Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
5(1), 2017, 07-14

ISSN 2347 – 7393

Survey Article

ATTACKS, SUSCEPTIBILITIES AND SECURITY SCHEMES IN MANET: A SURVEY

Bhagyshri Khorgade, Prof. Achint Chugh

Mittal Institute of Technology, Bhopal, India

Abstract: In Mobile ad hoc Network nodes area unit established association and deliver knowledge in dynamic surroundings. Security is that the one in the entire main drawback in Mobile ad hoc Network (MANET) because of unique characteristics of Manet, it creates variety of important challenges to its security style to beat the challenges, there's a need to build a security theme that achieves each in depth protection and fascinating network performance from attacks. In mobile ad hoc networks wherever the topology animatedly changes, straight methods can't be used efficiently. the various security schemes against attack area unit improves the network performance in presence of attacker to disable wrongful conduct activity. In this paper we tend to examine the behavior of various attacks result in network during this survey we tend to majorly highlight the behavior of various attacks with specific consistence of Flooding attack and defense schemes in Manet. The multipath routing schemes is additionally mentioned to improve the network performance in network however condition is that flooding condition area unit possible to occur by attacker. In presence of attacker security theme area unit continually provides the secure path then in multipath routing the possibility of secure routing is increased in presence of attacker and security theme.

Keywords: Security, Attack, Routing, MANET, Multipath

Introduction: All A mobile ad-hoc network is a self-organizing network that consists of mobile nodes that are capable of communicating with each other without the help of fixed infrastructure. On the contrary to traditional wired networks that use copper wire as a communication channel, ad-hoc networks use radio waves to transmit signals [1]. Two nodes will have multiple links between them for communication and deployed in an exceedingly complete fashion, appropriate for price and time effective setting, and for a scenario wherever infrastructure is troublesome to setup. Security is difficult in MANETs [2] attributable to its characteristics like peer to see design,

For Correspondence:
lucky.shree301@gmail.com.
Received on: November 2016
Accepted after revision: January 2017
Downloaded from: www.johronline.com

operational while not central arranger, dynamic topology, insecure operational setting, and frequent link breakage attributable to mobile nodes, battery period of time, machine capability and non-uniformity[3]. Communication in MANETs is thru single hop in link layer protocols and multi hop in network layer protocols, supported the belief that each one the nodes in an exceedingly network are cooperative in coordination method, however sadly this statement isn't true in hostile setting. Malicious attacks [2] will simply disrupt network operation by violating protocol specifications .The network layer operation in MANETs are supported routing and knowledge packet forwarding each are susceptible to malicious attacks.

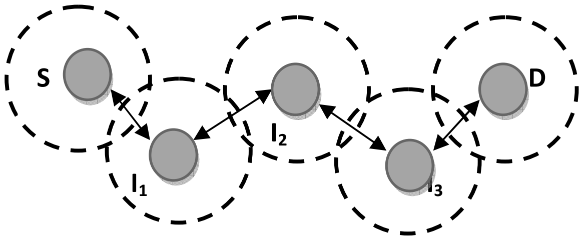

Fig 1 Ad Hoc Network

Mobile ad-hoc networks are inclined to a large number of security threats. The basic reality that mobile ad-hoc networks lack permanent infrastructure and use wireless link for interaction makes them very predisposed to an adversary's spiteful attacks. Attackers are severe security threats in ad-hoc networks which can be employed with no trouble by exploiting susceptibility of on-demand routing protocols such as AODV. This tries to use Intrusion Detection (ID) to prevent attacks imposed by both single and multiple nodes and the Detection and healing routing misbehaviour under MANET. we try to reach up to the specific solution maximizes network performance by the help of minimizing production of control (routing) packets as well as successfully opposing attacks against mobile ad-hoc networks [1].

MANET Susceptibilities: Susceptibility is a weakness in security system. A meticulous system may be susceptible to illegal data manipulation because the system does not verify a user's distinctiveness before allowing data access [2, 6]. MANET is more susceptible than wired network. Some of the susceptibilities are as follows:

Absence of centralized Authority: MANET doesn't have a centralized authority. The absence of centralized authority makes the detection of attacks difficult because it is not east to monitor the traffic in a vibrant and large scale MANET.

Lack of predefined Boundary: In MANET we cannot exactly identify a substantial boundary of the network. The nodes work in a itinerant environment where all nodes are free to join and leave the network at any instance of time. As soon as an opponent comes in the radio range of a node it will be able to communicate with that node.

Supportive in communication: The Routing protocol of MANETs usually assumes that mobile nodes are cooperative and reliable (not malicious). The routing misbehavior through malicious attacker can easily become disrupt network operation.

Limited power supply: The nodes in MANER are completely performing energy or power dependent operations need to consider restricted power supply, which will cause several problems. A node in MANET may behave in a selfish manner when it is finding that there is only limited power supply.

Opponent inside the Network: In MANET any new nodes can freely join and leave the network at any time instant. The suspected nodes within network may also behave maliciously. In dynamic network it is rigid to perceive that the behavior of the node is malicious attacker. Attack is harmful on that kind of network.

Routing Protocols in MANET: In dynamic network the topology is usually changes that are the reason behind link breakage. The direct connection in between sender and receiver isn't potential. The connections are created as multiple-hop until the destination isn't found. The routing protocol is enjoying a necessary role at network layer for knowledge exceptive and forwarding through every router or node. the info is causing by sender and accepted by receiver in that procedure routing strategy is extremely necessary a part of communication [4, 5]. For connecting to destination and knowledge delivery the routing protocol is important for routing the info in between sender to receiver. each routing protocol has completely different routing strategy of affiliation institution however has same technique of choose shortest path in between sender and receiver. The shortest path is decided on the premise of minimum hop count value in Manet. The classifications of routing protocols in painter area unit as follows:-

Proactive Routing Protocol: The proactive routing protocols are also called as table driven routing protocol and these routing protocols are maintaining the routing information of each node that are participating in routing procedure. In Mobile Ad hoc network the topology in network is changes by that the overhead of maintain the information of each and every node is very difficult and required large amount of memory for storing routing information in network. In ad hoc network if the nodes are moves at slow speed then that protocol is suppose to be better for communication. The example of proactive routing protocol is DSDV routing protocol.

Reactive Routing Protocol : The Reactive routing protocols are known as on demand routing protocol and these routing protocols are maintaining the routing info on the basis of demand of request receives by the neighbour. there's no routing info is keep of every node that are collaborating in routing procedure. In Mobile unexpected network the topology in network is changes by that the overhead of maintain the data of every and each node isn't required to maintained. In ad hoc network if the nodes are moves randomly speed then that protocol is supposes to be higher for communication. the instance of reactive routing protocol is AODV routing protocol.

Hybrid Routing Protocol: Since proactive and reactive protocols every work best in oppositely completely different eventualities, hybrid technique uses each. it's accustomed realize a balance between each protocols. Proactive operations are restricted to tiny domain, whereas, reactive protocols are used for locating nodes outside those domains.

Security Threats in MANETS: The current mobile ad-hoc networks offer many various kinds of attacks. Although the analogous exploits put together exits in wired networks but it's easy to repair by infrastructure in such a network. Current MANETs are primarily at risk of two differing types of attacks: active attacks and passive attacks. Active attack is attack once misbehaving node should bear those energy costs so on perform the threat [6]. On the other hand, passive attacks are within the main attributable to lack of cooperation with the aim of saving energy selfishly. Nodes that perform active attacks with the aim of damaging totally different nodes by inflicting network outage are thought-about as malicious whereas nodes that make passive attacks with the aim of saving battery life for his or own her communications are thought-about to be stingy [7]. Throughout this the attacks are classified as modification, impersonation, fabrication and lack of cooperation.

Types of attack in MANET: There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types [8]:

External attacks: In External attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

Internal attacks: In Internal attack the adversary wants to gain the normal access to the network and involve you in the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

In the two categories shown above, external attacks are similar to the normal attacks in the traditional wired networks in that the adversary is in the proximity but not a trusted node in the network, therefore, this type of attack can be prevented and detected by the security methods such as membership authentication or firewall, which are relatively conventional security solutions. However, due to the pervasive communication nature and open network media in the mobile ad hoc network, internal attacks are far more dangerous than the internal attacks: because the compromised nodes are originally the benign users of the ad hoc network, they can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services that should only be available to the authorized users in the network, and they can use the legal identity provided by the compromised nodes to conceal their malicious behaviors. Therefore, we should pay more attention to the internal attacks initiated by the malicious insiders when we consider the security issues in the mobile ad hoc networks. In the following, we discuss the main attack types that emerge in the mobile ad hoc networks.

Flooding Attack: Flooding attack [9] is a denial of service type of attack in which the malicious node broadcast the excessive false packet in the network to consume the available resources so that valid or legitimated user can not able to use the network resources for valid communication. Because of the limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network.

The flooding attack is possible in all most all the on demand routing, depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

1. RREQ flooding
2. DATA flooding

RREQ Flooding: In the RREQ flooding attack, the attacker broadcast the many RREQ packets per time interval to the IP address which does not exist in the network and disable the limited flooding feature. On demand routing protocols uses the route discovery process to obtain the route between the two nodes. In the route discovery the source node broadcast the RREQ packets in the network. Because the priority of the RREQ control packet is higher than data packet then at the high load also RREQ packet are transmitted. A malicious node exploits this feature of on demand routing to launch the RREQ flooding attack.

Flooding Attack or Data Flooding: In the data flooding, malicious node flood the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of bogus data packets. These useless data packet exhausts the network resources and hence legitimated user can not able to use the resources for valid communication.

The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack [8]. There are some attacks against routing that have been studied and well known [10]:

- ✓ Impersonating another node to spoof route message.
- ✓ Advertising a false route metric to misrepresent the topology.
- ✓ Sending a route message with wrong sequence number to suppress other legitimate route messages.
- ✓ Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages

Denial of Service (DoS) : The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. In the practice, the attackers exactly use the radio flooding and battery exhaustion methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities.

Impersonation: Impersonation attack is a severe threat to the security of mobile ad hoc network [11]. As we can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

Previous Work Done in Field of Attack

Let's look out various researches already done by various researchers.

In this scheme [12], the first criterion that has been checked is the authenticity of a new node that wants to join the network. The authors proposed a secure algorithm based on cryptography. After authenticating it, if the node is approved to be reliable, then it is authorized to some of the network related jobs. In spite of granting full authorization, we move on to the second phase of detection if the newly joined node is found to be malicious. For this, we send an entire data set divided into some smaller parts. The node is able to construct an entire data getting minimum number of those data parts if it is non-malicious. If not, the same process is repeated again with an increase in the minimum number data sets to construct the original data. Post this phase; in case the node is detected to be malicious, then it is eliminated from the network.

In this study [13] examined multipath routing protocols that will react to communication disturbance on-demand. In particular, a source node selects multiple different paths for reaching the destination in advance. The availability histories of paths are efficiently recorded and calculated via "availability history vectors". Leveraging AHVs, we have presented two AHV-based multipath selection algorithms: one selects multiple paths with the full knowledge of AHVs in the network, and the other computes the path in a distributed manner. AHV-based algorithms can effectively identify multiple paths that provide high end-to-end availability, even in the presence of a new jammer that did not affect the network before path selection. Additionally, the proposed distributed AHV-based algorithm accomplishes higher availability than AODV at a smaller communication cost for long-lived communication sessions

In this paper [14] we proposed a hierarchical dynamic trust management protocol for cluster-based wireless sensor networks, considering two aspects of trustworthiness, namely, social trust and QoS trust. We developed a probability model utilizing stochastic Petri nets techniques to analyze the protocol performance, and validated subjective trust against objective trust obtained based on ground truth node status. We demonstrated the feasibility of dynamic hierarchical trust management and application-level trust optimization design concepts with trust based geographic routing and trust-based IDS applications, by identifying the best way to form trust as well as use trust out of individual social and QoS trust properties at runtime to optimize application performance. Here trust-based IDS algorithm outperforms traditional anomaly-based IDS techniques in the detection probability while maintaining sufficiently low false positives.

The authors [15], discuss the different types of security attacks that can be launched easily in MANETs and related solutions needed for ensuring network security. This paper implements the secure ad hoc on-demand distance vector routing protocol (SAODV) and compares the performance of protocol with existing AODV protocol in the presence of black hole attack. Since public key cryptography is used in this scheme, it takes significant amount of time to compute digital signature at each node. Also, this leads to high overhead and processing power requirements.

In this paper author proposed FACES (Friend-Based Ad-hoc routing using Challenges to Establish Security) [16], that provides a list of trusted nodes to the source node by sending challenges and sharing friend lists. Based on the extent of successful data transmission and the friendship with other nodes in a network, the nodes in the friend lists are rated. The trust level of each node varies from -1 to 4. The nodes in the network are placed in one of the three lists, i.e. question Mark list, friend list and unauthenticated list. The periodic flooding of challenge packet and sharing of friend lists increases the control overhead.

In this paper [17] author proposed per-IP traffic behavioral analysis, in this they present a real-time DDoS attack detection and prevention system which can be deployed at the leaf router to monitor and detect DDoS attacks. The advantages of this system lie in its statelessness and low computation overhead, which makes the system itself immune to flooding attacks. Based on the synchronization of TCP and UDP protocol behavior, this system periodically samples every single IP user's sending and receiving traffic and judges whether its traffic behavior meets the synchronization or not. A new nonparametric CUSUM algorithm is applied to detect SYN flooding attacks. Moreover, this system can recognize attackers, victims and normal users, and filter or forward IP packets by means of a quick identification technique. It has three advantages shown as follows.

Based on per-IP traffic behavior analyses, it is easier to differentiate the attackers from the normal users.

Because our approach needs less computation and memory, the system could be deployed for on-line DDoS detection and prevention.

By applying the non-parameter CUSUM algorithm and decision algorithm, this system can detect attacks accurately at the earlier attack stage.

Moreover, this system can quickly filter the attack traffics and forward the normal traffics simultaneously by means of the fast identification technology.

In this [18] research, rejection of Service attack is applied in the network, evidences are collected to design intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to find out the accuracy of detection engine by using support vector machine. Universal Detection Engine will generate the friend list according to trust level, higher the trust level of the node may be used for other different processes similar to routing, and deciding the cluster head for scalable ad-hoc networks. Aspect takes out for Routing parameters and MANET Traffic generation parameters can be used for different routing protocols.

Expected Work against Flooding Attack

Flooding of link between the nodes may cause severe damage, even fails whole of the network. In proposed work we create a new protection scheme against misbehaviour of nodes. In this scheme first analyze the routing behaviour of malicious nodes against the behaviour of flooding attack then apply the proper well planned security scheme on it that block the whole misbehaviour of malicious nodes and enhance the network performance. The steps of identify flooding attack are:-

1. Calculate the number of paths established through multipath routing protocols.
2. Check the proper packet delivery in each link that has deliver data to destination.

We will propose a new robust rate adaptation scheme that is resilient to flooding attack in a wireless multi-hop tactical network. It improves the wireless link utilization by detecting the flooding attack and adapting the data delivery in dynamic network.

Conclusion & Future Work

In Mobile Ad hoc Network security is one of the major concerns in case of routing. The secure data communication is necessary for deliver the actual information in right way to receiver. The different types of attack and behavior are observe in this synopsis and also discuss the some scheme against different attack but the flooding attack security schemes are mainly focus on this research. In this study, we used the AOMDV routing protocol. But the other various routing protocols could be simulated also. In this paper, we try to resolve flooding attack effect in the network. But the detection of this attack is also a future work that has simulated in future. Our solution looks the multipath in the AOMDV level. Finding the attacker nodes with connection oriented protocols could be different work as for a future study.

In our future scope of work, we would hold this approach in maximizing the performance of a network from flooding attack in term of flooding packets in network by that the link are congested. We simulated attack in the ad-hoc networks and find its affects.

References

[1] S.Madhavi, “An Intrusion Detection System In Mobile Adhoc Networks”, International Journal of Security and Its Applications Vol. 2, No.3, pp. 1-16, July, 2008

[2] V.P.and R. P. Goyal, "MANET: Vulnerabilities, Challenges, Attacks, Application," IJCEM International journal of Computational Engineering & Management, 2011.

[3] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, “Analyzing the Energy Consumption of Security Protocols,” Proceeding of International Symposium of Low Power Electronics and Design (ISLPED ’03), 2003.

[4] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55,April 1999.

[5] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of Various Routing Protocols for MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, pp. 251-259, November 2011.

[6] S. Ali Dorri and Seyed Reza Kamel and Esmail Kheyrkhah," Security Challenges In Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, pp. 15-29, February 2015

[7] M. Mukesh and K.R. Rishi, “Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review,” International Journal of Computer Applications, Vol. 12, No. 2, pp. 37-43, Dec. 2010.

[8] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[9] P.Yi, Z.Dai, S.Zhang, Y.Zhong,“A New Routing Attack In Mobile Ad Hoc Networks,” International Journal of Information Technology, vol. 11, no. 2, pp. 83-94, 2005.

[10] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 2002.

[11] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc

Networks, in Book The Handbook of Ad Hoc Wireless Networks , CRC Press LLC, 2003.

[12] Swagata Singha Abhijit Das, "Detection and Elimination of the Topological Threats in Mobile Ad Hoc Network: A New Approach", IEEE International Conference on Advances in Computer Engineering and Applications (ICACEA), pp.907-911, 2015.

[13] Hossen Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu, Member, IEEE, and Adrian Perrig, "Jamming-Resilient Multipath Routing", IEEE Transactions on Dependable And Secure Computing, Vol. 9, No. 6, pp. 852-863, November/December 2012.

[14] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection IEEE Transactions On Network And Service Management, Pp. 169-182, Vol. 9, No. 2, June 2012

[15] Preeti Sachan, Pabitra Mohan Khilar, "Security Attacks and Solutions in MANET", Proceedings of International Conference on Advances in Computer Engineering, 2011ACEEE, pp 172-176

[16] Pravina Dhurandher, "FACES: Friend Based Ad hoc Routing Using Challenges to establish security in MANET Systems" IEEE SYSTEMS Journal ,Volume 5, No 2, June 2011,pp:176- 188.

[17] Yi Zhang, QiangLiu "A Real-Time DDoS Attack Detection and Prevention System Based on per-IP Traffic Behavioral Analysis", 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 163 – 167, 2010 .

[18] Husain. Shahnawaz, Gupta S.C., Chand Mukesh "Denial of Service Attack in AODV & Friend Features Extraction to Design Detection ", IEEE International Conference on Computer & Communication Technology (ICCCT), pp. 292-297, 2011.