ISSN 2319-2720
Volume 3, No.4, October - December 2014
International Journal of Computing, Communications and Networking
Available Online at http://warse.org/pdfs/2014/ijccn01342014.pdf

A Survey Of Routing Attacks And Detection Schemes In MANET

Anuradha
M.Tech CSE, Galaxy Global Imperial Technical Campus, Dinarpur, Ambala.
singh.anuturka@gmail.com

Dr. Puneet Goswami
Professor & HOD (CSE), Galaxy Global Imperial Technical Campus, Dinarpur, Ambala.
goswamipuneet@gmail.com

Gurdeep Singh
M.Tech CSE, MMU, Sadopur, Ambala
gurdeepssingh@hotmail.com

ABSTRACT

The insecurity of the wireless links, power and energy constraints, poor physical protection of nodes in a hostile environment, and the vulnerability of statically configured security schemes poses challenges for routing and secure data transfer in wireless networks. No part or component of the network is dedicated to support specific network functionalities such as routing, security, load balancing, topology discovery, data forwarding etc individually. The absence of infrastructure and the consequent absence of authorization facilities impede the usual practice of establishing a line of defense, separating nodes into trusted and nontrusted. This paper focuses on different kinds of attacks in MANETs and then countermeasures and some detection mechanisms are discussed.

Key words : MANET, Attacks, Security, Intrusion Detection System

1. INTRODUCTION

A mobile ad hoc network is formed by multiple nodes connected through wireless links. Mobile nodes are willing to forward packets for neighbors. Every node can be a router and discover routes to other nodes so these networks have no fixed or dedicated routers. All nodes are capable of moving and can be connected dynamically in an arbitrary manner [1]. The responsibilities for organizing and controlling the network are distributed among the nodes themselves. In this type of networks, some of the terminals are outside the transmission range of other terminals and may not be able to communicate directly with them, so they rely on other terminals to deliver messages to the respective destinations. Such networks are referred as multi-hop or store-and-forward networks. The nodes may carry them or very small devices.

MANET posses several advantages due to its mobility and infrastructure-less structure such as fast establishment, dynamic topologies, fault tolerance, connectivity, mobility and cost. MANET doesn't require proper installation or network of wires.

It can easily be created and destroyed so it is easily adaptable. In MANET, nodes can enter or leave the network haphazardly that is why network topology graph seems to vary continuously. MANET supports fault tolerance, i.e., whenever there is failure of connection between nodes alternate paths may be provided for routing. In MANET, nodes can easily communicate with other nodes within its transmission range to forward data packet. There is no need of centralized links and gateways for communication. MANET supports mobility i.e. wireless mobile nodes can move in different directions that may increase complexity. So, routing algorithms must be designed to handle this complexity level. Cost of establishment of MANET is quite less because infrastructure is not required.

Although mobile ad-hoc networking is the need of hour but there are various limitations associated with them such as bandwidth constraint, processing capability, energy constraints, high latency, transmission errors and limited security. The capacity of wireless link is less than their wired counterparts. For example, wireless LAN has capacity 2 Mbps while that of wired LAN is in powers of Gbps. Routing and data transmission processes normally consumes a lot of power of mobile devices. Mobile devices have limited battery power backup. Their energy can't be wasted in employing cryptographic techniques for security and battery saving algorithms should be used instead. Mobile nodes remain in inactive state when they don't send data packets and come in latent state while sending state from dormant or inactive state which will increase delay. Attenuation and intervention increases the transmission error and thus effect the network performance. MANET suffers from various vulnerabilities that can be exploited by an attacker for harming the network and its resources.

2. SECURITY ATTACKS IN MANET

The security threats on MANET can be classified on the basis of mode of attack as active or passive) and origin of attack as internal or external. A classification of the security attacks in MANET is presented in Figure.1.

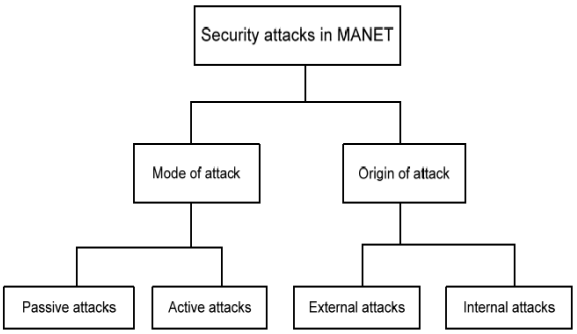

Figure 1. Classification of security attacks in MANET

2.1 Classification Based on the Mode of Attack

A. Passive Attack

The attackers in a passive attack can obtain the data exchanged in the network without disrupting any network operations. They can also launch an active attack by using the previously obtained information [2]. Due to the nature of the shared wireless communication medium, it is easier for an attacker to launch passive attacks in MANET than in wired networks. Examples of passive attacks include: eavesdropping which involves intercepting and reading messages by unintended receivers, and traffic analysis where the attackers analyze the data on who is communicating with whom, how often, how much and when [3] as shown in Figure 2.

B. Active Attack

In an active attack, the attackers disrupt the normal functionality of the network, which includes activities such as information interruption, modification, or fabrication as referred in the Figure 3. Examples of active attacks are: sleep deprivation torture, which targets the batteries; jamming, which results in channel unavailability by overusing it; hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them and attacks against routing protocols. Most of these attacks cause denial of service (DoS), which is degradation or complete halt in communication between nodes.

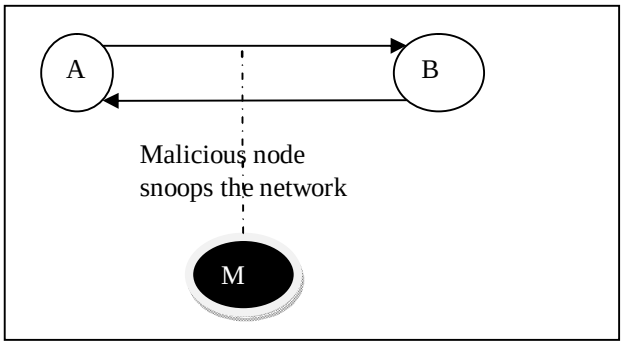

Figure 2: Passive attack

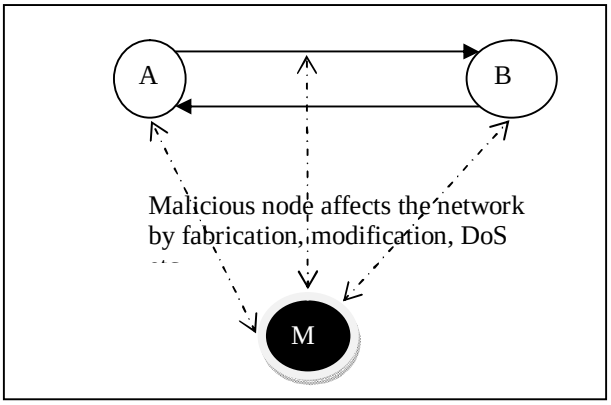

Figure 3: Active attack

2.3 Classification Based on the Origin of Attack

A. External Attack

External attacks are launched by a node or a group of nodes that does not belong to the logical network. [Referred in Figure 4] Therefore, the attackers are not capable of accessing the network and that limits their ability to disrupt the network services. Nevertheless, the attackers can attempt to jam the communication channel to interrupt the availability of the network. It is also possible that the attackers form a wormhole tunnel, which misguides two distant nodes in believing that they are direct neighbors of each other. In the extreme case, the attackers can eliminate a node from the network [4].

B. Internal Attack

Internal attacks are carried out by an internal compromised or malicious node which a part of the network domain. [Referred in Figure 4] This is a more severe attack because the attacker knows secret information and possesses privileged access rights. So, the internal attackers have the same capabilities of outside attackers, plus the ability to participate in the network protocols and eventually deviate from the normal behavior of the protocols. Some possible internal attacks include route disruption attacks such as routing loops, black holes, grey holes, packet dropping, wormhole with selective forwarding, rushing attack, and Byzantine attacks (e.g. Byzantine wormhole attack) [4].

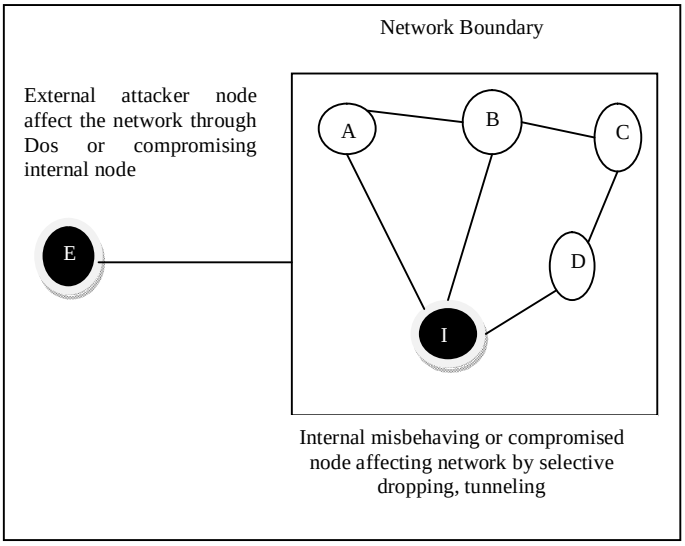

Figure 4. Internal attack vs. External attack

2.3 Attacks against the Routing Protocols

Routing is a process of searching and analyzing different possible routes from source to destination in the network so that data travels with optimal speed and minimal delay. It includes two prominent activities: route discovery phase and packet forwarding phase. Network layer protocols extend the connectivity from neighboring one-hop nodes to all other nodes in MANET. MANET routing protocols exchange routing messages between nodes and maintain routing states at each node. The data packets are forwarded by intermediate nodes along an established route to the destination. The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. By attacking the routing protocol, the attackers can inject themselves into the path between the source and destination. A variety of attacks that target the routing protocols in MANET are as follows:

A. Flooding Attack

Ad hoc flooding attack acts as DoS against all on demand ad hoc routing protocols like AODV, DSR, SAODV. The aim of this type of attack is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation of the performance of the network. For instance, in AODV protocol, a malicious node can send a large number of RREQs within a short period of time to a destination, which is not in the network domain. As a result, the RREQs will flood the whole network but no reply (RREP) will be generated, because the destination node does not exist.

B. Rushing Attack

On-demand routing protocols that suppress duplicate messages during the route discovery phase are vulnerable to rushing attack. A malicious node receiving Route Request packet generally floods the network with the route request packet quickly before other nodes receive the same Route Request packet from alternate path. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. This causes later legitimate route requests to be suppressed, and increases the probability that any route discovered by the source node would always contain the malicious node as one of the intermediate nodes.

C. Routing Cache Poisoning Attack

The routing protocols like DSR maintain route cache for storing routes. Routing cache poisoning attack occurs when these entries are either deleted; modified or false information is inserted. Malicious node M can broadcast spoofed packets with route to some node X through itself. Neighboring nodes will overhear the packet routed to X via M and may add the fake route in their route caches [5].

D. Blackhole Attack

In a blackhole attack, the attacker attracts data packets and then drops them by distributing false routing information [6]. The attacker claims that it has an optimum route. As a result, other good nodes tempt to route data packets through the malicious node.

E. Wormhole Attack

Wormhole attack is one of the most severe routing attacks in wireless networks. In this attack, an attacker node intercept packets at one location, tunnels them to another node at some other location of the network, where it is retransmitted in the network by a colluding attacker [7].

F. Byzantine Attack

In a MANET, the participating nodes are considered legitimate after a formal authentication procedure. Once authenticated, these nodes are given full control of the network and allowed to participate in network operation. This leads to the Byzantine wormhole problem when these authenticated nodes start misbehaving and disrupting the network operations [8]. The aim of the Byzantine nodes is to disrupt the communication of other nodes, but still participate in the routing protocol correctly. It is possible to deploy the following types of attacks by the Byzantine nodes in MANET: black hole attack, flood rushing attack, Byzantine wormhole attack, and Byzantine overlay network wormhole attack.

G. Sybil attack

A Sybil attack is an attack in which malicious node portrays two or more nodes rather than a single node like other attacks. The

Sybil nodes are created through a series of false identities, or impersonation of nodes and these additional node identities could be generated by possessing multiple physical devices [9].

H. Routing table overflow attack

This is the kind of multiple node attack that sends non-existent node data into the MANET and also tries to degrade the rate at which new updates are made into the routing table [10]. This kind of attack is aimed at flooding or disrupting the routing node of the victim with non-existent node data and it usually occurs against proactive routing protocols like OSPF and OLSR. Proactive routing protocols use periodic updates of routes even before they are required to transpire and this make them vulnerable to routing table attack. On the contrary, reactive routing protocols only produce a route when it is required, thus it is not vulnerable to routing table overflow attack.

3. SECURITY GOALS

Following security goals need to be addressed:

- **Availability**

Network resources are accessible for intended users. Loss of availability leads to DoS attack.

- **Integrity**

Recognized and authenticated parties can modify, preserve or transmitted information. A message could not be changed by malicious users.

- **Authentication**

Verifying the origin of the message i.e. message is sent by a node that claims to be. Without authentication, an attacker could impersonate any address.

- **Confidentiality**

It guarantees that information or data is never disclosed to unintended or malicious users. It can be ensured by cryptography.

- **Non-repudiation**

Disclosure and confinement of associated nodes are done under this property.

- **Authorization**

It describes the privileges of the nodes within network.

4. PREVENTION AND DETECTION OF ROUTING ATTACKS

4.1 Trust Based Security Solutions

The performance of ad hoc networks depends highly on cooperation and trust among nodes since no central authority is involved. When a node establishes trust in other nodes, it can predict the future behavior whether nodes will forward or drop packets based on direct and indirect trust value. A real number, trust value, can be computed further helps in decision making to improve security. Trust value is not symmetric i.e. if a node A trusts node B that does not mean B also trusts A.

Dhurandher et al. proposed [11] a message trust based solution which is applicable to the multipath routing scenario. Initially each node is given a zero trust value which specifies an unknown trust level. The assigned trust value is either incremented or decremented on the basis of behavior of the nodes. These values can be positive, negative or zero, which signifies known, malicious, or unknown behavior.

Mangrulkar et al. [12] proposed a scheme in which an extra field is added in the RREQ packet of AODV protocol called Trust Value. When source node broadcasts RREQ packet, it allocates the initial trust value. The trust value of all the nodes falling on the route of destination is incremented as soon as it receives RREP from the destination node. A valid route having higher trust value is selected by the source through the addition of this extra field rather than selection of the shortest route. This circumvents the disruption of the network because most of the attacks are synchronized on the shortest route to the destination.

Sen [13] suggested an approach to detect the packet dropping attack on MANETs. The process is dependent on the trust of each node which in turn is calculated by analyzing the packet forwarding behavior of the nodes.

Halim et al. presented Agent-based trusted solution to secure the DSR protocol [14]. The secure model uses a multi-agent system (MAS) for attaining the task of monitoring agent (MOA) and routing agent (ROA). The MOA in the routing process monitors its hosting node behavior and then computes the trust value for that node. ROA is responsible to use this trust value and searching the most reliable path to the destination.

4.2 Intrusion detection systems

Intrusion detection systems are not attack specific and are designed to deal with more than one kind of attack. Elhadi et. al proposed EAACK [15] which overcomes demerits of Watchdog [16] like false misbehavior, limited transmission power and receiver collision through the use of digital signatures for verifying node's identity. It relies completely on acknowledgements received for packets successfully delivered at destination. In this scheme, the source node switches to misbehavior report authentication (MRA) mode and first confirms the misbehavior and not believing blindly the occurrence of the misbehavior. If misbehavior is detected, alternate route to reach destination node is selected or route discovery is initiated again.

In anomaly based IDS, normal and secure state of the network is compared with present state of the network and any deviation from normal is treated as an attack. Such systems involve two phases: training phase based on neural networks, probabilistic models like chi-square, Markov chain etc and testing phase based on mathematical or statistical methods for comparing both networks [17].

Another kind of IDS is Specification Based (SBID) systems in which detection is based on monitoring the syntax and semantics of operations. Jahnke et al. proposed the use of finite state machines for specifying the routing behavior of routing protocols and monitoring incorrect request and reply packets using distributed Network Monitors [18]. This technique is effective against man in the middle attack, wormhole attack, blackhole attack etc.

Negar et al. suggested an Intrusion Detection System (IDS) [19] on the basis of the interaction between the user and the kernel processes that differentiates the normal behavior from anomalous behavior by generating a feature list. A new function called the Wrapper Module is instigated to the Linux Kernel for logging initial data to create the intended feature list. In the proposed scheme SVM neural network is applied to categorize the input vectors. In comparison to other systems the authors tried to enhance the accuracy, training time and testing time.

Saravanakumar et al. [20] tackled the problem of complexity and throughput that are apparent in the current Intrusion Detection Systems (IDS). They contrasted various IDS systems that employ different algorithms for detecting the intrusions. The authors also suggested a scheme for designing an IDS that uses a combination of various Artificial Neural Network (ANN) algorithms that delivers better performance by converging faster.

Nikolova and Jecheva [21] proposed an anomaly based Intrusion Detection System (IDS) which is based on data mining techniques such as classification trees for describing the normal activity of the system. Similarity coefficients are used for comparing the similarity between the normal behavior and the observed behavior which detects the intrusion in the system. Based on the measured similarity, a decision is made whether the system is under attack or not.

Banerjee et al. [22] suggested an Ant Colony based IDS for tracking the intruder trails. The proposed method gives higher level of security to the sensor networks through its synchronization with the default learning based detection systems.

5. CONCLUSION

High mobility, resource constrained and geographically distributed MANETs makes it more vulnerable to routing attacks. This study investigated different routing attacks in MANET and reviewed existing trust based and intrusion detection schemes. Some of the techniques are specific for particular attacks while others are quiet general to deal with a variety of attacks. Even though effective detection schemes have been proposed, attackers usually employ new methods to attack the networks. Therefore, it is a never ending research area and new schemes thus need to be devised. Intrusion based detection systems are observed as an emerging method to mitigate routing attacks.

REFERENCES

1. [1] Pahlavan and Kaveh, "**Principles of wireless networks: A unified approach**", John Wiley & Sons, Inc., 2011.
2. [2] D. Djenouri, L. Khelladi, and A. Badache, "**A survey of security issues in mobile ad hoc and sensor networks**". IEEE Communications surveys & tutorials, 2005. 7(4): p. 2-28.
3. [3] C. Gray, J. Byrnes, and S. Nelakuditi, "**Pair-wise resistance to traffic analysis in MANETs". SIGMOBILE Mobile Computing and Communications Review**, 2008. 12(1): p. 20-22.
4. [4] Rajakumar, P.; Prasanna, V.T.; Pitchaikkannu, **A., "Security attacks and detection schemes in MANET,"** Electronics and Communication Systems (ICECS), 2014 International Conference on , vol., no., pp.1-6, 13-14 Feb. 2014.
5. [5] Y. Hu and A. Perrig, **A survey of secure wireless ad hoc routing.** IEEE Security and Privacy magazine, 2004. 2: pp. 28-39.
6. [6] Tarunpreet Bhatia and A.K. Verma, **Performance Evaluation of AODV under Blackhole Attack**, International Journal Computer Network and Information Security, 5 (2), pp 35-44, 2013.
7. [7] J. Baras, S. Radosavac, G. Theodorakopoulos, **Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR. In Proceedings of Military Communication Conference** (MILCOM '07), 2007, pp. 1-7.
8. [8] A. Sangi, J. Liu, and L. Zou. **A performance analysis of AODV routing protocol under combined byzantine attacks in MANETs.** In Preceedings of International Conference on Computaional Intelligence and Software Engineering (CiSE '09), December 2009. p. 1-5.
9. [9] A. Mishra, **Security and Quality of Service in Ad Hoc Wireless Networks,** 2008.
10. [10] S. Sampalli, S. Jamwal, L. Lei, P. Moradiya, S. Parikh, T. Potluri, T. Shingne, A. Thangaraj and A. Trabulsi, "**Routing Intrusions on Mobile Ad Hoc Networks: Test bed and Vulnerability Analysis",** In Proceeding of Software, Telecommunications and Computer Networks, 2007. SoftCOM 2007. pp: 1-5.
11. [11] Sanjay K. Dhurandher, Vijeta Mehra, "**Multi-path and Message Trust-Based Secure Routing in Ad Hoc Networks",** International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT '09., Dec. 28-29,2009, pp.189-194.
12. [12] R. S. Mangrulkar, Mohammad Atique, "**Trust Based Secured Ad hoc on Demand Distance Vector Routing Protocol for Mobile Ad Hoc Network**", 2010 Sixth International Conference on Wireless Communication and Sensor Networks (WCSN), Dec. 15-19 ,2010,pp.1-4.
13. [13] Jaydip Sen, "**A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks**", Proceedings of the 3rd International Conference on Network Security and Applications, Chennai, India, 2010, pp. 538- 537.
14. [14] Islam Tharwat A. Halim, Hossam M. Fahmy, Ayman, M. Bahaa El-Din, Mohamed H. El-Shafey, "**Agent-based Trusted On-Demand Routing Protocol for Mobile**

Ad-hoc Networks", 2010 4th International Conference on Network and System Security (NSS)Sept. 1-3, 2010, pp. 255-262.

15. [15] Elhadi M. Shakshuki, Nan Kang, Tarek R. Sheltami "EAACK—**A Secure Intrusion-Detection System for MANETs**", (2013), IEEE Transactions on Industrial Electronics, vol. 60, no. 3.
16. [16] S. Marti, T.J. Giuli, K.Lai and M. Baker, "**Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks**",(2000), Proceedings of International Conference on Mobile Computing and Networking, pp 255-265.
17. [17] N. Ye, X. Li, Q. Chen, M. Emran and M. Xu, "**Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data**", (2001) IEEE Transactions on Systems, Man, and Cybernetics, Vol. 31, No. 4, July.
18. [18] J. Tolle, M. Jahnke, N. gentschen Felde and P. Martini, "**Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System**", (2006), Proceedings of the 25th Military Communications Conference (MIL-COM).
19. [19] Almassian Negar, Azmi Reza, Berenji Sarah, "**AIDSLK: An Anomaly Based Intrusion Detection System in Linux Kernel",** Information Systems, Technology and Management Communications in Computer and Information Science, 2009, Publisher: Springer Berlin Heidelberg, pp. 232-243.
20. [20] S. Saravanakumar, Umamaheshwari, D. Jayalakshmi, R. Sugumar, "**Development and implementation of artificial neural networks for intrusion detection in computer network**", Int. Journal of Computer Science and Network Security. 2010. vol. 10, no. 7, pp. 271-275.
21. [21] Evgeniya Nikolova, Veselina Jecheva, "**Some similarity coefficients and application of data mining techniques to the anomaly-based IDS**", Telecommunication Systems, December, 2010, Publisher: Springer Netherlands, pp. 1-9.
22. [22] S. Banerjee, C. Grosan, A. Abraham, P. K. Mahanti, "**Intrusion detection in sensor networks using emotional ants**," Proceedings of 5th International Conference on Intelligent Systems Design and Applications, (ISDA '05), Wroclaw, Poland, Sept. 8-10, 2005, pp. 344- 349.