ISSN:0975-9646

Secure Enhance Protocol for Vehicular Ad-hoc Networks

Manish Kumar Soni[#1], Ashish Vashistha[*2]

[#1]*Research Scholar, Department of IT, IET Alwar, Rajasthan, India*

[*2]*Assistant Professor, Department of IT, IET Alwar, Rajasthan, India*

***Abstract*— Location -based routing algorithms eradicate some of the limitations of topology-based routing by using the information of the physical location of the participating nodes; therefore they are good candidates for VANETs. One type of capable location-based routing algorithm is location-based greedy forwarding: a node forwards a packet to its one-hop neighbour that is located closer to the destination than itself. Since vehicles can move with a high speed, the vehicle's moving direction has been regarded as a very important factor in routing decisions. As a consequence, the authentication of the supplier of traffic situation information and the authorization of entity's to admittance this information is essential. Accordingly it's indispensable to expand an advance security method for VANETs protocol. In this paper to proposed progress the security of location-based routing. This illumination can challenge almost each of the attacks, still those attacks which at in attendance obtainable security protocol can't treaty between, such as the maliciously drop-packets-attack approximating black hole attack, a scheme is anticipated to improve the security concert of SEVP. This method has proved effectiveness and has enhanced security.**

***Keywords*— VANET, protection, SEVP,Authentication, security method, location-based routing.**

I. INTRODUCTION

With a huge enhancement in technological improvement, we find Vehicular Communication as a explanation to several problems of our modern day communication system in roads. Vehicular Communication involve the use of short range radios in every vehicle, which would permit a variety of vehicles to converse with each other which is also known as communication and with road side infrastructure communication. These vehicles would then form an instantiation of ad hoc networks in vehicles, commonly known as VANET. It is a subset of Mobile Ad Hoc Networks. The correspondence among these two networks is characterized by the association and self organization of nodes. Also the dissimilarity between these ad hoc networks is that MANET nodes cannot renew their battery power where as VANET nodes are able to recharge them recurrently. [2][3][4] VANET is mostly planned to afford safety related information, traffic management, and infotainment services. Safety and traffic supervision necessitate real time information and this convey information can concern life or death decisions. easy and effective security method is the main problem of deploying VANET in public. Without security, VANET system is extensive open to a number of attacks such as proliferation of false warning messages as well as repression of definite warning messages, thereby causing accident. This constructs security a issue of main concern in structure such networks. VANET are of prime significance, as they are probable to be between the first profitable applications of ad hoc network technology. Vehicles are the preponderance of all the nodes, which are accomplished of forming self organize networks with no prior information of each other, whose security level is extremely low and they are the mainly vulnerable part of the network which can be attacked effortlessly. The ability of VANET technology is high with a extensive range of function being deployed in aid of consumers, commercial establishments such as toll plazas, entertainment companies as well as law enforcement authorities. However, exclusive of securing these networks, harm to life and belongings can be done at a superior extent. [1] This research work we focus on provided that the indication of VANET security and production successfully with the problems. initially, the indication of the network and security requirement will be discussed. Security in V ANETs is conserved with one of two techniques. Vehicles can moreover rely on the security services innate from the use of public key communications, outstanding to the need of such communications the load of preserve the security is absent on the vehicles of the network. It is dominant to be intelligent to trace misbehaving vehicles and turn out them from the network in a opportune manner to avoid the misbehaving vehicles from because further harm to the network This technique utilize digital signature to declaration the distinctiveness authentication, data reliability and non-repudiation. The divergence to almost all of other solutions is that an estimate method is proposed, which can distinguish malicious nodes that drop routing data. This method has been demonstrate effectiveness and has improved security and network NS2 simulation.

II. RELATED WORK

Norbert in at al[1] they have proposed concept is based on the computation of trust information regarding neighboring VANET nodes. Successful detections are used subsequently to exclude disturbing nodes from the VANET until they have proven their benignity. As great attention is given to scalability, flexibility and practicability, the proposed scheme aims to provide a basis for automated misbehavior detection in ITS.

Vivek Pathak in at al[2] In this research, they have design an infrastructure-free secure geographic routing protocol. The significance of their approach, in comparison to existing location authentication work, is that it does not require out-of-band communication or shared secret initialization. They have solution is able to achieve adhoc security management by introducing inter-nodal periodic broadcast messages for monitoring node behavior. Also

develop a novel method called geographic hash for encoding unforgeable geographic location data. Superior resource provisioning of vehicular nodes makes our solution reasonable and efficient for VANETs.

Miguel Garcia de la Fuente in at al[3] In this research they have present a performance comparison study between SIFT, a scalable, spatial-aware, TBF approach, and DREAM, a stable, largely tested PB routing scheme. The performance was evaluated within a real-world urban scenario, deploying up to 1000 nodes that move according to SSM (Stop Sing Model) , a realistic mobility pattern for VANETS.

Ghassan Samara in at al[4] Vehicular Ad Hoc Networks is an emerging and promising technology, this technology is a fertile region for attackers, who will try to challenge the network with their malicious attacks. They have gave a wide analysis for the current challenges and solutions, and critics for these solution, we also proposed a new solutions that will help to maintain a securer VANET network

Huma Ghafoor in at al[5] they have proposes a novel position-based routing protocol for city scenario by considering both the buses and cars as vehicular nodes moving in both clockwise and anti-clockwise directions. Buses are the city buses running according to their predefined routes. As in previous researches, junctions are also called as 'anchors' here, where the decision is taken.also, consider the two scenarios when the network is sparse and when any node has left its initial position, and show that our proposed protocol performs better.

V. Valli Kumari in at al[6] they have proposes a technique which eliminates the risk of establishing the secure channels like using public key trees like .The main objectionable issue with is that it reveals the private key to other members which is totally against the principle of public key cryptography. The proposed technique not reveal any private keys. The storage requirements as well as work done by each member as part of re-keying and computational complexity are also been reduced further.

S. S. Dorle in at al[7]proposed evaluation of performance parameters for three routing protocols DSDV, AOMDV and AODV in VANET is carried out. matched with the expected output and are found satisfactorily. As expected, reactive routing protocol performance is the best considered because of its ability to maintain link by periodic exchange of information, which is required for TCP based traffic. AODV performs predictably. Virtually all packets delivered at low node mobility, and decreases the converge as node mobility increases and DSDV performs well but still requires the transmission of many routing overhead packets.

III. PROPOSED METHODOLOGY

The system replica and security necessities will be obtainable in this section. When security method is declare, we assume that there is a public key supervision method obtainable. The data transfer among each two vehicles is signed by the sender and the signature requirements to be established no issue which node received it. The VANETs System replica is immediately consisted of several wireless nodes set on vehicles. The vehicles are set to move through a crossroad for the meantime some of them do multi-hop wireless communications based on the protocol. show the structural design of the network, and the regular routing multi-hop path. When one vehicle requirements to send a message to a further far away it will get the position information of the target vehicle several way, such as during GPS or other position located devices. And then it is packaged jointly with the sending message, routed by the position-based protocol resourcefully to the destination. nodes send message by attractive benefit of the position information of added nodes and jointly with the security strategy to prefer which node is the subsequently hop. furthermore this replica tries best to fit the district of the real transportation system. The method can be abbreviation into two aspects: (1) Routing message protection mechanism; (2) Node evaluation mechanism. For the protection of the routing message, a signature verified scheme is employed to achieve end-to-end authentication and integrity of the data. And for the evaluation mechanism, every node is turned on hybrid surveillance mode and checks every packet send by its neighbor. The protocol estimate the reliability of neighbor nodes by checking its forwarding ratio (the ratio of packets forwarded to received). We perform the experiment 2.0 GHz Processor required (Pentium D and above) Minimum 2 GB RAM , 25 GB hard disk space

Operating System and Tool ,Ubuntu 12.04.1 Network simulator (NS-2): The Network simulator is created in C++ and Otcl program language. It can be used under UNIX and UNIX-like systems, as, Linux, Sun Solaris, Ubuntu 12.04.1. Also can be used in Windows platform (95/98/NT/XP). In our work we make tcl (tool command language) script and so we will simulate .

Experiment has been carried out for three different numbers of nodes under various cases and results are drawn and evaluated. The numbers of nodes used are:

I. 4 nodes
II. 10 nodes
III. 25 nodes

Results are compared for following cases:

CASE 1: Throughput of sending packets.

CASE 2: Throughput of receiving packets.

CASE 3: Throughput of dropping packets.

CASE 4: Packet Size vs Average throughput of sending packets.

CASE 5: Packet Size vs Average throughput of receiving packets.

CASE 6: Packet Size vs Average throughput of dropping packets.

CASE 7: Throughput of sending bits vs Average simulation End2End delay.

CASE 8: Throughput of receiving bits vs Average simulation End2End delay. Various parameters used for performance evaluation are: 1) Throughput: It is the amount of data per time unit that is delivered from one node to another via a communication link. The throughput is measured in Packets per unit TIL or bits per TIL. TIL is Time Interval Length. More is the throughput of sending

and receiving packets better is the performance. Lesser is the throughput of dropping packets better is the performance. 2) Average throughput: It is the average of total throughput. It is also measured in Packets per unit TIL or bits per TIL.

3) Packet Drop: It shows total number of data packets that could not reach destination successfully. The reason for packet drop may arise due to congestion, faulty hardware and queue

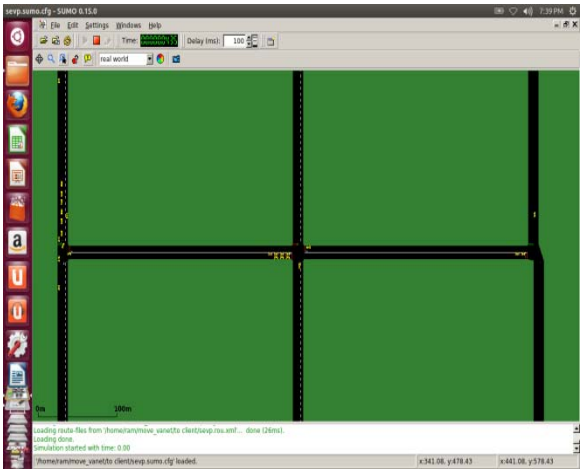

Figure: 1 Simulation

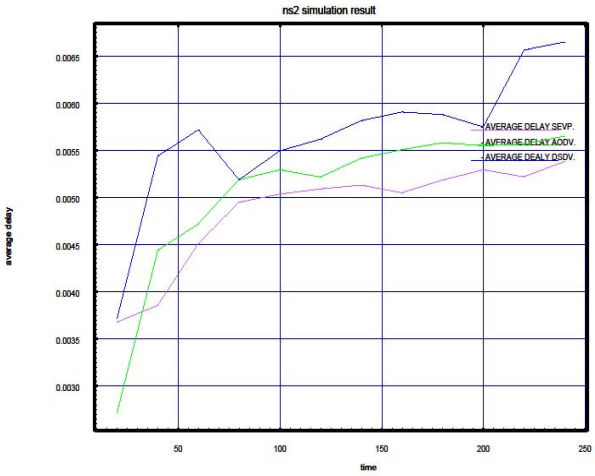

Figure 2:compare SEVP,AODV and DSDV from average deley

We compare our proposed SEVP and AODV ,DSDV overflow etc. Lower packet drop rate shows higher protocol performance. 4) Packet size: Size of packets in bytes. 5) Average simulation End to End delay (End2End delay): This metric gives the overall delay, from packet transmission by the application agent at the source node till packet reception by the application agent at the destination node. Lower delay shows higher protocol performance. The following equation is used to calculate the average end-to-end delay, Average End to End Delay = (T_DataR – T_DataS), Where T_DataR = Time data packets received at destination node T_DataS = Time data packets sent from source node. The end to end delay is important metrics because VANET needs a small latency to deliver quick messages. It shows the suitability of the protocol for the VANET. Simulation time: Total time taken for simulation. It is measured in seconds.

IV. CONCLUSIONS

VANET is an emerging and promising technology, this technology is a fertile region for attackers, who will try to challenge the network with their malicious attacks. This paper gave a wide analysis for the current challenges and solutions, and critics for these solution, we also proposed a new solutions that will help to maintain a securer VANET network, in the work we want to expand our idea about certificates of the safety messages, how to be created, discarded, and verified and test it by simulation.

REFERENCES

[1] Norbert Bißmeyer, Joël Njeukam, Jonathan Petit, Kpatcha M. Bayarou," Central Misbehavior Evaluation for VANETs based on Mobility Data Plausibility" VANET'12, June 25, 2012, Low Wood Bay, Lake District, UK. Copyright 2012 ACM 978-1-4503-1317-9/12/06.

[2] Vivek Pathak , Danfeng Yao , Liviu Iftode "Securing Location Aware Services Over VANET Using Geographical Secure Path Routing" Vehicular Electronics and Safety, 2008. IEEE International Conference on ICVES 2008.

[3] Miguel Garcia de la Fuente, Houda Labiod," Performance Analysis ofPosition-Based Routing Approaches in VANETS" Mobile Wireless Communications Networks, 2007 9th IFIP International Conference on- 19-21 Sept. 2007.

[4] Ghassan Samara, Wafaa A.H. A-Salihy, R. Sures," Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on- 11-13 May 2010.

[5] Huma Ghafoor, N. D. Gohar, Rizwan Bulbul" Anchor-based Connectivity Aware Routing in VANETs" 978-1-61284-683-5/12/-2012 IEEE.

[6] V. Valli Kumari D.V.NagaRaju K.Soumya1 KVSVN Raju," Secure Group key Distribution Using Hybrid Cryptosystem" Second International Conference on Machine Learning and Computing-2010.

[7] S. S. Dorle Bhushan Vidhale, Megha Chakole ," Evaluation of Multipath, Unipath and Hybrid Routing Protocols for Vehicular Ad Hoc Networks" Fourth International Conference on Emerging Trends in Engineering & Technology IEEE-2011.

[8] W Ren, K Ren, W Lou, Y Zhang,"Efficient user revocation for privacy-aware PKI", - Proceedings of the 5th International ICST Conference, 2008.

[9] P Papadimitratos, L Buttyan, JP Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Private Vehicular Communications", 7th International Conference on ITS, 2007.

[10] R Lu, X Lin, H Zhu, PH Ho, X Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular", In proceeding The 27th Conference on Computer Communications, INFOCOM 2008.

[11] X Lin, R Lu, C Zhang, H Zhu, PH Ho, "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, April 2008.

[12] J J Haas, Y C Hu, K P. Laberteaux," Design and analysis of a lightweight certificate revocation mechanism for VANET", Proceedings of the sixth ACM international workshop on Vehicular Internetworking , 2009.