Protocol in VANET

Sandeep Kumar Arora*, Akhil Gupta, Shakti Raj Chopra, Gurjot Singh Gaba

Lovely Professional University

Jalandhar, India

*Corresponding author: sandeep.16930@lpu.co.in

Abstract: Security is major concern in vehicular networks and we know that its important to secure the data exchange between vehicles but it is difficult assignment to plan efficient protocol to secure the session between the vehicles. Many protocols have been proposed for securing session. We also proposed session initiation protocol based on authentication to address the security issue. The proposed scheme is safe from the different attacks. Various performance analysis has been shown based on NS-2 simulations which shows the effectiveness of the proposed scheme.

Keywords: adhoc, session, attack, security

I. Introduction

Wireless Networks are the network the various two nodes or any conversation devices that makes use of the radio waves to talk. As the growth in era, the usage of transportable and small community devices is growing every day. The requirement of wireless community has additionally extended. In early instances, stressed network become taken into consideration greater secure and speedy, however with the evolution of technology wi-fi community became more famous. Wireless networks due to their ease of access and infrastructural flexibility; they are used in small and massive industries.

Vehicular Ad hoc Networks (VANET) have been added to gain more secure using environment via smart automobiles and smart roads. VANET incorporates critical types of elements: Road Side Units (RSUs), and On-Board Units (OBUs). RSUs are normally established at a road-facet area to aid the statistics exchange with vehicles, even as OBUs are hooked up in automobiles to enable the periodic exchange of protection statistics for some secure and comfortable driving surroundings as shown in Fig.1. Adhoc wi-fi systems are depicted in light of the fact that the classification of Wi-fi systems that use multi-bounce radio transferring and can running without the guide of any consistent framework and nodes impart on the double among each other over Wi-fi channels. As the wireless channels are brazenly to be had and propagate through the air, security in adhoc networks is of number one challenge [1].

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

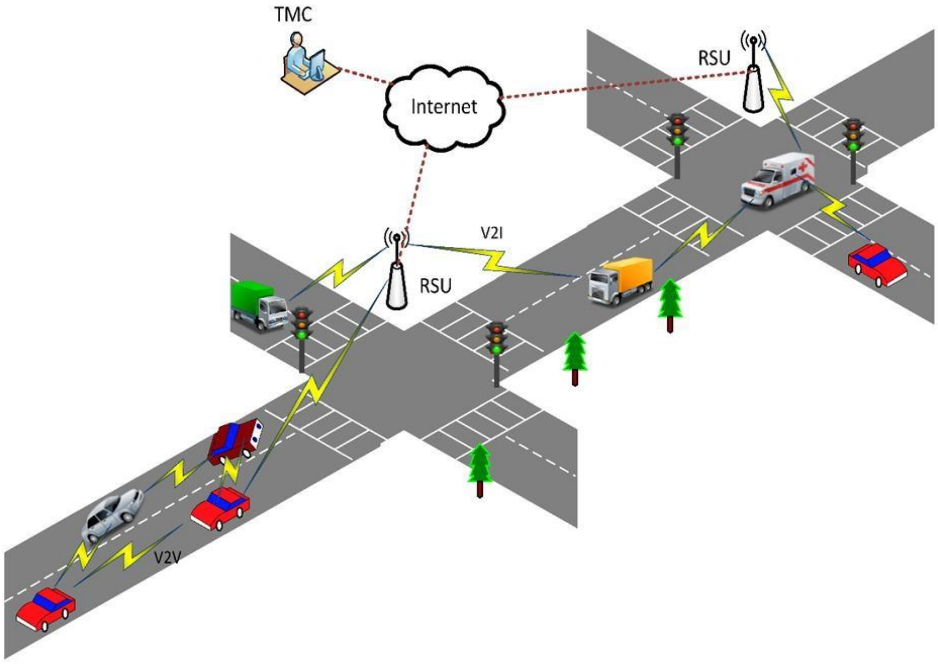

Fig.1 Architecture of VANET

II. Related work

For session initiation protocols Tsai's authentication scheme is at danger for user anonymity and verifier attack. Keeping in mind they have offered ECC using discrete logarithmic problem. The projected authentication system not handiest opposes these attacks but rather additionally manages more security and execution [2].

The recommended authentication scheme using Elliptic Curve derived from Diffie Hellman Key Exchange compromises the same robust structure against offline password guessing and server spoofing attacks. In addition, it is more capable and best in the submissions/gadgets requires low memory and quick interactions [3].

Another validation scheme for SIP, which defeats the intrinsic shortcomings of Otherwise known as plan, accomplishes the authentication and a common mystery in the meantime and gives provable security in CK security show [4].

Various parameters are defined such as quality of service, routing, broadcasting, securities. This paper also describes about the advantages, disadvantages and limitation of these parameters. There is also need of some modification regarding the reliable and secure VANET [5].

III. Security and routing protocols in VANET

The routing protocol proposed for indicate point communications in VANET can be characterized into topology-based and position-based protocols. For the outline of vehicular system, routing protocol is the primary test because of increment in nature of element

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

topology [6]. As Routing is the best way to transmit information from one vehicle to others. To give the safety or safe place to the individual, trading of messages ought to be finished with between vehicle communication. Routing in VANET is more testing than the MANET in light of exceedingly changes in element topology attributes [7,8]. So, finding and keeping up the best ways of communication in attractive condition is the most troublesome undertaking in VANET.

Topology based and position-based routing protocol are predominantly utilized by the VANET framework. As in topology-based Routing protocol, for sending information from source to goal it uses connection's data inside the system. It can be characterized by two approach: proactive and responsive Routing protocol. Proactive is table driven protocol which utilizes most limited way algorithm to exchange information. The tables are additionally imparted to the neighbours to locate the ideal way amongst source and the goal on the grounds that if any refresh required, then every node can refresh their routing table. Responsive routing protocol is approached request protocol since it keeps up route disclosure prepare inside the system. The routing protocol are named appeared in figure 2.

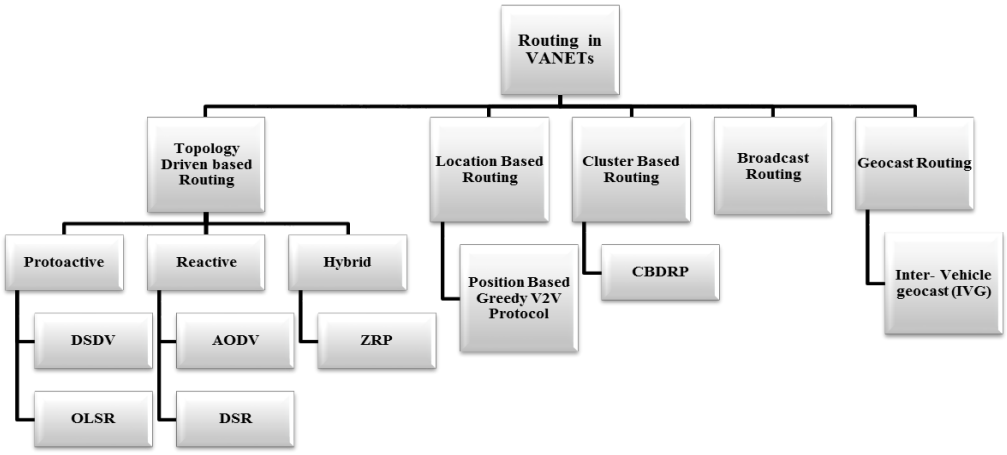

Fig 2 Routing protocols in VANET

ECC is a new cryptography technique, and considered as an excellent method because of the small size of key for the user. It is difficult to break. An attacker needs more time to exploit the key. ECC, with the size of 160-bit key provides better security than the protocol cryptography RSA with a size of 1024-bit. ECC provides the more security to the message. The key size is small, which gives the fast-cryptographic procedures, running on more compact software's. For the ECC, the hardware implementation is also compact due to a small key

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

size. It is a sufficient cryptography system for wireless networks. Because it provides the bandwidth saving. ECC was introduced by V. Miller [9] and Neal Koblitz. ECC is a more secure algorithm; it cannot be easily breached by the intruder.

In the ECC, there is public key as well as a private key. Private Key is the hidden key of the algorithm. In the concept of symmetric key cryptography, single key is used only for encryption and decryption. In asymmetric key cryptography, public key is used for message encryption. Public Key is distributed publicly and known to everyone. ECC has used asymmetric key cryptography scheme for encryption and decryption [2].

The ECC is used in huge application. ECC can give better security with small key size than other algorithms. By using the ECC, speed can be enhanced. This can enhance the bandwidth, and storage that are the fundamental limitations of resource-constrained devices. The Elliptic curve Discrete Logarithm Problem (ECDLP) (Hankerson et al., 2004) is the impossible computational problem for Elliptic curve [2].In Figure 3, Elliptic curve whose point at infinity far to the top and bottom of graph.

$$Y^2=x^3+ax+b \qquad (1)$$

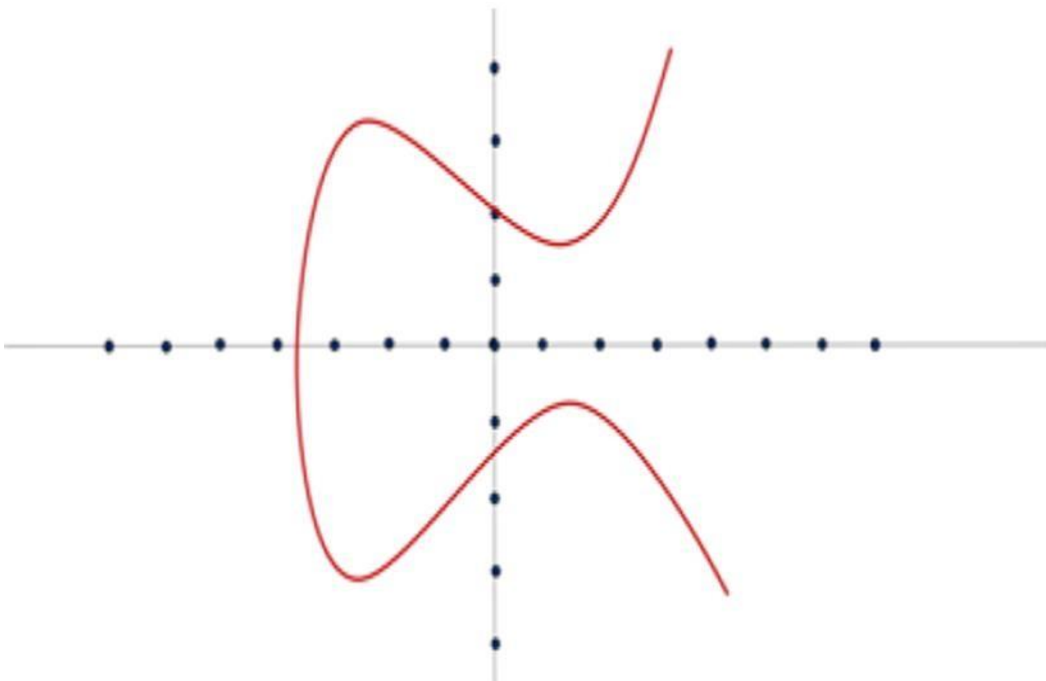

Fig 3 Elliptic curve

IV. Simulation setup and performance metrics

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

We have simulated the different session initiation protocols scenario in high traffic as given. These are the following simulation parameters that we have represented in Table 1.

Table 1

Simulation Parameters	**Values**
Number of nodes	50
Propagation model	Two ray ground
Antenna type	Omni directional
Routing protocol	AODV
MAC	802.11
Packet size	200
Simulation area	500*500

A) Packet Delivery Ratio: As shown is Fig. 4, with the increase in number of nodes the PDR is reducing. This is due to increased number of connections in the network leading to more congestion which furthermore leads to packet drops. But since the number of packets transmitted are also high due to augmented number of connections so the value for the throughput increased with number of nodes. While on the other hand, the delay is found to exhibit almost similar values in the high traffic scenarios. The below graph shows the performance of proposed scheme against number of nodes.

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

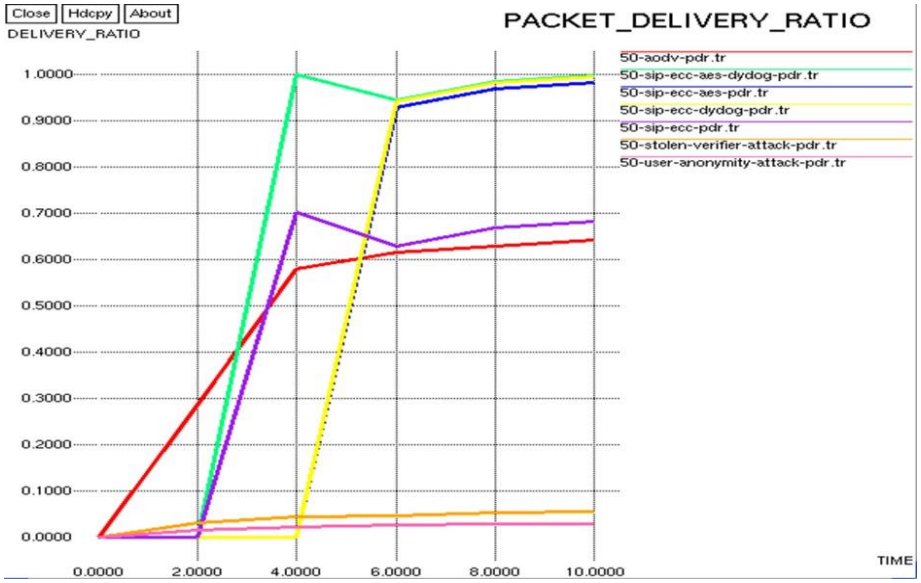

Fig. 4. Comparison of PDR (50-Nodes)

B) Average Delay:

When there is an attack the delay is increasing. After the application of the ecc-aes-dydog mechanism along with the encryption techniques the value of delay is found to be best of all the other modules tested as shown in Fig. 5.

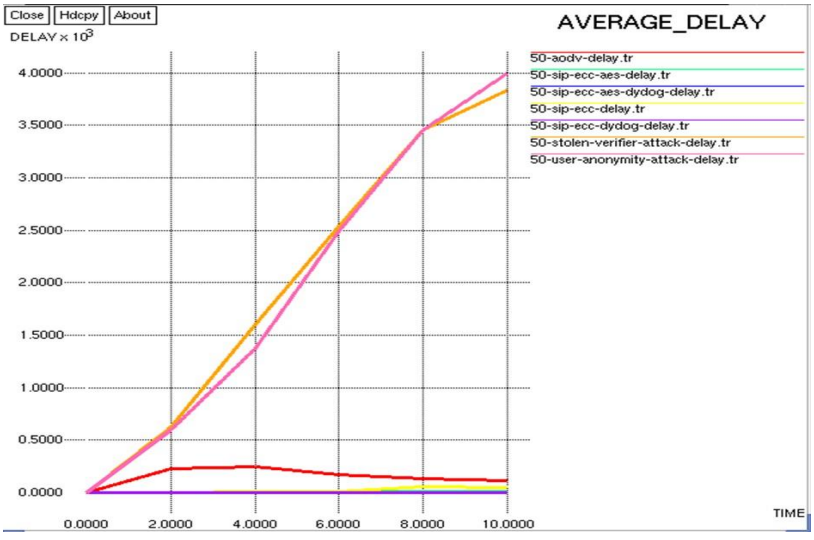

Fig.5 Comparison of average delay (50-Nodes)

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

C) Average throughput: In case of high traffic**,** throughput is decreasing with increase in number of nodes. But when SIP is applied then throughput will increase as shown in Fig.6.

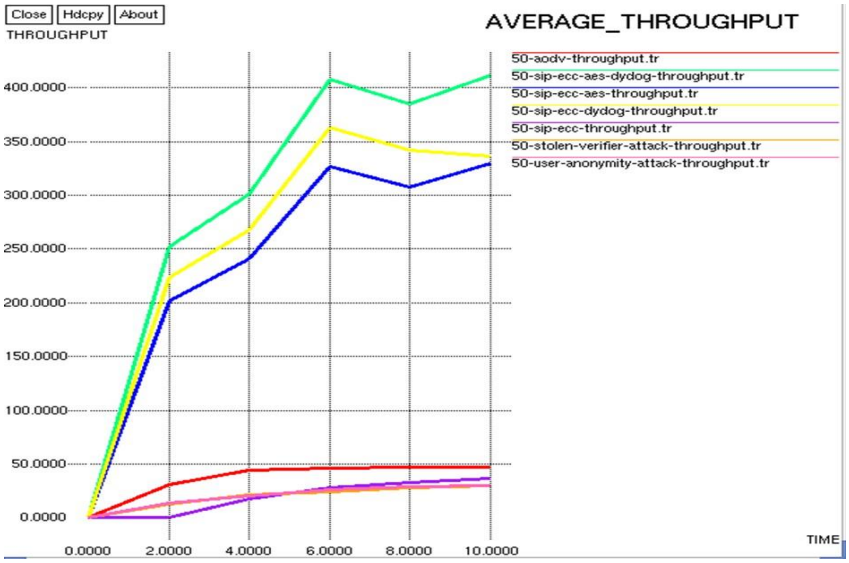

Fig.6 Comparison of average throughput(50-Nodes)

V. Conclusion

In this paper, we have checked the performance metrics for different encryption techniques using ECC protocols under session initiation routing and found that using ECC SIP the performance of the system improved in VANET and furthermore it improves the security of the system also.

References

[1] V. Kumar, N. Chand, "Efficient Data Scheduling in VANETs," Journal of Computing, vol.2, no.8, pp. 32-37,2010.

[2] A.Rashid, I. Nam, "Elliptic curve cryptography based mutual authentication scheme for session initiation protocol," Multimedia Tools Applications, vol.66,no.2, pp.165–178,2013.

[3] A. Durlanik, I. Sogukpinar, "SIP authentication scheme using ECDH," World Informatika Society Transactions on Engineering Computing and Technology, Vol. 8, pp.350–353, 2005.

[4] L. Wu, Y. Zhang and F. Wang, "A new provably secure authentication and key agreement protocol for SIP using ECC," Computer Stand Interfaces, vol. 31, no. 2, pp.286–291, 2009.

[5] S. Zeadally, R.Hunt, Y.Chen, "Vehicular ad hoc networks: status, results, and challenges," Springer Science & Business Media, vol. 9, no. 2, pp.4-10, 2010.

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

[6] A. Dhamgaye, N. Chavhan, "Survey on security challenges in VANET," International Journal of Computer Science vol.2, no.2, pp.34-40, 2013.

[7]. J. Kakarla, S. Siva Sathya, B.G. Laxmi, B. Ramesh Babu, "A survey on routing protocols and its issues in VANET", International Journal of Computer Application, vol. 28, no.4, pp.234-242, 2011.

[8]. Z. Wang, L. Liu, M. Zhou, N. Ansari, "A position-based clustering technique for ad hoc intervehicle communication," IEEE Transaction System Man Cybern, vol.38, no.2, pp. 34-40, 2008.