ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

A Secure Routing Protocol for Vehicular Ad Hoc Network: A Survey

Mukesh Tripathi[1], Sandeep Rai[2]

M.Tech Scholar, Computer Science and Engineering[1]

Assistant Professor, Computer Science and Engineering[2]

Technocrats Institute of Technology (Excellence), Bhopal, India[1,2]

Abstract: A vehicular Ad Hoc Network specially appointed system (VANET) utilizes as portable hubs in a MANET to make a versatile network. A VANET transforms each partaking nodes into a remote switch or hub, permitting nodes roughly 100 to 300 meters of one another to join and, thusly, make a system with a wide range. The requirement for vigorous VANET systems is firmly reliant on their security and protection characteristics, which will be examined in this paper. In this paper a different sorts of security issues furthermore difficulties of VANET been broke down and examined; we likewise examine a set of arrangements displayed to take care of these difficulties and issues. It turns into a key part of the adroit transport framework. A great deal of works has been carried out towards it yet security in VANET got less consideration. In this article, we have examined about the VANET and its specialized and security challenges.

Keywords: VANET, MANET, Security, ITS.

1. Introduction

Intelligent Transportation Systems (ITS) are very circulated, and relying upon some metadata trading,offering, and following components. To adapt to this, some studies [1-3] have demonstrated to that industry standards to give decentralized benefits on dynamic system. What's more, administrations on an incorporated server by means of unique foundations have additionally been specified in [4]. Notwithstanding, these frameworks are not ready to give a nonstop administration conveying on a portable hub.

Ways in a VANET can regularly disengage because of hub developments and the system topology may be sporadic because of man-made bases and impediments. The hub thickness in a VANET can have an extensive variety of range contingent upon street movement conditions on diverse allotments of street fragments. Besides, on the grounds that the system may be extensive with a few a great many hubs, established specially appointed steering conventions which regularly create loads of overhead parcels just can't scale. In any case, a VANET has gainful qualities that may be exploited. The hubs in a VANET have unsurprising versatility designs in that hub developments are limited in street portions, and have a tendency to correspond with adjacent vehicles [5]. All these Protocols make utilization of, a solitary course and don't use numerous exchange courses and ways. Multipath steering permits the foundation of numerous ways between a solitary source and single end hub and when a way breaks an exchange way is utilized as opposed to launching another course disclosure, subsequently multipath steering speaks to a guaranteeing steering technique for remote versatile impromptu systems[6].

So the first aim is to take the advantage of multipath way to the represented nodes. Then the security concern must be considered [7].

This paper study and discuss the plan for dependable information conveyance in Vanets considering the versatility of the vehicles as a real concern. Proposed plan distinguishes the sending zone and expected zone. The vehicles with greatest pace for convey the information parcel in the sending zone, with a desire of minimizing the deferral. Later in the normal zone of the terminus vehicle the information bundles are telecasted until they achieve the terminus vehicle. Sending zone and expected zones are circles, the span for forwarding circle is the separation in the middle of source and terminus vehicle computed utilizing the Euclidean separation. The sweep of the normal zone circle is twice of the sending zone circle [8].

VANET security [9][10][12][13][14][15][16] is the primary issue these days to handle on the grounds that numerous noxious drivers are going into the system to make disturbances and decrease the system execution. In this paper, PBSRP directing convention is intended to discover an effective directing way and transfer the information by scrambling it with the Session Key (SK) [11]to keep the information from getting caught by an interloper. PBSRP is a mixture directing convention which incorporate the ideas of MFR [17] and B-MFR [17] to discover the ideal hub to hand-off the information. In the wake of discovering the ideal hub the principle thing is to check whether the hub is real or not, for that station to station key administration convention is utilized which does not utilizes an outsider for checking the hubs validity yet it utilizes the testaments for the vehicles to check whether the hub is a veritable.

2. Supporting Work

In 2011, Abhijit Das et al. [18] propose to utilize imparted cryptography to secure message correspondence in adhoc system. In this methodology we separate any data into various imparts and transmit the distinctive shares by means of numerous disjoint ways between any pair of

DOI 10.17148/IJARCCE.2015.4521

imparting hubs and if conceivable at diverse purpose of time. At the less than desirable end the first data is recreated by joining the shares got through distinctive ways at diverse purpose of time. We have additionally proposed to keep repetition in the quantity of shares to withstand loss of a few imparts because of misfortune in transmission or security assaults.

In 2011, Farzad Sabahi et al. [19] propose that Vehicular Adhoc system (VANET) is another formof Mobile Adhoc Network (MANET). It coordinates versatile integration conventions to speed up information exchange between vehicles and in addition between roadside gear and accessible activity in system. In VANET, Wireless gadget sends data to adjacent vehicles, and messages can be transmit starting with one vehicle then onto the next vehicle. Hence, utilizing VANET can expand security and movement improvement. Like other innovation, in VANET there are some essential and discernible issues. A standout amongst the most vital of them is Security. Since the system is open and available from all over the place in the VANET radio reach, it is relied upon to be a simple focus for vindictive clients. They watch the security issues as a standout amongst the most essential issues in Vehicular Adhoc system.

In 2011, Irshad Ahmed Sumra et al. [20] present the Vehicular specially appointed system (VANET) Security R&d Ecosystem is talked about. The R&d Ecosystem can be separated into four noteworthy perspectives i.e. scholastic exploration, auto producers, government powers, and end clients.

In 2012, G.gowtham et al. [21] recommend that avanet is an adhoc organize that uses moving autos as hubs in a system to make a portable system. VANET permits autos more or less 100 to 300 meters of one another to interface and thus make a system with a wide range. As autos drops out of the sign range and goes out of the system and different autos takes after the same system and now versatile system is made. Here the correspondence between the hubs happens in a secured manner by utilizing security calculations like TESLA and Ecdsa.vanet utilizes an equipment called Tpm(trusted stage module) to give a secured correspondence between the hubs. For a secured correspondence between the hubs, a hub must trust the speaking hub before correspondence with it and in the event that it is discovered legitimate then speak with it. While trusting, if that hub is discovered to be malignant one, maintain a strategic distance from correspondence with it. In their proposed work, as opposed to keeping up long records of hub points of interest in focal trusted power, utilizing watchword generator produce a secret word and guardian hub will appropriate them to the kid hubs.

In 2012, Ganesh S. Khekare et al. [22] propose that the unlimited advancement in the remote advances developed another kind of systems, for example, Vehicular Ad Hoc Networks (Vanets), which gives correspondence between vehicles themselves and in the middle of vehicles and base. Different new ideas, for example, brilliant urban communities and living labs are presented in the late years where Vehicular Ad Hoc Networks (Vanets) plays an imperative part. An audit of different Intelligent Traffic Systems (ITS) accessible and different steering conventions regarding our proposed plan is carried out in this paper. They presents another plan comprise of a savvy city system that transmit data about activity conditions that will help the driver to take fitting choices. Their proposed plan comprise of a cautioning message module made out of Intelligent Traffic Lights (Itls) which gives data to the driver about ebb and flow activity conditions.

In 2012, Khyati Choure et al. [23] propose that in the present situation, in impromptu system, the conduct of hubs is not extremely steady. They don't work legitimately and palatable. They are not helpful and acting egotistically. They demonstrate their childishness to impart their assets like transmission capacity to spare life of battery; they are not delay to square the parcels sent by others for sending and transmit their own particular bundles. Because of higher Mobility of the diverse hubs makes the circumstances much more muddled. Different steering conventions particularly for these conditions have been produced amid the last few years, to discover advanced courses from a source to some end. At the same time it is still hard to know the real briefest way without assailants or terrible hubs. Specially appointed system experience the ill effects of the part of issues i.e. blockage, Throughput, delay, security, organize overhead. Parcel conveyance degree is the issues of continuous examination. Reason for hub disappointment may be either common disappointment of hub connections or it might be because of demonstration of an aggressor or terrible hub which may corrupt execution of system gradually or radically, which additionally need to recognize or decided. In this paper, they distinguish the great and awful hubs. A reproduction has been performed to attain to better execution of changed AODV. Great result has been acquired as far as Throughout, Packet Delivery Ratio.

In 2012, Ranbir Sinha et al. [24] present an idea of improving the security in remote correspondence. A Computer Network is an interconnected gathering of self-governing processing hubs, which utilize a decently characterized, commonly concurred set of standards and traditions known as conventions, connect with each other seriously and permit asset offering ideally in an anticipated and controllable way. Correspondence has a real effect on today's business. It is fancied to correspond information with high security. Nowadays remote correspondence has turned into a crucial manifestation of correspondence in all parts of everyday life. The primary purpose behind this notoriety besides everything else like the rate of correspondence and minimal effort is the comfort of overseeing and taking care of information exchange. However this correspondence is decreased by the unreliability of communication.

DOI 10.17148/IJARCCE.2015.4521

In 2013, Bhoi et al. [25] presents another Position Based Secure Routing Protocol (PBSRP) which is a mixture of Most Forward inside Radius (MFR) and Border Node based Most Forward inside Radius (B-MFR) steering conventions. A security module is included this convention by utilizing station to station key understanding convention to keep the framework from different assaults. It comprises of three stages: instatement stage, ideal hub choice stage and secure information conveyance stage. Reproduction results shows PBSRP shows preferable results over MFR and B-MFR in terms of end to end postponement and parcel conveyance proportion when vindictive drivers are incorporated in the system.

In 2013, Li et al. [26] proposes a data scattering plan for urban VANET with high vehicle thickness and different hotspots. They acquire legitimate steering and additionally to spare the system assets the extent that this would be possible by presenting the idea of the Steiner tree issue. Reenactments are led with NS-2.35 and MOVE. The recreation results demonstrate that our plan performs better than RTDF plot in the execution of bundle conveyance delay.

In 2013,Liya et al. [27] investigate the problem ofoptimal road side units (RSUs) placement in Vehicular AdHoc Network (VANET) on a highway, which enables theVANET maintain a good connectivity. Their goal is to find outminimal number of road side units, such that the vehicles couldcommunicate with RSUs. These road side units are connectedby wire. They develop a randomized algorithm to deploy roadside units in the VANET. It gives an approximation to theoptimal distance to guarantee the information can be passedto RSUs from the accident site via the VANET. Simulations areconducted to show the performance of our proposed method.

In 2013,Meng et al. [28] proposes an adaptive strategy basedon the combination of these two situation and then apply this strategyto Location-Aided Routing (LAR) protocol to keep the routingperformance from degradation. In the adaptive strategy they usethe Multiple Attribute Decision Making (MADM) to establish thecontrol function which can accommodate message transmission tothe circumstances dynamically. Theoretical analysis and simulationperformance prove that this strategy can improve the packetdelivery ratio (PDR) of LAR protocol effectively.

In 2014, Correa et al. [29] work endeavors are concentrated, essentially, to analyze working settings in conventions like AID, DBRS, and ADDHV for scattering messages. A benchmarking investigates procedures that address difficulties, for example, system parceling and the telecast storm issue, which embrace the scattering. The aftereffects of a set of measurements got in diverse vehicular movement plans finish the exchange held. Contemplations for answers in scope, postponement, rate of conveyance, telecast, and bundle misfortune help this activity and inspire the advancement of a versatile answer for variances in transporter thickness.

3. PROBLEM DOMAIN

In the wake of mulling over a few examination papers we watch the need of security in both the beneficiary and sender side. In [30] propose another distributed computing environment where they approach a trusted cloud environment which is controlled by both the customer and the cloud environment administrator. Their methodology is essentially separated into two sections. Initially part is controlled by the typical client which gets authorization by the cloud environment for performing operation and for stacking information. Second part demonstrates a protected trusted figuring for the cloud, if the administrator of the cloud need to peruse and upgrade the information then it takes consent from the customer environment. This gives an approach to shroud the information and ordinary client and can ensure their information from the cloud supplier. This gives a two way security convention which helps both the cloud and the typical client. From which they can receive two way securities. This idea is likewise stretched out in [31].

We expect to further assess the adequacy with increment in the quantity of reproduction runs utilizing distinctive genuine world movement situations and increment in number of hubs. We will likewise consider the impact of encryption and unscrambling of the verifiers begins time and perceives how it would influence the execution of the calculation. We will further break down the impact of distinctive variables included like pace, number of vehicles, removes between the hubs and diverse activity practices. This suggestion is taken from [32].
We can consider the encryption technique as per the discussion shown in [33].

Table1: Execution Time (Milliseconds) of Encryption of Different data packet size [33]

Input Size(KB)	3 DES	DES	RSA
45	50	25	55
55	44	29	46
96	76	45	89
236	113	39	119
319	155	89	157
560	171	131	169
899	299	240	309
5345.28	1166	1296	1441
Throughput (MB/Sec.)	2.08	3.01	1.67

Table2: Execution Time (Milliseconds) of encryption of Different data packet size [33]

Input Size	3 DES	DES	RSA
45	49	34	61
55	47	22	59
96	63	53	57
236	67	62	64
319	85	98	154
560	161	125	163
899	171	152	183
5345.28	835	783	827
Throughput	4.03	5.012	2.147

Table3: Comparison [33]

Features	DES	RSA	DES + Random Password
Key	Same key is used for encryption and decryption Purpose.	Different keys are used for encryption and decryption Purpose.	Same key is used for encryption and decryption Purpose. But it is random at all-time even the file is same in the next process.
Scalability	It is scalable algorithm due to varying the key size and block size.	No scalability occurs.	It is scalable algorithm due to varying the key size and block size.
Avalanche Effect	No more effected	More effected	No more Effected due to DES nature.
Power Consumption	Low	High	Low due to DES nature.
Confidentiality	High	Low	High due to DES nature

Based on [33] DES is better but we can use RC5 and RC6 algorithm for higher security or the combination or rivest cipher as suggested in [34],[35][36] and [37].

4. Analysis

After studying several research papers we can concentrate on the following security issues:

Authentication

The real concern in VANET security is verification as it guarantee sending of messages by the genuine hubs and Thus Reduces Considerably the assaults by the advisories and some other undesirable hub ,notwithstanding, confirmation likewise includes protection concern since connecting the character of the sender with the message may permit following of vehicles by undesirable components. Along these lines it is essential that a message sent has a certain property which gives verification according to application.

Message Integrity

Message uprightness implies that the message imparted is in its unique and unaltered structure. As per the study in[8] message honesty guarantee that there is no adjustment in a message this can be accomplished through suitable means, for example, expansion of any bit with the message to distinguish any change in the first message.

Message Non-Repudiation

This implies that it can be created who has sent the message and the sender cannot deny having sent the message it may not be functional for individual beneficiaries who distinguish the hub from which a message has been sent thus there must be a specific power or focal executive to recognize the sending hub from a validated message.

Entity authentication

The entity validation guarantees that the sender of a message has not left the system at the time of the receipt thereof, that is, the message has been sent just a short while back.

Access control

Access control means guaranteeing that all hubs capacities as per the parts of benefits with which they have been approved in the system. For access control the approval needs to detail what is not can do in the system and what messages can be produced by it.

5. CONCLUSION

Vehicular Ad Hoc Networks is promising technology, which gives abundant chances for attackers, who will try to challenge the network with their malicious attacks.This paper gave a wide examination for the current difficulties and arrangements, and commentators for these arrangements, in our future work we will propose new arrangements that will help to keep up a securer VANET system, and test it by recreation. So all the above security necessities we can execute or any of them.so that we can get the immaculate information as well as recognize the malevolent Attacker. Identifying false position data and decreasing the shots of assaults are the keys to achievement in securing VANETS.

References

[1] S. Noguchi, M. Tsukada, T. Ernst, A. Inomata, and K. Fujikawa, "Location-aware Service Discovery on IPv6 GeoNetworking for VANET," in Proceedings of the 11th International ITS Telecommunications (ITST), pp. 224-229, Aug. 2011.

[2] Z. Ou, M. Song, H. Chen, and J. Song, "Layered Peer-to-Peer Architecture for Mobile Web Services via Converged Cellular and Ad Hoc Networks," in Proceedings of the 3rd International Conference on Grid and Pervasive Computing Workshops, pp. 195 – 200, May 2008.

[3] A. Rowstron and P. Druschel, "Pastry: Scalable, Decentralized Object Location, and Routing for Large-scale Peer-to-Peer Systems," in Proceedings of the 2001
IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg, pp. 329-350, Nov. 2001.

[4] T. Fujii, K. Yamori, and Y. Tanaka, "Ad hoc Network Service with Relay Reward and Its Routing Performance," in Proceedings of the 2010 8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT), pp. 1-6, Jun. 2010.

[5] Wongdeethai, Singha, and Peerapon Siripongwutikorn. "Multipath query spreading over vehicular ad-hoc networks." In Computer Science and Engineering Conference (ICSEC), 2013 International, pp. 255-260. IEEE, 2013.

[6] K.V.Kulhalli, Prajakta Rane, “On Demand Multipath Routing Algorithm for Adhoc Wireless Networks ", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-14, March-2014, pp.357-363.

[7] Aruna Rao S.L, K.V.N.Sunitha, “Secure Geographical routing in MANET using the Adaptive Position Update ", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-16, September-2014, pp.785-794.

[8] Kambalimath, Mahantesh G., S. K. Mahabaleshwar, and S. S. Manvi. "Reliable Data Delivery in Vehicular Ad Hoc Networks." In Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on, pp. 316-322. IEEE, 2013.

[9] T. Leinmuller, E. Schoch, and C. Maihofer, “Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks,” IEEE 4th Annual Conference on Wireless on Demand Network Systems and Services, pp. 84-91, 2007.

[10] H. Hartenstein, and K. P. Laberteaux, “A Tutorial Survey on Vehicular Ad Hoc Networks,” IEEE Communications Magazine, pp. 164-171, Jun 2008.

[11] C. Langley, R. Lucas, and H. Fu, “Key Management in Vehicular Ad-Hoc Networks,” IEEE International Conference on Electro/Information Technology, pp.223-226, 18-20 May 2008.

[12] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Strengthening Privacy Protection in VANETs,” IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, pp. 508-513, 2008.

[13] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, “Security and Privacy Issues for Inter-vehicle Communications in VANETs,” IEEE Sensor, Mesh and Ad Hoc Communications and Networks Workshops, pp. 1-3, 2009.

[14] F. Schaub, Z. Ma, and F. Kargl, “Privacy Requirements in Vehicular Communication Systems,” IEEE International Conference on Computational Science and Engineering, pp. 139-145, 2009.

[15] F. Sabahi, “The Security of Vehicular Adhoc Networks,” IEEE Third International Conference on Computational Intelligence, Communication Systems and Networks, pp. 338-342, 2011.

[16] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, “[.

[17] R.S. Raw, and D.K. Lobiyal, “B-MFR routing protocol for vehicular ad hoc networks,” Networking and Information Technology (ICNIT), 2010 International Conference on, pp.420-423, 11-12 June 2010.

[18] Abhijit Das Soumya Sankar Basu Atal Chaudhuri, “A Novel Security Scheme for Wireless Adhoc Network”,IEEE 2011.

[19] Farzad Sabahi, “The Security of Vehicular Adhoc Networks”, 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks.

[20] Irshad Ahmed Sumra, Halabi Hasbullah and Jamalul-lail Ab Manan, “VANET Security Research and Development Ecosystem”,IEEE 2011.

[21] G.Gowtham, E.Samlinson, “A Secured Trust Creation In V Anet Environment Using Random Password Generator”,International Conference on Computing, Electronics and Electrical Technologies [ICCEET],2012.

[22] Ganesh S. Khekare, Apeksha V. Sakhare, “Intelligent Traffic System for VANET: A Survey”, International Journal of Advanced Computer Research (IJACR), Volume-2, Number-4, Issue-6, December-2012.

[23] Khyati Choure, Sanjay Sharma, “Identification of node behavior for Mobile Ad-hoc Network”, International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4, Issue-6, December-2012.

[24] Ranbir Sinha, Nishant Behar, Devendra Singh,” Secure Handshake in Wi-Fi Connection (A Secure and Enhanced Communication Protocol)”, International Journal of Advanced Computer Research (IJACR) Volume 2, Number 1, March 2012.

[25] Bhoi, Sourav Kumar, and Pabitra Mohan Khilar. "A secure routing protocol for vehicular Ad Hoc network to provide ITS services." In Communications and Signal Processing (ICCSP), 2013 International Conference on, pp. 1170-1174. IEEE, 2013.

[26] Li, Y., J. Yang, and S. L. Wu. "A Steiner tree based information dissemination for urban vehicular Ad Hoc networks." In Computational Problem-solving (ICCP), 2013 International Conference on, pp. 113-117. IEEE, 2013.

[27] Liya, Xu, Huang Chuanhe, Li Peng, and Zhu Junyu. "A Randomized Algorithm for Roadside Units Placement in Vehicular Ad Hoc Network." In Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on, pp. 193-197. IEEE, 2013.

[28] Meng, Jia, Hao Wu, Hengliang Tang, and Xingyu Qian. "An Adaptive Strategy for Location-Aided Routing Protocol in Vehicular Ad Hoc Networks." In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on, pp. 405-410. IEEE, 2013.

[29] Correa, Claudio, Jo Ueyama, Rodolfo Ipolito Meneguette, and Leandro Aparecido Villas. "VANets: An Exploratory Evaluation in Vehicular Ad Hoc Network for Urban Environment." In Network Computing and Applications (NCA), 2014 IEEE 13th International Symposium on, pp. 45-49. IEEE, 2014.

[30] Ashutosh Kumar Dubey, Animesh Kumar Dubey Mayank Namdev, Shiv Shakti Shrivastava ,”Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment”,Conseg 2012, Published by IEEE.

[31] Rajendra Kumar Patel,” Secure and Cost Effective Framework for Cloud Computing Based On optimization and Virtualization”, International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4 Issue-6 December-2012.

[32] Penna, Kiran, Venkatesh Yalavarthi, Huirong Fu, and Ye Zhu. "Evaluation of active position detection in Vehicular Ad Hoc Networks." In Neural Networks (IJCNN), 2014 International Joint Conference on, pp. 2234-2239. IEEE, 2014.

[33] Kumar, Aman, S. Jakhar, and S. Kakkar. "Comparative Anal ysis between DES and RS A Algorithm‟ s." International Journal of Advanced Research in Computer Science and Software Engineering 2, no. 7 (2012): 386-391.

[34] Bhavesh Joshi and Anil Khandelwal, " Rivest Cipher based Data Encryption and Clustering in Wireless Communication " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-2, January-2015 ,pp.17-24.

[35] Priyanka Tavse, Anil Khandelwal, " A Critical Review on Data Clustering in Wireless Network " , International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-16, September-2014 ,pp.795-798.

[36] Priyanka Tavse and Anil Khandelwal , " An Efficient K-means Clustering approach in Wireless Network for data sharing " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-2, Issue-2, January-2015 ,pp.9-16.

[37] Bhavesh Joshi, Anil Khandelwal, " Clustering with Data Encryption in Wireless Communication: A Critical Survey “, International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-16, September-2014, pp.813-818.