International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

Message Authentication inVANET Using CRP

Sayeda Ayesha, Poonam Dhamal

Ayeshasayed15@gmail.com and 8983899433

Abstract — Now a days VANET is becoming wide range application as its more abilities and less cost compare to wired network. We should provide security as VANET is of inherent nature. Attack of flooding is belonging to DOS attacks. Attack of flooding disturbs performance by generating the floods of request packets. It blocks the original data packet which supposed to travel to destination. It weakens the VANET by consuming power batteries space and the bandwidth. Malicious node flooded the hello packets continuously. So the next node cannot send packets to destination. In this case one of neighbor send the error packet to source and source again start the rout discovery function. So the hello interval value updated and informs other node securely. This process will avoid attack of flooding considerably. This process calculates packet delay, packet delivery ratio, throughput etc. Algorithm achieved by the AODV and will get test in ad hoc network. It will decrees control overhead by 2%.

Keywords— VANET, Flooding, Challenge-response-protocol, Malicious _ Node _ Table, AODV, Detection of malicious node.

INTRODUCTION

VANET is consisting of nodes which are mobile in nature and the links between the mobile nodes. These are getting disturb due to the various attacks occurred on VANET. Network is constructed by components mobile nodes and links. VANET defines their characteristics according to such components. Nodes consisting of characters like mobility, constrained resources, poor physical protection. Wireless link have unique properties like bandwidth and open transmission medium. It shows in fig.1. VANET is influenced by different kind of attacks. DOS is one who makes the VANET harmed. This attack is consisting of attack of flooding, wormhole and black hole. These kinds of attacks increase delay, packet loss, usage of bandwidth. It affects the throughput. In black hole attack source received the fake rout reply from attacked node. In such case node do not forward the packet to destination. In wormhole attack only one attacked node is getting involved.

In attack of flooding message from source is delivered to all nodes and it has relevance in ad hoc networks. For example, algorithms like AODV and DSR depends on flooding to get routing data. Flooding is belonging to DOS attack, and it floods either the control packets or data packet too. It damages the network. It affects resources power, and bandwidth. In the discovery of rout process it may flood RREP or RREQ packets. In such scenario source becomes malicious node. When new node enters in VANET, it will send RREQ to its neighboring nodes for validity in network.

Then neighboring node will send a data packet containing one secret question using a CRP (challenge-response protocol) and a hash key to newly entered node. (CA will provide a common Hash key to all authenticated nodes in VANET)

If the newly entered node is authenticated node, then it will use same hash key to answer the question and reply to neighboring nodes. If the newly entered node is not an authenticated node, then it will use its own hash key to answer the question and reply to neighboring nodes. This elaborated in fig1.

Neighboring node will check a reply packet, if answer is same as expected then it will forward a RRES packet to newly entered node, else it will declare newly entered node as malicious node and keep its information in Malicious Node Table. And will broadcast a data packet containing information about malicious node.

Then neighboring node will discard all incoming messages from malicious node, which prevents flooding a routing table or other scars resources in node.

When SENDER node wants to send a data packet to DESTINATION node, it will broadcast a RREQ for routing information to forward a packet using AODV routing protocol.

- Its neighboring nodes will reply to sender using RRES as per the route available to destination node.

- A sender node then checks the routing path with MNIT to check if any node in route is malicious node. If it found any malicious node in route, it will discard that route and select next shortest route.
- In this way with a secure path, data packet will be delivered to destination node.

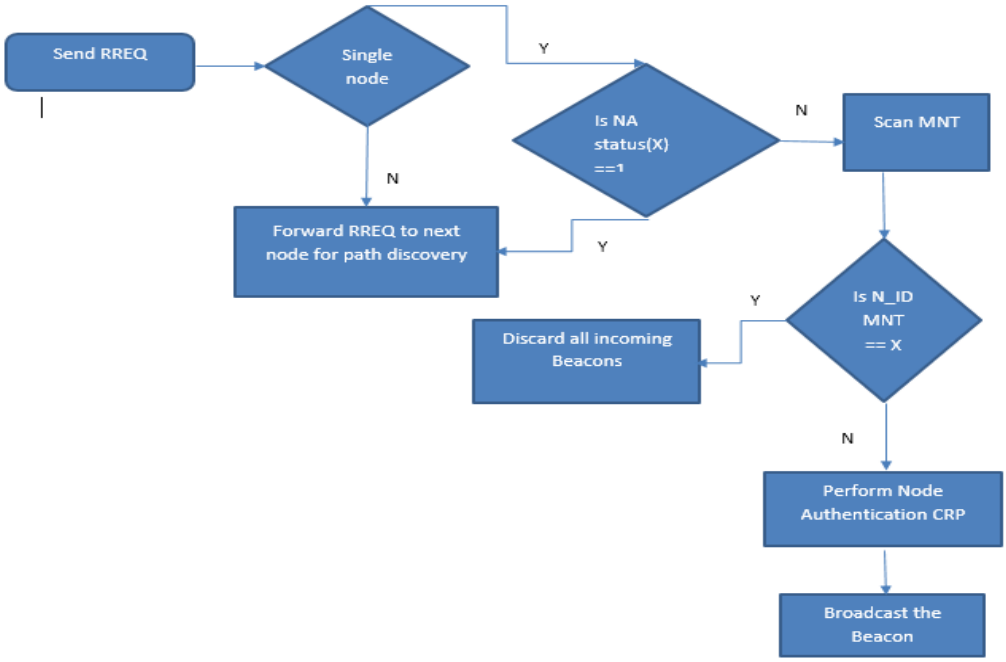

Fig 1: System flow

a. Motivation:

To prevent VANET from flooding attack by detecting malicious node, we are using the node authentication framework. This framework is based on a challenge – response protocol and a hash function. In this framework, a node gets authenticated by its legitimate neighbor node present in the network. If the malicious node is detected during the authentication, its information will be broadcasted by legitimate neighbor nodes. Other legitimate nodes keep this information in their Malicious Node Table (MNT). Then other legitimate nodes will discard all incoming packets from malicious node by checking its entry in MNT. In this way legitimate nodes will get prevention from flooding attack by the malicious node. For data packet delivery from source node to a destination node, AODV routing protocol will be used.

LITERATURE SURVEY

Significant works have been done in securing the ad hoc network. Some researches defined the techniques for secure routing but secure routing also can not able to handle the flooding attack. Nikos Komninos et al. used the zero knowledge protocol and challenge response protocol for node authentication. The work is divided into two steps. In first step, the node authentication procedure attempts to determine the true identity of the communicating nodes through a non-interactive zero knowledge protocol. In second step the authentication procedure seeks again the identities of the communicating nodes through a challenge-response protocol. They used challenge response protocol for node to node authentication. The main problem with this method was increased network overhead due to multiple packets used for node authentication [1].

C. Perkins et al. presents concept of AODV routing protocol. AODV routing protocol uses RREQ, RRES, and RERR control packets. RREQ is route request control packet send by node to find a route for packet forwarding; RRES is route response packet send against RREQ. RERR is route error packet broadcast when node leaves the network. In this paper authors explained working of AODV routing protocol [2].

Madhavi et al. have been proposed a methodology to detect and prevent the flooding attack using signal strength and client puzzle method. To implement this author uses concept of Hello message. Hello message is RREP Route reply message. Two variables Allowed _ Hello _ Loss and Hello _ Interval are used to determine lifetime of Hello message. This approach decreases

the control overhead by 2%. The result obtained in this work is pertaining to the presence of only one kind attack that is flooding attack. Presence of more than one kind of attacker may affect the performance of the network [3].

Ping Yi et al. have proposed the distributive approach to prevent the flooding attack, in which three threshold values are used; Rate _ Limit and Blacklist _ Limit and Blacklist _ Timeout. This approach checks RREQ count of each node with Rate _ Limit Threshold value and Blacklist _ Limit threshold value. This method can Handel the network with high mobility [4].

Jian-Hua Song et al. have analyzed the flooding attack in anonymous communication. In this approach, the threshold tuple is used which consist of three components: Transmission _ Threshold, Blacklist _ Threshold and Whitelisting _ Threshold. If any node generates RREQ packet more than transmission threshold then its neighbor discards the packet. If it crosses the transmission threshold more than blacklist threshold then it black list the node. But to deal with accidental blacklisting they defined white listing threshold. If any node performs good for number of intervals equal to white listing threshold then it again start treating as a normal node. Problem with this approach is increased node overhead as every time node has to check status of other nodes [5].

Venkat Balakrishnan et al. used the extended DSR protocol based on the trust function to mitigate the effects of flooding attack. In this technique, authors have categorized the nodes based on the trust value: Friends, acquaintance and stranger. Friends are trusted nodes, Stranger are non-trusted nodes, and acquaintance has the trust values more than stranger and less than friends. Based on relationship they defined the three threshold value. If any node receives the RREQ packets then checks the relationship and based on that it checks for the threshold value if it is less than the threshold then forward the packet otherwise discard the packet and blacklist the neighbor node. The main problem with this method was it does not work well with higher node mobility [6].

Djamal DJENOURI et al. have presented different security requirements in VANET, VANET features and their impact on security in VANET. Also authors have discussed different attacks at different layers in network. Also different routing attack and their impact in network is discussed. Then different existing solutions to different attacks have been discussed. Some of them are, Authentication during all phases by using trusted functions provided by certificate authority, Define new merits by providing trust value, secure neighbor detection by using three round authenticated message exchange between two nodes [7].

Yiu-Chun hu et al. have presented rushing attack defense mechanism Using Secure neighbor detection, Secure route delegation, and Randomize route request forwarding. Secure neighbor detection by using three round authenticated message exchange between two nodes. Secure route delegation in which receiver of route request performs secure neighbor detection for initiator of route request. In Randomize route request forwarding, it randomly select the by collecting maximum route request in given timestamp. Problem with this mechanism is node overhead increases if multiple nodes sends route requests at same time or with very little time span [8].

H Deng et al. Have used concept of Identity-based cryptography and threshold secret sharing for distributed key management and authentication. Authors have used self-organizing way to provide key generation and key management service instead of using traditional pre-fixed trust relationship between nodes. In this scheme authors avoid centralized certificate authority to distribute public keys and certificates which saves network bandwidth and reduces network overhead [9].

B. Wu et al. have described attacks at different layers in MNET and their countermeasures. They have discussed security mechanisms such as prevention mechanism, defense against physical layer, link layer, and key management attacks [10].

In our work, we are using concept of node authentication via challenge response protocol(CRP) and hash key same as [1], which will prevent flooding of authenticated node from malicious node by identifying malicious node and discarding all incoming messages from malicious node. In AODV routing protocol, node uses RREQ and RRES control messages to establish route for message forwarding. Message authentication is based on RREQ control message generated by AODV routing protocol and secret questions and answers generated by CRP. Also we are using MNT for storing information about malicious message detected by CRP. For routing and message forwarding, we are using AODV routing protocol, security will be maintain by MNT.

SYSTEM ARCHITECTURE

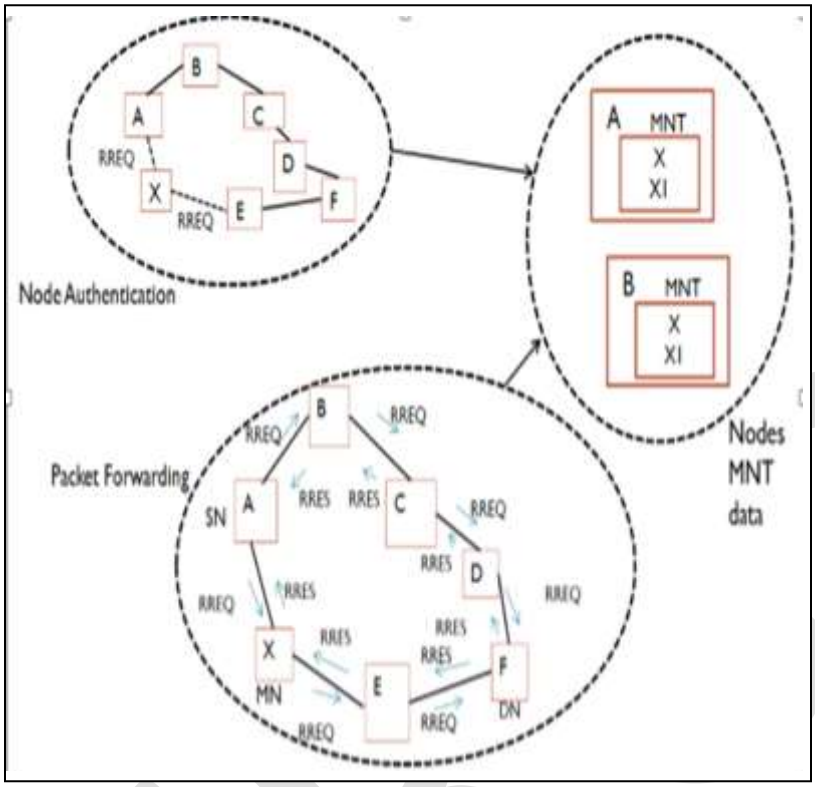

Fig. 2 System Architecture

Where,

X: Newly entered node

A, B, C, D, E, F: Authenticated nodes in VANET

RREQ: Route Request

RRES: Route Response

MN: Malicious node

SN: source node

DN: Destination node

MNT: Malicious Node Table

As shown on fig.2**,** this system is mainly divided into two parts,

1. New Node authentication

2. Packet forwarding

In above figure, during node authentication phase, when X enters in VANET, it sends RREQ to A and E. Then node A and E perform CRP to authenticate new node. During packet forwarding phase, suppose node A wants to forward a data packet to node F, it broadcast RREQ to F through its neighboring nodes. Then node F sends RRES. Routes as shown in figure are A-X-E-F and A-B-C-D-F. As A-X-E-F is shortest path, A will select this route and check all intermediate nodes, if any malicious node present in selected path using MNT. In this case we are considering X as malicious node. Therefore first selected route contains malicious node, so A will discard this route and select second shortest route.

The main goal of our approach is to provide resource aware node authentication framework to prevent flooding attack in VANET, i.e which consumes less resources to perform node authentication and flooding attack prevention.

- **Node authentication using CRP**

Our Node authentication framework is based on RREQ control packet generated by the AODV routing protocol and secret questions and answers generated by CRP.

To prevent flooding attack using MNT information

We are using the Malicious Node Information Table (MNT) for keeping information about a malicious node detected by CRP. A Flooding attack can be tackle by checking RREQ requester node's entry in MNT and discarding further incoming packets from requester node, if it is present in MNT.

Routing using AODV routing protocol

For the data packet forwarding from originator node to destination node, AODV routing protocol is used.

- **System components**

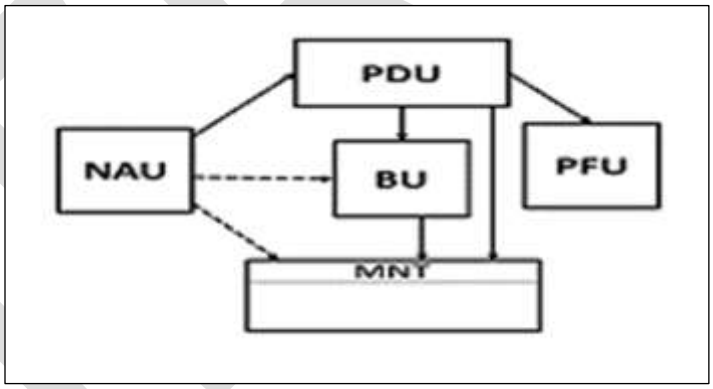

Fig. 3 system components

Fig. 3 shows system components of our system. Our system includes; Node authentication Unit (NAU) to perform new node authentication using CRP; Path Discovery Unit (PDU) to discover secure path for data packet forwarding using AODV routing protocol; Broadcast Unit (BU) to broadcast RREQ control packet generated by PDU also to broadcast data packet containing information about malicious node gathered from NAU; Malicious Node Table (MNT) is used to keep information about malicious node broadcasted by NAU; Packet Forwarding Unit (PFU) to forward data packets from originator node to destination node.

- **Advantages:**

Due to existence of large number of VANET applications in society today, the security of VANET plays a significant role. As VANET is infrastructure-less multi-hop network, every node in VANET is responsible for secure packet delivery. Hence, we have proposed the node authentication framework which prevents VANET from flooding attack in higher mobility. Also this framework reduces nodes resource consumption. Our node authentication framework required less authentication time to authenticate nodes in

VANET than existing system. Also Control overhead is decreases as minimum control packets are transmitted during node authentication and path discovery.

IMPLEMENTATION DETAILS

A. Proposed system

The proposed system of our approach contains following modules:

1. Flooding prevention using CRP and AODV

2. Secure message forwarding using MNT and AODV

1. Flooding prevention using CRP and AODV:

Fig. 1 shows system flow of our approach. In our approach, whenever a new message enters in VANET, it will send control message containing RREQ and token using AODV routing protocol to its s for validity in network. Then Neighboring message will respond to newly entered message via a data message containing one secret question using a challenge response protocol and a hash key provided by certificate authority.

- If the newly entered message has authenticated hash key, then it will use same hash key to generate answer for the question asked by Authenticated message s and respond to them. Neighboring Authenticated message s will check a reply message, if answer generated by newly entered message is same as answer generated by Authenticated message s, then it will forward a RRES control message using AODV routing protocol to newly entered message , and allow it to provide fresh route in VANET.
- Else Authenticated message s will declare newly entered message as malicious message by broadcasting a data message containing information about malicious message in VANET and keep its information in MNT.

- If newly entered message is malicious message, then neighboring messages will discard all incoming messages from malicious message, which prevents flooding a routing table or other scars resources in message.

2. Secure message forwarding using MNT and AODV:

To forward a data message to destination node, a sender node has to broadcast a RREQ for routing information using AODV routing protocol. Then intermediate nodes will reply to SENDER using RRES control message as per the route availability from sender message to destination message. After receiving a shortest route, a sender message checks the routing path with MNT to check whether any message in a route is malicious message. If it found any malicious message in route, it will discard that route and select next shortest route. In this way with a secure path, data message will be delivered to destination.

B. Algorithms

a. Challenge- response protocol for message authentication:
This protocol is based on exchanging secret questions and answers between Nodes. In our approach, we are using CRP for authenticating new messages validity in Network using RREQ generated by AODV routing protocol.

Algorithm 1: Message authentication using CRP

1. X, A, HashK, ans, AN, MM, SQ;

Where X = new message, A= Authenticated message,

AN=Authenticated node, MM = malicious Message, ans=answer generated by messages, HashK = Hash key of messages, SQ = secrete question

2. newMessage (X) { new message enters in VANET }

3. sendRREQ (X, (A,..)) { new message send RREQ to

Neighboring messages for their validity in VANET}

4. genSQ(HashF) {generate secrete question using CRP and Hash function}

5. sendSQ((A,..),X) {Authenticated message send SQ to X}

6. genAns(HashF) {ans = SQ+HashK}

7.sendAns(X,(A,..)) {X send(ans) to neighboring nodes}

8. chkAns(ans){

9. If (ans(X) = ans(A,..), then {X = AN

10. sendRRES((A,..),X)}

11. Else X = MM Insert into MNT (X);

12. If(X = MM), then {Sql query for inserting data about

Malicious message into MNT}

13. Broadcast( ) { sendData(X)}

14. Discard( ) {RREQ from X}

b. AODV routing protocol for message forwarding:

In AODV routing protocol, message uses RREQ and RRES control messages to establish route for message forwarding.

Algorithm 2: Message _ forwarding

1. Message A, B, C, D, E, F, X, route

Consider message A= sender message and message F =receiver message

2. sendRREQ(A,F) {A send RREQ to F via Neighboring messages}

3. rcvRREQ(message) {message receives RREQ}

4. sendRRES(F,A) {via Neighboring messages }

5. routeSelect(){

6.rcvRoute(route)

7.if (route(message = X) scan route using MNT, then delete(route)

8. else frwdpckt(A, F) }

C. Mathematical Model

a. Initialization and data packet forwarding in OTNA

Input: N2 = new node, N1 = legitimate node in VANET, RREQ= Route Request, MNT(NodeName) = Malicious node table, N1(RTStatus) = Routing table's status field

1: N1 ← RREQ(X) //'N1' receives RREQ from N2

2: 'N1' checks its routing table's status field for N2's validity in the network.

3: **if** N1(RTStatus(X)) = 1 then

4: Then proceed RREQ for route discovery

5: **else**

6: Check entry of N2 in MNT

7: **if** MNT(NodeName) = N2 then

8: discard all incoming packets from N2

9: **else**

10: call algorithm 1 //perform Node authentication

11: **end if**

12: **end if**

b. CRP based Node Authentication in OTNA Protocol

Inputs: N2 is new node, N1 is legitimate node in VANET. M_n = Messages

1: N1 : CRPK ← {0,1}ι // node 'N1' takes ι - bit long dynamically generated CRP key.

2:(M1) = (CRPK) //'N1' generates secret question CRPK on dynamically generated input and send it to 'N2'.

3: N1 → N2: <Challenge,M1>

4: $(M2)_H$ = SHA1(CRPK) // 'N1' computes answer for the same question using hash function.

5: $(M3)_H$ = SHA1(CRPK) // 'N2' computes answer for the same question using hash function.

6: N1 ← N2: <Response,M3> //'N1' receives answer from 'N2'

7: **if** $(M2)_H = (M3)_H$ then

8: N1 → * : <LN> // declare N2 as is legitimate node and broadcast LN to all legitimate nodes in VANET.

9: **else**

10: N1 → * : <MN> // 'N1' declare 'N2' as malicious node and broadcast MN to all legitimate nodes in VANET.

11: **end if**

12: All nodes store this information in their MNT

13: Set (RTStatus(N2) = 0)

RESULT ANALYSIS

Fig 4 shows control overhead v/s number of nodes. The term Control Overhead (CO) can be defined as the total number of exchange of control packets from source to destination before transmission of packets divided by total number of packets to be transmitted into the network.

CO = *Number of control packets / Total number of packets data and control*

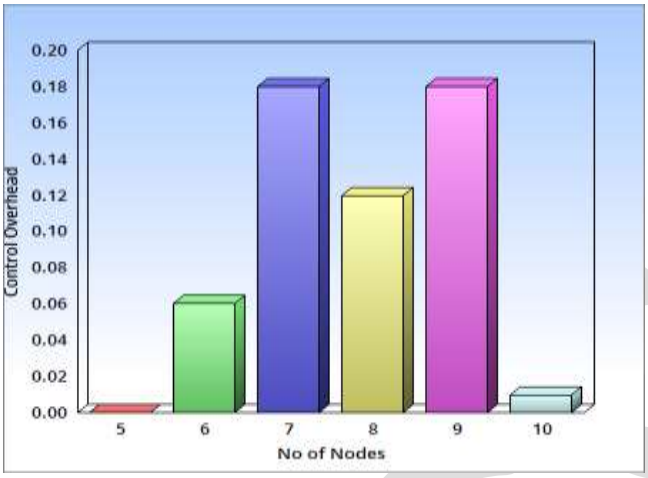

Fig 4: Control overhead

In our approach, we are performing the node authentication for each node only once; therefore control overhead is reduced because minimum control packets are transmitted during the node authentication and a path discovery. As shown in Fig. 4, at number of nodes 7 and 9 control overhead increases as we are performing node authentication for new nodes. Whereas at number of nodes 8 control overhead decreases as at this point RREQs are from the legitimate nodes. Fig 5 shows node authentication time v/s number of nodes. We have calculated time required to perform the node authentication by using system timer. As shown in Fig 4, the authentication time required to authenticate multiple nodes simultaneously is comparatively decreases when the number of nodes increases in the network.

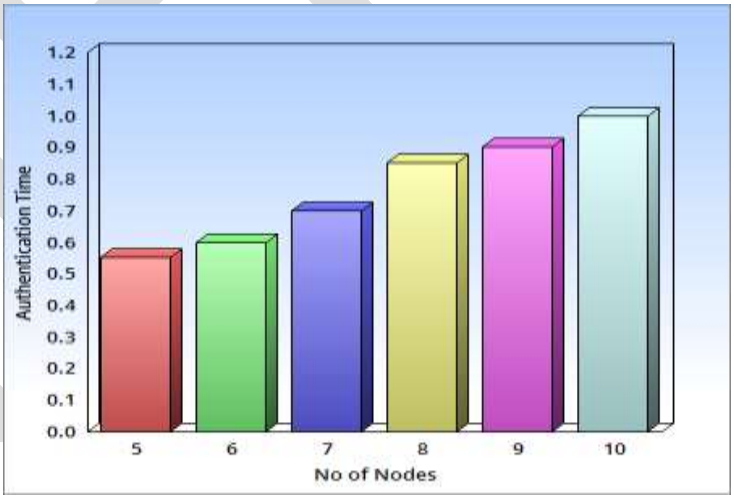

Fig 5 Authentication time

ACKNOWLEDGMENT

This is to acknowledge and thank all the individuals who played defining role in shaping this IJERGS paper. Without their constant support, guidance and assistance this paper would not have been completed. Without their Coordination, guidance and reviewing this task could not be completed alone.

I avail this opportunity to express my deep sense of gratitude and whole hearted thanks to my guide Prof. Poonam Dhamal for giving her valuable guidance, inspiration and encouragement to embark this paper.

I would personally like to thank Prof. Mrs. Poonam Gupta, Head of PG, Computer Dept. at GHRCEM, Pune, and our principal Dr. D. D. Shah sir who creates a healthy environment for all of us to learn in best possible way.

CONCLUSION AND FUTURE SCOPE

Due to existence of large number of VANET applications in society today, the security of VANET plays a significant role. As VANET is infrastructure-less multi-hop network, every node in VANET is responsible for secure packet delivery. Hence, we have proposed the node authentication framework which prevents VANET from flooding attack in higher mobility. Also this framework reduces nodes resource consumption. Our node authentication framework required less authentication time to authenticate nodes in VANET than existing system. Also Control overhead is decreases as minimum control packets are transmitted during node authentication and path discovery. We have provided secure data packet delivery by using MNT and AODV. In future we can implement same framework for other routing protocols in VANET.

In the future work, the proposed scheme will be simulated to measure the different performance metrics like packet delay Data Packet Delivery Ratio, throughput, control overhead and Number of nodes.

REFERENCES:

[1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,” Proc. Workshop Standards for Privacy in User Centric Identity Management, July 2006.

[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “CARAVAN: Providing Location Privacy for VANET,” Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.

[3] A. Wasef, Y. Jiang, and X. Shen, “DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.

[4]M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks, ”J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5]Y.Sun,R.Lu, X.Lin, X.Shen, and J.Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets,” IEEE Trans. Vehicular Technology, vol. 61, no. 1,pp. 86-96, Jan. 2012.

[7]US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/Passenger_vehicles_in_the_United_States, 2012.

[8] J.J. Haas, Y. Hu, and K.P. Laberteaux, “Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,” Proc. Sixth ACM Int’l Workshop Vehicular Inter Networking, pp. 89-98, 2009.

[9] IEEE Std 1609.2-2006, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[10] “5.9 GHz DSRC,” http://grouper.ieee.org/groups/scc32/dsrc/ index.html, 2012.

[11] A. Wasef and X. Shen, “MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks,” Proc. IEEE GlobeCom, 2009.

[12] J.P. Hubaux, “The Security and Privacy of Smart Vehicles,” IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

[13] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs,"Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), pp. 1-9, 2009.

[14] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P.Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 15571568, Oct. 2007.

[15] P.P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate Revocation List Distribution in Vehicular Communication Systems,"Proc. Fifth ACM Int'l Workshop Vehicular Inter-Networking, pp. 86-87, 2008.

[16] K.P. Laberteaux, J.J. Haas, and Y. Hu, "Security Certificate Revocation List Distribution for VANET," Proc. Fifth ACM int'l Workshop Vehicular Inter-Networking, pp. 88-89, 2008.

[17] H. Chan, A. Perrig, and D. Song, "Random Key Pre distribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 197-213, 2003.

[18] L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

[19] S. Zhu, S. Setia, S. Xu, and S.Jajodia, "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks," J. Computer Security, vol. 14, pp. 301-325, 2006.

[20] A. Wasef and X. Shen, "PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 1458-1463, 2008.

[21] A. Wasef and X. Shen, "EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 9, pp. 5214-5224, Nov. 2009.

[22] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. 21st Ann. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.

[23] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.

[24] "Crypto++ Library 5.5.2," http://www.cryptopp.com, 2012.

[25] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic CurveDigital Signature Algorithm (ECDSA)," Int'l J. Information Security,vol. 1, no. 1, pp. 36-63, 2001.

[26] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM, pp. 246-250, 2008.

[27] "The Network Simulator - ns-2," http://nsnam.isi.edu/nsnam/index.php/User Information, 2012.

[28] "Traffic and Network Simulation Environment - TraNS," http://trans.epfl.ch, 2012.