A-DSR: A New Approach to Improve Performance of E-DSR Algorithm for Security in Vehicular Ad Hoc Network

Patel Juhi Kaushal[1] Chaita Jani[2]
[1]M.E Student [2]Assistant Professor
[1,2]Department of Computer Science Engineering
[1,2]Kalol Institute Of Technology, Kalol, Gujarat, India

Abstract— A Vehicular Ad-Hoc Network or VANET is a sub form of Mobile Ad-Hoc Network that provides communication between vehicles and between vehicles and road-side base stations. Vehicular Ad hoc Network can ease our life by making driving safe in near future. Privacy navigation utilizes the online road information collected by a vehicular ad hoc network (VANET) to guide the drivers to desired destinations in a real-time and distributed manner. In this proposed system DSR-RS routing protocol and AES(RC6) routing algorithm is used for improve new A-DSR routing protocol using NS-2 simulator. We compare the performance of these routing protocol on the basis of various parameters such as throughput, packet delivery ratio, delay and control overhead.

Key words: Vehicular Ad-hoc Network; DSR Routing protocol; NS2 (Simulator);RC6 Encryption Algorithm; Throughput; Delay; Packet Delivery Ratio; Control Overhead

I. INTRODUCTION

VANET is an ad-hoc network formed between vehicles as per their need of communication. A Vehicular Ad-Hoc Network or VANET is a sub form of Mobile Ad-Hoc Network or MANET that provides communication between vehicles and between vehicles and road-side base stations. VANET is mainly aimed at providing safety related information and traffic management. VANET is very beneficial in providing safety to the road users and comfort to the passengers. VANET introduces more challenges aspects as compare to MANET because of high mobility of nodes and fast topology changes in VANET. A VANET is a wireless network that does not rely on any central administration for providing communication among the so-called On Board Units (OBUs) in nearby vehicles, and between OBUs and nearby fixed infrastructure usually named Road Side Unit (RSU).

The DSR is a very simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes .DSR allows the network without the need for any existing network infrastructure. The Dynamic Source Routing protocol allows mobile sources to discover paths towards any desired destination dynamically. Every data packet includes complete list of nodes, which the packet must pass before it reaches the destination. DSR can support fast network topology changes and service even asymmetric links; it can successfully find paths and forward packets in unidirectional link environments.

The RC6 encryption algorithm helps to secure the data or message which is transmitted between the sensor nodes.RC6 is considered to be a strong algorithm with a fast and easy hardware Implementation. RC6 is a symmetric block cipher based on RC5 and developed by Rivest, Sydney, and Yin for RSA security. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits like RC5. It also uses an extra multiplication operation that is not there in RC5.

II. LITERATURE SURVEY

Paper presented by D. B. Jagannadha Rao ,Karnam Sreenu, Parsi Kalpana [1] that A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks which is proposed that DSR protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. Source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. DSR is usually on-demand. This paper gives all information about Route Discovery and Route Maintenance. Further improvements are to the performance of DSR, for example to allow scaling to very large networks, and the addition of new features to the protocol, such as multicast routing. Its goal is to create an integrated set of protocols that allow mobile computers, and the applications running on them and communicating with them.

Paper presented by V.Anji Reddy, P.Siva Prasuna, Rittika.D.Varu, P.Nikhila, N.SriLakshmi [2] that Performance Analysis of DSDV, DSR Routing Protocols in Vehicular Ad-Hoc Network(Vanets) which is proposed that author can calculate different types of performance metrics such as Throughput, End-To-End Delay. By calculating such type of performance author can estimate which Vanets protocol is better by comparing the same metric in all the routing protocols. In this paper author use VanetMobisim and NS2 to simulate DSDV and DSR routing protocols with realistic mobility model. This paper conclude that DSR is preferable for end to end delay is compare to DSDV and as number of nodes increases throughput of DSR as compare to DSDV.

Paper presented by Abduladhim Ashtaiwi,Abdusadik Saoud and Ibrahim Almerhag [3] that Performance Evaluation of VANET Routing Protocols which is proposed that in vehicular networks, routing Collision Avoidance Messages (CAMs) among vehicles is a key communication problem. Many routing protocols have been adapted for VANETs, such as DSDV (Destination Sequenced Distance Vector), AODV (Ad-hoc On demand Distance Vector), and DSR (Dynamic Source Routing). This work compares the performance of those routing protocols at different driving environments and scenarios created by using the mobility generator (VanetMobiSim) and network simulator(NS2). The obtained results at different vehicular densities, speeds, road obstacles, lanes, traffic lights, and

transmission ranges. This paper conclude that DSR protocol showed better performance, at certain values of simulation parameters, than AODV and DSDV protocols.

Paper presented by Amol Bhosle [4] that Improving Performance And Securing Data In MANET With AES which is proposed that to improve the security of such network and to improve the efficiency of Adhoc on demand distance vector routing protocol technique proposed here is SMDNA (Securing MANET Data using Node Authentication) that combines the features of Symmetric and asymmetric cryptographic algorithms and digital signature. This protocol design provides the integrity, confidentiality, nonrepudiation and authentication with the help of AES, and digital signature. In this paper author use symmetric encryption algorithm. Proposed method works better with AES than IDEA and DES symmetric cipher algorithms.

Paper presented by Mamoun Hussein Mamoun [5] that A Proposed Route Selection Technique in DSR Routing Protocol for MANET which is proposed that performance results show that the propagated route request overhead can be reduced by more than 30% under high node mobility also proposed algorithm can significantly reduce the average end-to-end delay. In this paper author use fuzzy logic based rebroadcasting decision as a route selection method. The proposed DSR-RS algorithm is compared with the DSR algorithm in terms of route request overload, packet delivery ratio and end-to-end packet delay. The packet delivery ratio is higher for our proposed algorithm as it is compared with DSR routing algorithm.

Paper presented by Sharmin Sultana, 2Salma Begum, 3Nazma Tara, 4Ahsan Raja Chowdhury [6] that Enhanced-DSR: A New Approach to Improve Performance of DSR Algorithm which is proposed that this paper analyzes through simulating an improvement of basic DSR to enhance its performance. In the Enhanced-DSR (E-DSR), to reduce Route Request Packet overhead, multicasting approach is used using Route Record field of Route Request option. The basic problem of DSR has been improved by reducing Route Request overhead and shortening packet length which has been shown by using the extended version of ns2.This paper concluded that reducing Route Request packet and Truncating the packet header length E-DSR gives better performance than DSR.

III. E-DSR ALGORITHM

E-DSR means ENHANCED DSR. During the route discovery process, each node takes part in forwarding Route Request (RREQ) packet. Each node except the intended destination forwards the Route Reply (RREP) packet to create the route. These RREPs increase the number of multiple paths to reach destination, they increase the control packet load of the network. Its proposal is to modify the basic DSR to reduce the redundant RREPs and the control packet overhead.

A. Reduction of Control Packet Overhead:

In Basic DSR, any host discovers a route to any other host through route discovery method. A host initiating a route discovery process, multicast a route request packet RREQ. When the host for which the route is requested receives the route RREQ packets, sends a route reply packet to the sender.

In DSR, to discover a route from source to destination, source broadcasts the RREP packets to its neighbors. DSR protocol maintains a neighbor table to keep track of neighbors. To overcome the problem of flooding in DSR, multicast of RREQ packet is preferable to broadcast which has proposed in E-DSR.

If in an average each node has x neighbors and there are y hops from source to destination and R is the total no. of RREQ packets then basic DSR requires,

R = xy RREQ packets to be broadcast.

This broadcast of RREQ packets imposes a higher degree of overhead in DSR.When a node X receives a RREQ packet, it will perform following steps:

1) X finds out all of its neighbors from its neighbor table.
2) X selects addresses of those nodes from neighbor table which are not present in the Route Request option [4].
3) X forwards RREQ packets to the nodes found in step 2.

B. Reduction of Packet Header Length:

To send a packet to another host, the sender sends the source route in the packet's header, giving the address of each host in the network through which the packet should be forwarded in order to reach the destination host. The sender then transmits the packet over its wireless network interface to the first hop identified in the source route. When a host receives a packet, if this host is not the intended destination of the packet, it simply transmits the packet to the next hop identified in the source route in the packet's header. Once the packet reaches its final destination, the packet is delivered to the network layer software on that host.

DSR is suited for small to medium sized networks as its overhead can scale all the way down to zero, After the route discovery when sender founds a complete route to the destination in its cache it can count the total number of hop in the route. Based on the hop count source will select a value for TTL field.

C. Data Delivery Ratio:

In E-DSR number of control packet is reduced, number of sent packet is also reduced. So there is less traffic in the network and delivery ratio is high. E-DSR is more efficient than DSR.

IV. AES (RC6) ENCRYPTION DECRYPTION ALGORITHM

RC6 algorithm has a modified Feistel structure and presented symbolically as RC6-w/r/b. w means 32 bits as the size of word, r denotes the number of round. If the size of block is 128 bits, then r, the number, is 20. b means 16byte as the number of a key.

A+B integer addition modulo 2^w
A-B integer subtraction modulo 2^w
A×B integer multiplication modulo 2^w
A<<B rotation of the w-bit word A to the left by the amount given by the least significant log w bits of B
A>>B rotation of the w-bit word A to the right by the amount given by the least significant log w bits of B
(A,B,C,D)=(B,C,D,A) parallel assignment

f(A, B) = (A2 + B2 – AB – 7) mod 2^w, two-variable algebraic expression.

(A, B, C, D, E, F, G, H) = (B, C, D, E, F, G, H, A) parallel assignment

RC6 is very similar to RC5 in structure, using data dependent rotations , addition modulo 2^w and XOR operation, in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word and not just the least significant few bits.

V. PROPOSED WORK

In proposed work I use E-DSR routing algorithm for improve A-DSR routing algorithm in Vehicular Ad Hoc Network[6]. Because E-DSR routing algorithm is get better performance of all above improved DSR routing algorithms. Our proposal is to modify the basic DSR to reduce packet delivery ratio, Average End-To-End Delay, Throughput and Packet Overhead. I will also use AES(RC6) algorithm for security purpose.

Steps for proposed work as below:

1) Using DSR routing protocol in VANET load 20 nodes and compute it in 100 meter speed of transmission range and 2Mbps transmission speed to improve accuracy of my proposed protocol.
2) Determine Route Discovery and Route Maintenance mechanisms to allow nodes to discover and maintain.
3) Apply shortest path algorithm and RC6 encryption algorithm to secure data or message transmission.
4) Now merge this two algorithms and apply proposed A-DSR algorithm.
5) Then compute routes and discover path P in Expired time T.
6) Now if route discover <T
7) Then evaluate this protocol using network simulator and mobility model.
8) Otherwise go to step 2.
9) Perform Metrics of proposed algorithm.
10) Get result.

VI. CONCLUSION

In this paper A New Approach A-DSR routing algorithm to performs better than E-DSR routing algorithm. From research AES(RC6) algorithm for provide security in Packet Delivery Ratio, Average End-To-End Delay, Throughput and Packet Overhead. This approach use shortest path algorithm and AES(RC6) encryption/decryption algorithm to improve performance of A-DSR routing algorithm.

ACKNOWLEDGEMENT

The authors would like to thank Principal, and teaching staff of Computer Science and Engineering department for providing their valuable guidance and support to carrying out this work.

REFERENCES

[1] D. B. Jagannadha Rao ,Karnam Sreenu, Parsi Kalpana, "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 8, October 2012.
[2] V.Anji Reddy, P.Siva Prasuna, Rittika.D.Varu, P.Nikhila, N.SriLakshmi , "Performance Analysis of DSDV, DSR Routing Protocols in Vehicular Ad-Hoc Network(Vanets)" , International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015.
[3] Abduladhim Ashtaiwi,Abdusadik Saoud and Ibrahim Almerhag, "Performance Evaluation of VANET Routing Protocols" , College of Information Technology, University of Tripoli.
[4] Amol Bhosle, "Improving Performance And Securing Data In MANET With AES" , International Journal of Research in Advent Technology (IJRAT) Vol. 1, No. 1, August 2013, ISSN: 2321–9637.
[5] Mamoun Hussein Mamoun, "A Proposed Route Selection Technique in DSR Routing Protocol for MANET " , International Journal of Engineering & Technology IJET-IJENS Vol: 11 No: 02.
[6] Sharmin Sultana, Salma Begum, Nazma Tara, Ahsan Raja, "Enhanced-DSR: A New Approach to Improve Performance of DSR Algorithm", International Journal of Computer Science and Information Technology, Volume 2, Number 2, April 2010.
[7] Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho, "An improved RC6 algorithm with the same structure of encryption and decryption".
[8] Ms Rupa Rani , 2Prof. Sapna Khapre ,3Prof. Nishant M. Borkar, "A Survey on Providing Privacy of Navigation In Vehicular Ad Hoc Networks (VANETs)"International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 4, Issue 1, January-February 2015.
[9] Kirti Aggarwal, "Comparison of RC6, Modified RC6 & Enhancement of RC6", 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA).
[10] Varun Patil, Premala S. Patil , "Secured and Privacy Preserving Navigation for VANET", International Journal of Electrical and Electronics Research Vol. 3, Issue 2, pp: (305-309), Month: April - June 2015.
[11] Rukaiya Y. Shaikh , Disha Deotale, "Survey on VSPN: VANET-Based Secure and Privacy-Preserving Navigation", Int. Journal of Engineering Research and Applications Vol. 4, Issue 10(Part - 5), October 2014.
[12] Monika, Sanjay Batish and Amardeep Dhiman, "Comparative Study of AODV, DSDV and DSR Routing Protocols in Vehicular Network Using EstiNet Simulator", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012.
[13] Manpreet Kaur ,Amit Kumar, "Performance Analysis in Routing Protocols for VANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.
[14] Divya Chadha, Reena," International Journal of Innovative Research in Computer and Communication Engineering" Vol. 3, Issue 3, March 2015.

[15] Ali Osman Bayrak, and Tankut Acarman," A Secure and Privacy Protecting Protocol for VANET" 2010 IEEE Intelligent Vehicles Symposium University of California, San Diego, CA, USA June 21-24, 2010.

