International Journal of Advanced Technology and Engineering Exploration
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
Volume-2 Issue-4 March-2015

Identifying Malicious Behavior in MANET: A Survey

Prakash Deshmukh[1*], Yogesh Rai[2] and Santosh Kushwaha[3]
M.Tech Student, Computer Science, SIST (Shree), Bhopal[1]
Assistant Professor, Computer Science, SIST (Shree), Bhopal[2]
HOD, Computer Science, SIST (Shree), Bhopal[3]

Abstract

A mobile ad hoc network (MANET) is auto configurable network of devices without any wires. The device in this environment is free to move randomly in any direction. These types of network are sometimes self-controlled or controlled by any internet area. The ease of use and freedom to relocate make this platform a wider use in the current network population. The data receiving and sharing in this environment is making this environment more friendly to use and adapt. But adapting the security mechanism is of greater concern. So our paper main aim is to identify the attack which will be generated in the meantime of data sharing and gathering. For this purpose this study has been done and analysis has been presented.

Keywords

MANET, Security, Attack detection, Data sharing and gathering.

1. Introduction

Because of the advance communication system mobile ad hoc network (MANET) is a trending platform for the current research. This also removes the limitations of communication range [1]. This system model presupposes that middle hubs are ready to convey movement other than their own[2]. At the point when impromptu systems are sent in unfriendly situations (strategic systems), or comprise of hubs that fit in with different autonomous substances, a convention agreeable conduct can't be accepted. Unattended gadgets can get to be bargained and drop travel activity keeping in mind the end goal to debase the system execution [3]. Additionally, new clients might misconfigure their gadgets to reject sending activity keeping in mind the end goal to save vitality. This kind of conduct is normally termed node misconduct [4][5]. 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 concentrates on and talks about the arrangement for trustworthy data transport considering the adaptability of the vehicles as a genuine concern. Proposed arrangement recognizes the sending zone and expected zone. The vehicles with most noteworthy pace for pass on the data divide the sending zone, with a yearning of minimizing the deferral. Later in the typical zone of the end vehicle the data groups are broadcasted until they accomplish the end vehicle. Sending zone and expected zones are circles, the compass for sending circle is the partition amidst source and end vehicle figured using the Euclidean division. The range of the typical zone circle is twice of the sending zone circle [8].

MANET security [9][10][12][13][14][15][16] is the essential issue nowadays to handle in light of the fact that various poisonous drivers are going into the framework to make aggravations and diminishing the framework execution. In this paper, PBSRP coordinating tradition is expected to find a viable coordinating way and exchange the data by scrambling it with the Session Key (SK) [11]to keep the data from getting got by an intruder. PBSRP is a mixture coordinating tradition which consolidates the thoughts of MFR [17] and B-MFR [17] to find the perfect center to hand-off the data. In the wake of finding the perfect center the standard thing is to check whether the center is genuine or not, for that station to station key organization tradition is used which does not uses an untouchable for checking the center point's legitimacy yet it uses the confirmations

*Author for correspondence

for the vehicles to check whether the center point is a veritable.

This technique can be ruined by the attackers so that there will be a chance to adopt the security mechanism in the middle of the attack [18][19].

2. Literature Review

In 2011, Irshad Ahmed Sumra et al. [20] present the Vehicular extraordinarily designated framework Security R & D Ecosystem is discussed. The R&d Ecosystem can be divided into four significant viewpoints i.e. educational investigation, auto makers, government powers, and end customers.

In 2012, G.gowtham et al. [21] prescribe that avanet is an adhoc compose that uses moving automobiles as centers in a framework to make a versatile framework. VANET grants automobiles pretty much 100 to 300 meters of each other to interface and in this way make a framework with a wide range. As automobiles drops out of the sign range and goes out of the framework and distinctive cars takes after the same framework and now flexible framework is made. Here the correspondence between the center points happens in a secured way by using security computations like TESLA and Ecdsa. VANET uses a gear called trusted stage module to give a secured correspondence between the centers. For a secured correspondence between the centers, a center must trust the talking center before correspondence with it and in case it is found honest to goodness then talk with it. While trusting, if that center point is found to be dangerous one, keep up a vital separation from correspondence with it. In their proposed work, instead of keeping up long records of center point purposes of enthusiasm for central trusted force, using watchword generator deliver a mystery word and gatekeeper center will proper them to the child centers.

In 2012, Ganesh S. Khekare et al. [22] suggest that the boundless progression in the remote advances created an alternate sort of frameworks, for instance, Vehicular Ad Hoc Networks (Vanets), which gives correspondence between vehicles themselves and amidst vehicles and base. Distinctive new thoughts, for instance, splendid urban groups and living labs are displayed in the late years where Vanets has basic impact. A review of distinctive Intelligent Traffic Systems (ITS) open and diverse directing traditions in regards to our proposed arrangement is completed in this paper. They displays an alternate arrangement contain an insightful city framework that transmit information about movement conditions that will help the driver to take fitting decisions. Their proposed arrangement contain an advised message module made out of Intelligent Traffic Lights (Itls) which offers information to the driver about rhythmic movement action conditions.

In 2012, Khyati Choure et al. [23] suggest that in the current circumstance, in improvised framework, the behavior of center points is not amazingly relentless. They don't work honest to goodness and attractive. They are not useful and acting vainly. They show their silliness to confer their benefits like transmission ability to extra existence of battery; they are not postpone to square the packages sent by others for sending and transmit their own specific packs. On account of higher Mobility of the assorted centers makes the circumstances a great deal more jumbled. Distinctive directing traditions especially for these conditions have been created in the midst of the most recent few years, to find propelled courses from a source to some end. In the meantime it is still hard to know the genuine briefest path without aggressors or frightful center points. Extraordinarily delegated framework encounter the evil impacts of the piece of issues i.e. blockage, Throughput, delay, security, arrange overhead. Package movement degree is the issues of ceaseless examination. Purpose behind center point dissatisfaction may be either basic frustration of center associations or it may be a result of show of an attacker or awful center point which may degenerate execution of framework slowly or drastically, which furthermore need to perceive or chose. In this paper, they recognize the immense and horrendous centers. A propagation has been performed to accomplish better execution of changed AODV. Awesome result has been procured the extent that Throughout, Packet Delivery Ratio.

In 2012, Ranbir Sinha et al. [24] present a thought of enhancing the security in remote correspondence. A Computer Network is an interconnected assembling of administering toward oneself transforming centers, which use an adequately portrayed, generally agreed arrangement of models and conventions known as traditions, interface with one another genuinely and license resource offering in a perfect world in a foreseen and controllable way. Correspondence has a genuine impact on today's business. It is fancied to relate data with high security. These days remote correspondence has transformed into a significant

sign of correspondence in all parts of regular life. The basic role behind this reputation other than everything else like the rate of correspondence and insignificant exertion is the solace of directing and dealing with data trade. However this correspondence is diminished by the untrustworthiness of correspondence.

In 2013, Bhoi et al. [25] presents an alternate 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) directing traditions. A security module is incorporated this tradition by using station to station key comprehension tradition to keep the system from distinctive strikes. It contains three stages: instatement stage, perfect center point decision arrange and secure data transport stage. Proliferation results shows PBSRP shows ideal results over MFR and B-MFR as far as end to end delay and bundle movement extent when malignant drivers are consolidated in the framework.

In 2013, Li et al. [26] proposes an information scrambling arrangement for urban VANET with high vehicle thickness and diverse hotspots. They gain true blue controlling and also to extra the framework resources the degree that this eventual conceivable by introducing the thought of the Steiner tree issue. Reenactments are driven with NS-2.35 and MOVE. The amusement results show that our arrangement performs better than RTDF plot in the execution of pack movement delay.

In 2013, Liya et al. [27] explore the issue of ideal street side units (RSUs) situation in Vehicular Ad Hoc Network (VANET) on a thruway, which empowers the VANET keep up a decent integration. Their objective is to discover insignificant number of street side units, such that the vehicles could speak with RSUs. These street side units are associated by wire. They add to a randomized calculation to send street side units in the VANET. It gives a close estimation to the ideal separation to ensure the data can be gone to RSUs from the mischance site through the VANET. Recreations are directed to demonstrate the execution of our proposed technique.

In 2013, Meng et al. [28] proposes a versatile technique in view of the blend of these two circumstances and afterward apply this methodology to Location-Aided Routing (LAR) convention to keep the directing execution from debasement. In the versatile procedure they utilize the Multiple Attribute Decision Making (MADM) to build the control capacity which can suit message transmission to the circumstances progressively. Hypothetical examination and reproduction execution demonstrate that this method can enhance the bundle conveyance proportion (PDR) of LAR convention successfully.

In 2014, Correa et al. [29] work tries are concentrated, basically, to examine working settings in traditions like AID, DBRS, and ADDHV for dissipating messages. A benchmarking explores methodology that address challenges, for instance, framework distributing the broadcast storm issue, which grasp the diffusing. The eventual outcomes of an arrangement of estimations got in different vehicular development arrangements complete the trade held. Examinations for answers in degree, delay, rate of movement, broadcast, and pack mishap help this action and move the headway of an adaptable response for changes in transporter thickness.

In 2013, Amendola et al. [30] proposed a novel neighbor discovery protocol for resource constraint devices (RFID tags) running according to the delay tolerant networking paradigm. The proposed protocol is based on the traditional P-Persistent CSMA algorithm, but with the addition of the sift-distribution (siftPersistent) in order to reduce the collisions during the response phase. Their proposal has been tested both in a simulator and in a real testbed under the OpenBeacon framework.

In 2014, Chasaki et al. [31] proposed a novel algorithm to accomplish connectivity tracking based on a space-efficient Bloom filter data structure and the use of aggregate signatures. They present simulation results on a real network trace that show the effectiveness of their design.

3. Problem Domain

There are several works are already progress in this direction to make data sharing and gathering efficiently, prevent attacks and detect attacks. There are several papers also which suggest encryption techniques for better security so that there is less chance of attacks. The security majors are also provided in different area like in [32]. Our main motivation is to improve the detection capability. Some of the MANET security threats are following:

1) Channel vulnerability: It allows the message to be broadcast or to eavesdrop the message to different sources.
2) Node vulnerability: The nodes are free to move in the MANET so it is not protected in any surface or by any physical background. So the chances of attacks are very high.
3) Absence of infrastructure: The certifications and validations authorities and representations are missing.
4) Dynamic changing nature: The nodes behavior and positions are change at run time so any static method will not help to protect the privacy for the long time.
5) Computational limitations: Applying the encryption algorithm for the dynamic environment is not so easy.

4. Analysis

Our analysis based on the above study suggests the following direction [33]:

Authentication
Authentication in MANET ensures that the communication node is genuine or not. It is fundamental for the correspondence members to demonstrate their characters as what they have asserted utilizing a few systems in order to guarantee the genuineness. In the event that there is not such a validation component, the enemy could mimic a kind hub and therefore become acquainted with classified assets, or even engender some fake messages to bother the ordinary system operations.

Message Integrity
The received message should not be altered in the middle of the attack prior to the receiving. A message can be evacuated, replayed or overhauled by an enemy with noxious objective, which is viewed as malevolent modifying; in actuality, if the message is lost or its substance is changed because of some kind disappointments, which may be transmission mistakes in correspondence or equipment blunders, for example, hard plate disappointment, then it is ordered as unintentional adjusting.

Message Non-Repudiation
Nonrepudiation guarantees that the sender and the collector of a message can't deny that they have ever sent or gotten such a message. This is valuable particularly when we have to segregate if a hub with some strange conduct is traded off or not: if a node perceives that the message it has gotten is wrong, it can then utilize the off base message as a confirmation to tell different hubs that the hub conveying the ill-advised message ought to have been bargained.

Entity authentication
The validation of the entity should be checked that the node should not pretend as the authentic node.

Access control
Access control means guaranteeing that all nodes 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.

Anonymity
It implies that all the data that can be utilized to distinguish the manager or the current client of the hub ought to default be kept private and not be dispersed by the hub itself or the framework programming. This rule is nearly identified with security safeguarding, in which we ought to attempt to shield the security of the hubs from self-assertive revelation to some other elements.

Denial of Service attack (DoS)
It assault, an assailant endeavors to keep genuine clients from getting to data or administrations. A disavowal of administration (DoS) assault is an assault that stops up such a great amount of memory on the target framework that it can't serve its clients, or it causes the target framework to crash, reboot, on the other hand overall refuse any assistance to true blue clients. Nowadays, DoS assaults are extremely regular; for sure, pretty much every server is certain to experience such an assault sooner or later or an alternate. Refusal of Service can without much of a stretch be propelled and surge the system with spurious steering messages through a pernicious hub that gives inaccurate redesigning data by claiming to be a real change of directing data.

Sybil attack
On the off chance that a malignant hub mimics some nonexistent hubs, it will show up as a few vindictive hubs planning together, which is known as a Sybil assault. A Sybil assault is one in which an assailant subverts the notoriety arrangement of a distributed system by making an extensive number of pseudonymous substances, utilizing them to increase a lopsidedly extensive impact. A notoriety

framework's defenselessness to a Sybil assault relies on upon how affordably characters can be created, the extent to which the notoriety framework acknowledges inputs from substances that don't have a chain of trust connecting them to a trusted substance, and whether the notoriety framework treats all elements indistinguishably.

5. Conclusion and Future Suggestions

Our study and analysis on MANET security shows the vulnerability and the leaks in security. Although there is several research work is already in progress in this direction. But the research vacuum in data security and attack detection is still the area of future research. In our view a proper encryption decryption process not completely cure this problem. But making a standard detection technique will be a powerful tool in future to prevent this in the greater extent.

References

[1] Zhang, Y.; Lazos, L.; Kozma, W., "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks," Mobile Computing, IEEE Transactions on , vol.PP, no.99, pp.1,1.

[2] G. Acs, L. Buttyan, and L. Dora. Misbehaving router detection in link-state routing for wireless mesh networks. InProc. of WoWMoM, pages 1–6, 2010.

[3] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information System Security, 10(4):11–35, 2008.

[4] K. Balakrishnan, J. Deng, and P. K. Varshney. Twoack: Preventing selfishness in mobile ad hoc networks. InProc. of WCNC, 2005.

[5] S. Buchegger and J.-Y. L. Boudec. Self-policing mobile ad-hoc networks by reputation systems.IEEE Comm. Magazine, pages 101–107, 2005.

[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] Ma'en Saleh, Ahmad Aljaafreh and Naeem Al-Oudat , " Hierarchal Scheduling Algorithm for Congestion Traffi Control Using Multi-Agent Systems", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-17, December-2014 ,pp.915-921.

[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, "Overview of security issues in Vehicular Ad-hoc Networks", IGI Global, 2011.

[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] Namrata Shukla, " Data Mining based Result Analysis of Document Fraud Detection " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014 ,pp.21-25.

[19] Namrata Shukla, Shweta Pandey, " Document Fraud Detection with the help of Data Mining and Secure Substitution Method with Frequency Analysis " , International Journal of Advanced

Computer Research (IJACR), Volume-2, Issue-4, June-2012 ,pp.149-156.

[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] Amendola, Danilo, Floriano De Rango, Khalil Massri, and Andrea Vitaletti. "Neighbor discovery in delay tolerant networking using resource-constraint devices." In Wireless Days (WD), 2013 IFIP, pp. 1-3. IEEE, 2013.

[31] Chasaki, Danai. "Identifying malicious behavior in MANET through data path information." In Computing, Networking and Communications (ICNC), 2014 International Conference on, pp. 567-572. IEEE, 2014.

[32] 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.

[33] Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2008): 1-23.

Mr. Prakash Deshmukh is from Seoni and was born on 16th January 1990 in Seoni(M.P). He has done his Schooling from Mission boy's H. S. School, Seoni (M.P) and has completed his graduation from Shree institute of science and technology Bhopal with 69.06%. He is a PG Scholar at Shree institute of science and technology Bhopal, Under Rajiv Gandhi Proudhyogiki Vishwavidhyalaya, Bhopal (M.P) and pursuing M.Tech in computer science and technology and willing to Work on Identifying Malicious Behavior in MANET.
Email: Prakash.deshmukh661@gmail.com