WWJMRD 2017; 3(8): 328-332
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Saruchi Panwar
M. Tech (Student)
Department of Computer Science and Engineering
GZS Campus College of Engineering & Technology, Bathinda India

Dinesh Kumar
Department of Computer Science and Engineering
GZS Campus College of Engineering & Technology, Bathinda, India

Correspondence:
Saruchi Panwar
M. Tech (Student)
Department of Computer Science and Engineering
GZS Campus College of Engineering & Technology, Bathinda India

Encryption Based Security for Position Based VANET Routing Protocol

Saruchi Panwar, Dinesh Kumar

Abstract

Security is a key concern for communication among vehicle to vehicle and vehicle to infrastructure in Vehicular Ad hoc Network(VANET), achievement of security is the purpose of this paper and comparison among parameters are also discussed for position based VANET routing protocol network. VANET is receiving a lot of attention from academicians, research & development (R&D) and industrial community as it plays a vital role in traffic safety besides ensuring a pleasant driving experience. Talking about expressways various vehicles moves with their maximum speeds and required to get information if any danger is ahead like accidents or construction are there, taking this advantage any disrupted unit can send false information about any situation. To prevent the network from this type of bogus. Symmetric key is used to cope with security challenges while communicating.

Keywords: Ad-hoc, Encryption, Symmetric key, VANET

Introduction

VANET

VANET (Vehicular Ad Hoc Network) enables vehicles which act as a node in network to communicate with other vehicles and with road- side infrastructure. VANET is a technology that enables nodes to create mobile network. It turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes [1].

VANET is extension of MANET (Mobile Ad Hoc Network). MANET can change locations and configure itself on the fly, Because MANETS are mobile, and they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. [2]. VANET is highly dynamic in nature as nodes changes their position very frequently whereas MANET don't change their positions frequently. Protocols used in MANET are not effectively used in VANET which allow us to implement new protocols which works well in VANET.

Difference between VANET and MANET

MANET and VANET both are mobile in nature but with little difference as in MANET topologies are changing with less frequency whereas in VANET topologies are changing with high frequency. In MANET, nodes move independently without any direction specified, but VANET is supported to fixed infrastructure as nodes movement is restricted i.e. RSU provide some service and access to stationary networks. Geographic communication environment is not relevant to MANET, whereas in VANET, according to the density of nodes environments are distinguished between two types that are urban and rural that shows relevancy to geographic communication environment. VANET is very much protected from geographical attacks and have a better physical protection unlike MANET.

VANET and Services

VANET provides a wide range of services to users such as information on vehicle safety and planning a trip by using communication devices. Furthermore, in order to safe guard the drivers and regulate the stream of vehicles, the drivers have to be alerted about the road conditions, traffic congestion and other related aspects. The accurate information and time is very vital to achieve this aim. The VANET will be able to address this issue.

1. Major intended uses for VANET regards safety. If a car spots dangerous road situation, such as black ice, it transmits information to car behind it that might be heading in the direction of danger.[3]
   This issue are needed to be addressed while choosing protocol that will be used.
2. Long distance between source and destination creates relay nodes (RN) that uses network bandwidth which causes loss in energy, it can cause huge amount of load on relay nodes which end up with congestion in network.
3. Packet delivery rate can be deceased in dense environment
4. End- to-end delay is another issue in VANET when distance between source and destination is maximum to which it cause delay in packet delivery.
5. Creating a secure communication among nodes is essential criteria which makes a safe transfer of data in V2V(vehicle to vehicle)communication and V2I(vehicle to infrastructure)communication

VANET and Security

Safety in VANETs is of special concern because human lives are constantly at stake whereas in traditional networks the major security concerns include confidentiality, integrity and availability none of which involves primarily with life safety. Nonetheless, security in VANET also indicates the ability to determine the driver's responsibility while maintaining driver's privacy. Information about the vehicles and their drivers must be exchanged securely and more importantly timely. Delay in message exchange may cause catastrophic consequences such as collision of vehicles.

The deployment of a comprehensive security system for VANET is very challenging in practice. A security breach of VANET is often critical and hazardous. Moreover, the nature of vehicular network is highly dynamic with frequent and instantaneous arrivals and departures of vehicles as well as short connection durations. In addition to its dynamic nature and high mobility, the use of wireless media also makes VANET vulnerable to attacks that exploit the open and broadcast nature of wireless communication.

Besides general networks security issues, unique security challenges rises because of the unique characteristics of VANET such as high mobility, dynamic topology, short connection duration and frequent disconnections. These unique features bring security issues such as trust group formation, position detection and protection as well as certificate management [4].

Looking at these security issues VANET allow us to establish an encrypted network using algorithms.

Encryption

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. Symmetric key is used for encryption and decryption. Security parameters are as follows:

- **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation*:*** A mechanism to prove that the sender really sent this message. So, that a sender cannot deny

.

Literature Survey

B. T. Sharef et al (2016): In concern with safety of drivers and secure communication among vehicles VANET has emerged with numerous of routing protocols in accordance with change in topologies.This work done concentrates on features and advancements of the VANET position-based routing protocols. Position-based routing protocol are most forceful in highly dynamic environments like VANETs whereas the geographic location of neighboring nodes in the main factor in determining the optimal route as the packets are forwarded. In this kind of routing protocols neither link state exchanges nor route setup is required unlike other routing protocols. These protocols still lacks in end –to-end delay and low packet delivery rate which can be enhanced for future work other than this security is another issue that needed to be solved [1].

P. Salvo et al(2015): In networking, packets among highway vehicles are not efficiently delivered for this implementation of effective algorithm is required. In this paper usage of timer with probalistic decimation logic makes the throughput rate and packet delivery ratio of system better [2].

P. tyagi, D. Dembla et *al (2015):* dynamic nature of network brings this paper which attempts to examine and investigate the security features of routing protocols in VANET.AODV protocols are applied to detect and handle attacks mainly black hole attacks. Stack operations are used in table for route replies which are calculated on the base of sequence number. Protocols like AODV, DSR,B-AODV are compared for their efficiency with respect to throughput, call drops and collision rate. Black hole attacks can be cured completely using AODV for further enhancements [3].

F. Cunha et al (2014): increasingly vehicles are being equipped with embedded sensors,processing and wireless communication capabilities. With dynamic scenario this work focuses on vehicular networks, architectural details, constraints of layers, protocols and applications. Geographical addressing, security and privacy can be more focused for future work [4].

R. S. Raw, M. Kumar et. al (2014): technical and security issues of VANET are centre of attraction that are required to be covered up with security measures. Here different technologies are used for different attacks in order to solve them. Authentication and privacy is majorly required in VANET [5].

N. k. Chaubey et al(2014): VANET has been an interested topic among researchers.security is always been an important and major challenge in VANET.in this paper, analysis of VANETs applications, challenges,requirements, attacks,security issues is done by various researchers with their possible solutions. New solutions and protocols can be invented to cope with malicious vehicles in VANET with target to reduce delay and packet drops additionally maintaining network throughput [6].

Algorithm

Step1 Build a network of given number of nodes in specific area on the fast ways.

Step2 Build a connection between the vehicle node and the road side infrastructure.

Step3 Binds the Nodes with AODV protocol for path identification either direct or through the intermediate nodes.

Step4 Encrypt the data packets while sending from vehicle node to the road side infrastructure.

Step5 Protect the data from misuse by the malicious nodes.

Flowchart

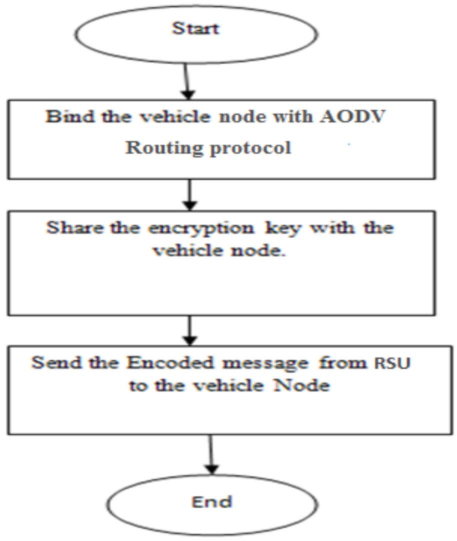
Start
Bind the vehicle node with AODV Routing protocol
Share the encryption key with the vehicle node.
Send the Encoded message from RSU to the vehicle Node
End

Fig. 1: Flowchart

Performance Metrics

Three important performance metrics are evaluated:

a. Packet Delivery Ratio

The Ratio of the data Packets Delivered to the Destinations to those generated by the traffic type Sources.

Where P_r is total Packet Received & P_s is the total Packet Sent.

PDR= (Pr/Ps)*100

b. Average End-to-End Delay of Data Packets

This includes all possible delays caused by buffering during route discovery, latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

$$\mathbf{D = (T_r - T_s)}$$

Where T_r is receive Time and T_s is sent Time

c. Success Rate

It is the rate at which success has been achieved while transmitting the packet from source to the destination. How many packets has been sent and how many packets has been received. The difference of these will be divided by the total no. of packets.

SR= (Nr-Ns)/TNp

Where N_r is number of packets received,

N_s is number of packets sent & TN_p is Total Number of packets.

Results and Analysis

Nam Animated network

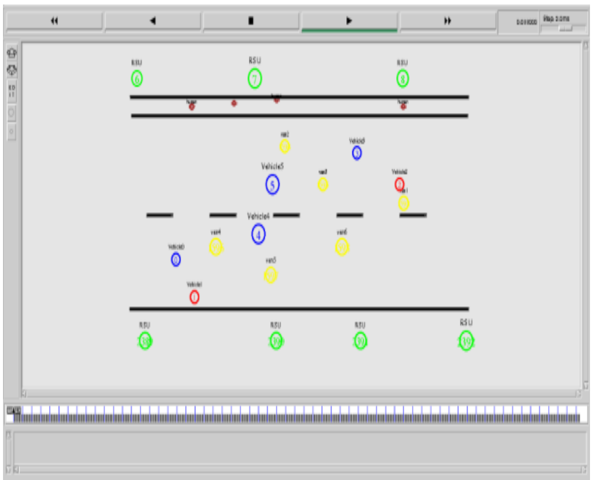

Fig. 2: Nam Animated Network

This network shows the different positioned vehicle nodes moving on the road. They moves in random way point. There are various road side equipment through which vehicle nodes communicates.

End to End Delay

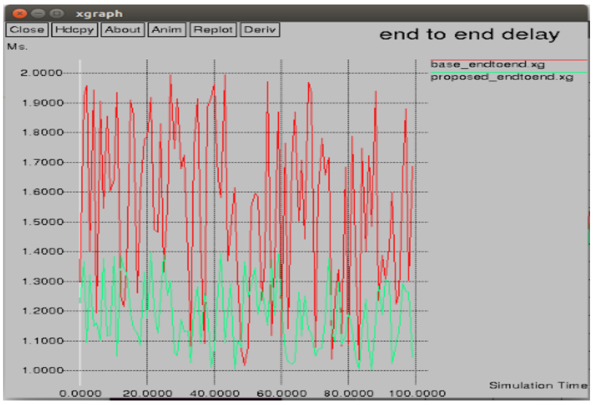

Fig 3: End To End Delay

This graph shows the end to end delay comparison of base technique and the proposed technique. Under the proposed technique symmetric key is used. So that only trusted node can communicate to each other. Red shows the end to end delay of the base paper. Green shows the end to end delay of the proposed technique. Proposed technique imparts better end to end delay. Such that the result for end to end delay has improved.

Graph for comparison

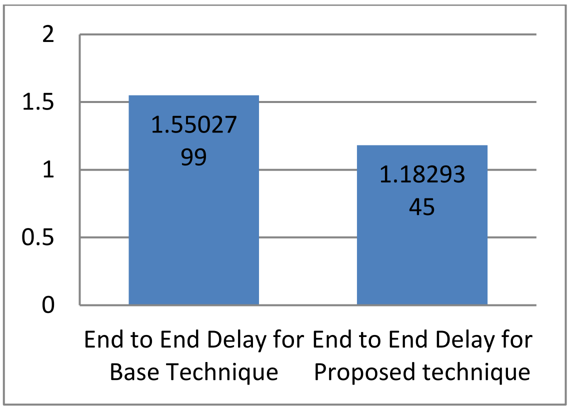

Fig. 4: End To End Delay

This graph shows the end to end delay comparison. It is clearly shown that the end to end delay has improved in the current research technique where symmetric key is used. The result has improved to 31%.

Packet Delivery Ratio

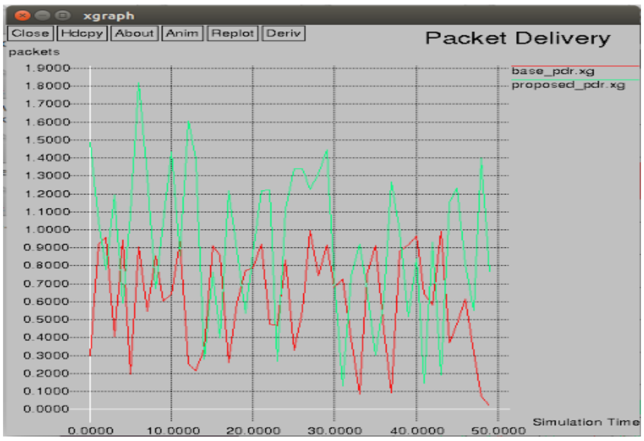

Fig 5: Packet Delivery Ratio

This graph shows the packet delivery ratio for both base and proposed technique. Proposed technique has better packet delivery ratio, such that more number of packets will be delivered to the destination.

Graph for comparison

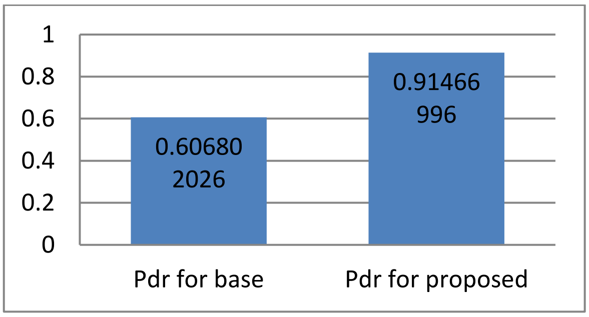

Fig. 6: Packet Delivery Ratio

This graph shows the packet delivery ratio for both base technique and the proposed technique.

Success Ratio

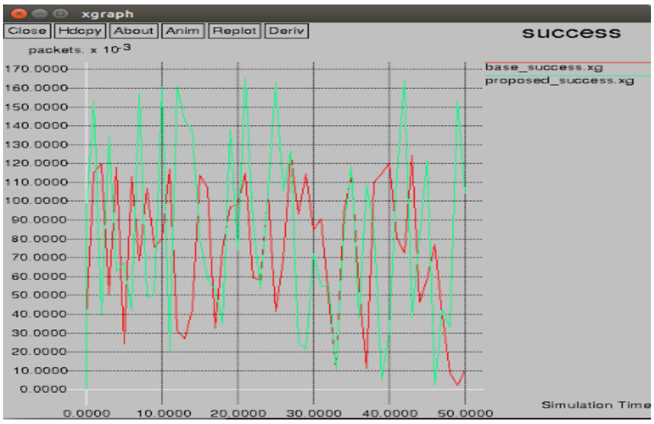

Fig. 7: Success Ratio

This figure shows the success rate for both previous and current research. Success ratio for proposed has higher range that signifies more packets are delivered successfully. Because the symmetric key builds the safe environment as compared to the direct communication without any security measure.

Graph for comparison

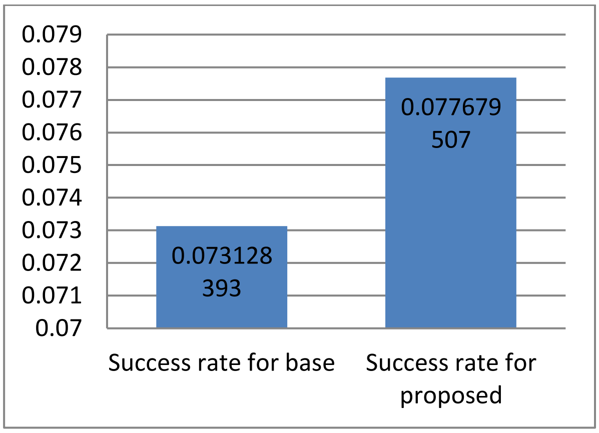

Fig. 8: Success Rate

The graph shows the success rate for both base and proposed technique. Success rate for proposed technique is better than the base. There is an improvement of 6.33% for proposed technique.

Percentage Improvement table

Table 1: Percentage Improvement Table

Parameter	Percentage Improvement
End to End Delay	31.053%
Packet Delivery ratio	33.65%
Success Rate	6.22%

Conclusion

For position based vehicle nodes, their position related information is required to send to other vehicles or to RSUs. The information being send must be secure from malicious vehicle nodes. While moving vehicle nodes communicates to the road side units, these road side units sends the message packets regarding road conditions. So that safe driving can take place. But during the communication various types of malicious nodes sniff the information which does not belongs to them. In such situation sometimes possible for malicious node to send wrong message packets. Under such condition the performance can be downgraded. Using symmetric key various types of nodes which are authorized can communicates. Such situation is useful for building safe environment. Under symmetric key various performance parameters has been checked such that various parameters has shown the improvement. End to End delay has improved by 31%, Packet Delivery Ratio has improved by 33.65% and Success Rate has improved by 6%.In future various other symmetric technique can be tested or symmetric technique can be deployed, So that performance can be further enhanced.

References

1. B. T. Sharef, D. Vinod Kumar "Survey: Secure Routing Invanet" *International Journal of Advanced Research in Computer Science & Technology* Vol. 4 pp. 456-463, 2016.
2. P. Salvo, Gregorio Martı,"TRIP, A_Trust_And_Reputation_Infrastructure-Based Proposal for Vehicular Ad Hoc Networks" *Journal of Network and Computer Applications* vol. 4, pp.934–941, 2015.
3. P. tyagi, D. Dembla "Trust Based Scheme for Location Finding in Vanets" *Advances In Optical Science And Engineering, Springer Proceedings* vol. 4 pp. 345-352, 2014.
4. F. Cunha, B. K. Chaurasia, "AHP Based Trust Model in Vanets" *2013 5th International Conference on Computational Intelligence and Communication Networks*, vol. 3 pp. 789-794, 2014.
5. R. S. Raw, M. Kumar, "Trust Computation In Vanets" *2013 International Conference On Communication Systems And Network Technologies*, vol. 3,pp.567-572,2014
6. N. k. Chaubey, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks" *IEEE SYSTEMS JOURNAL*, VOL. 8, NO. 3, pp. 321-330, 2014.
7. R S. Raw, M. K. N. Singh "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET" *International Journal of Network Security & Its Applications (*IJNSA), Vol.5, No.5, September 2013.
8. S. Vinothini, Mr. J. John Raybin Jose, "A Review On Routing Protocols In VANET" *International Journal Of Advanced Research In Computer And Communication Engineering* Vol. 4, Issue 7, July 2015.
9. J.Zhang, 2011, "A Survey on Trust Management for Vanets" *In International Conference on Advanced Information Networking and Applications,* Pp.105-112, 2014.
10. Vinh Hoa La, Ana Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey", *International Journal on Adhoc Networking Systems (Ijans)* Vol. 4, No. 2, April 2014.