Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Analytical Approach on Intrusion Detection System in MANETS for Attacks

Sakil Ahmad Ansari
Research Scholar
Al-Falah University,Faridabad, Haryana, India

Mohammad Danish
Assistant Professor, Dept of CSE
Al-Falah University,Faridabad, Haryana, India

Abstract- In this paper, we discuss attacks on mobile ad hoc networks. Mobile Ad hoc Networks is a collection of wireless mobile nodes, which form temporary networks without relying on any existing infrastructure or centralized administration or standard support services regularly available in wide area networks to which the host may normally be connected. In this paper we review the security attacks on mobile ad hoc networks like black hole, grey hole attacks ,wormhole attacks etc. the study on security attacks and intrusion detection system has led us to illustrate some of the particular security issues.Finally,we identify areas where further research could focus.

Keywords- MANETS, IDS, Security Attacks, Securing ad hoc networks.

I. INTRODUCTION

Mobile Ad hoc Networks is a collection of wireless mobile nodes, which form temporary networks without relying on any existing infrastructure or centralized administration or standard support services regularly available in wide area networks to which the host may normally be connected [3]. MANET is one of the most important technologies that have gained interest due to recent advantages in both hardware and software techniques. MANET technology allows a set of mobile uses equipped with radio interfaces (Mobile nodes) to discover each other and dynamically form a communication network. MANET incorporates routing functionality into mobile nodes so that they become capable of forwarding packets on behalf of other nodes and thus effectively become the infrastructure. Providing multiple routing paths between any source-destination pair of nodes has proved to be very useful in the context of wired networks [7].

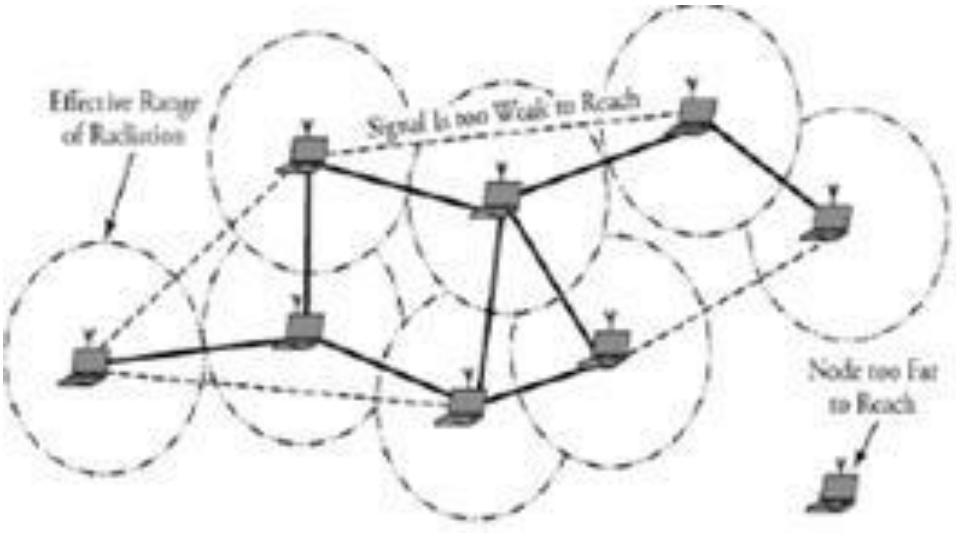

Figure 1: Typical Mobile ad-hoc network Diagram

Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense [1]. Most of the routing protocols for MANETs are thus vulnerable to various types of attacks**.** Security is a main concern in the establishment of MANETs. Literature is abundant in defining protocol extensions to provide more secure MANET communications. Also many techniques have been developed to identify different types of network attacks, such as the wormhole attack, for example. However, all these security solutions are designed for specific routing protocols [6]. In the absence of generic security architecture, nodes from different MANET domains cannot cooperate and benefit from security advantages across the entire network, such as secured inter-domain routing, etc. A lot of challenges come with implementing these networks [15].

We proposed a scheme for intrusion detection in MANET. They proposed distributed and cooperative framework to detect the attack. Every node in the MANET participates in the process of intrusion detection. It detects the sign of intrusion locally and independently and also propagates this information to other nodes in the network [11]. Intrusion Detection is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system and are abusing their privileges. The system protected is used to denote an information system being monitored by the Intrusion Detection system. The Intrusion Detection system (IDS) is a computer system that dynamically monitors the system and user actions in the network and computer system in order.

Additional challenges for IDSs in MANETs are as follows:
• MANETs lack concentration points where monitoring and audit data collection can be performed.
• Due to the nodes mobility, the network topology is dynamic and unpredictable, making the process of intrusion detection complicated.
• IDSs in MANETs are more complex because of the limited computational ability of most of the nodes.

II. BACKGROUND

Attacks on MANETs

At the highest level, the security goals of MANETs are not that different from other networks: most typically authentication, confidentiality, integrity, availability, and non-repudiation. Authentication is the verification of claims about the identity of a source of information. Confidentiality means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information systems.Availability refers to the ability of the network to provide services as required. Denial of Service (DoS) attacks has become one of the most worrying problems for network managers. In a military environment, a successful DoS attack is extremely dangerous, and the engineering of such attacks is a valid modern war-goal. Lastly, non-repudiation ensures that committed actions cannot be denied. In MANETs security goals of a system can change in different modes (e.g. peace time, transition to war, and war time of a military network). The characteristics of MANETs make them susceptible to many new attacks. At the top level attacks can be classified according to network protocol stacks. Some type of attacks could occur in any layer of the network protocol stack, e.g. jamming at physical layer, hello flood at network layer, and SYN flood at transport layer are all DoS attacks. Because new routing protocols introduce new forms of attacks on MANETs. Attackers against a network can be classified into two groups: insider and outsider attackers. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs. Routing algorithms are typically distributed and cooperative in nature and affect the whole system. While an insider MANET node can disrupt the network communications intentionally, there might be other reasons for its apparent misbehaviors. A node can be failed, unable to perform its function for some reason, such as running out of battery, or collisions in the network. The threat of failed nodes is particularly serious if they are needed as part of an emergency/secure route. Their failure can even result in partitioning of thenetwork,preventing some nodes from communicating with other nodes in the network. A selfish node can also misbehave to preserve its resources. Selfish nodes avail themselves of the services of the other nodes, but do not reciprocate. This research focuses on the attacks carried out by malicious nodes who intentionally aim to disrupt the network communication [1] and [3].

MANETs like other wireless networks are liable to active and passive attacks.In the passive attacks, only eavesdropping of data happens; while in the active attacks, operations such as repetition,changing or deletion of data are necessitated. Certain nodes in MANETS can produce attacks which cause congestion, distribution of incorrect routing information services preventing proper operation, or disable them [7].

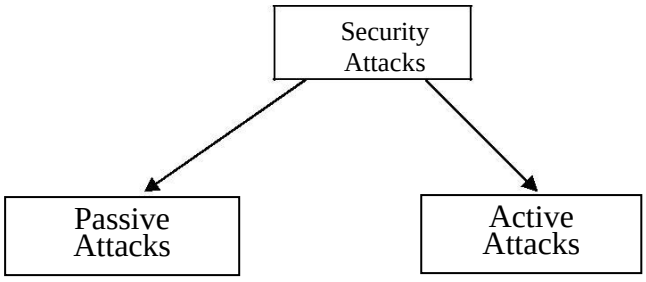

Figure 2: Attacks on Mobile Adhoc Network

Table 1: Network Security Attacks against MANETS

Passive Attacks	Active Attacks
Snooping,eavesdropping,traffic analysis ,monitoring	Wormhole, black hole, gray hole, information disclosure, resource consumption, routing attacks

Classification of Attacks: Attacks in MANETs can be divided into two main categories, namely passive attacks and active attacks, as shown in Figure 2.

A. Passive Attacks

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard. There is an attack which is specific to the passive attack a brief description about it is given below:

1) Snooping

Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

2) Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

3) Traffic Analysis & Location Disclosure

Attackers can listen to the traffic on wireless links to discover the location of target nodes by analyzing the communication pattern, the amount of data transmitted by nodes and the characteristics of the transmission. Although passive attacks do not directly affect the network functionality, in some MANET application scenarios, such as military communication, important information disclosure through traffic analysis or simply eavesdropping could prove costly [17][18].

B. Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.

1) Wormhole Attack

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

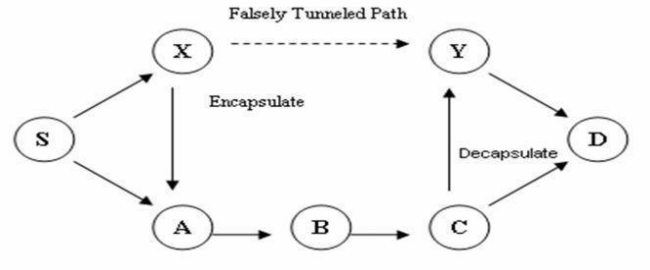

Figure 3: Wormhole attack

2) Black hole Attack

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the

packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

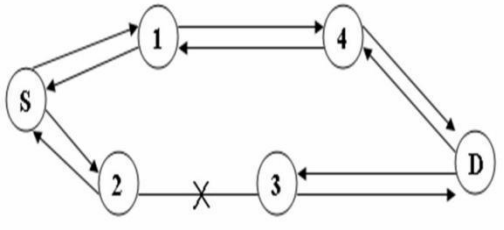

Figure 4: Black hole attack

3) Gray Hole Attack

Gray Hole attack is the attack on the adhoc network. Gray Hole attack can be act as a slow poison in the network side means we can't said that probability of losing the data. In Gray Hole Attack [6] a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node , When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination. We now describe the gray hole attack on MANET‟S .The gray hole attack has two important stages, In first stage, a malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interrupting or corrupting packets, even though route is spurious. In second stage, nodes drop the interrupted packets with a creation probability. Detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack. A variation of black hole attack s is the gray hole attack, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). Both types of gray hole attacks seek to disrupt the network without being detected by the security measures in place.

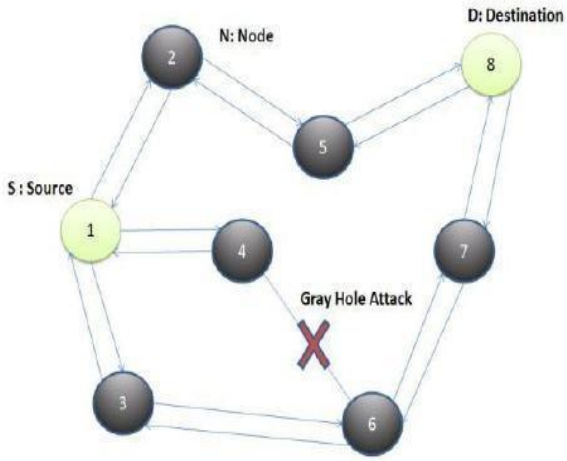

Figure 5: Gray Hole Attack in Mobile Adhoc Network

4) Rushing Attack

An attack where a node "rushes" a corrupt packet identified to match the real packet. The receiving node first accepts the corrupt packet, drops it and then, on receipt of the good packet matches the packet identity to that of the prior, and drops it.

5) Sybil Attack

Each node in a MANET requires a unique address to participate in routing, through which nodes are identified. However, in a MANET there is no central authority to verify these identities. An attacker can exploit this property and send control packets, for example PREQ or PREP, using different identities; this is known as a Sybil attack (SY) [18]. This is an impersonation attack where the intruder could use either random identities or the identity of another node to create confusion in the routing process, or to establish bases for some other several attack.

6) Routing Attacks

Both the reactive and proactive routing protocols are vulnerable to routing attacks because they route based on the assumption that all nodes cooperate to find the best path. Consequently, a malicious node can exploit the vulnerabilities of the cooperative routing algorithms and the lack of centralized control to launch routing attacks. In particular, the on-demand (reactive) MANET routing protocols, such as AODV [19] and DSR [20], allow intruders to launch a wide variety of attacks.

7) Malicious Packet Dropping

A path between a source node and a destination node in a MANET is established using a route discovery process. Once this has been done, the source node starts sending the data packet to the next node along the path; this intermediate node identifies the next hop node towards the destination along the established path and forwards the data packet to it. This process continues until the data packet reaches the destination node. To achieve the desired operation of a MANET, it is important that intermediate nodes forward data packets for any and all source nodes. However, a malicious node might decide to drop these packets instead of forwarding them; This is known as a data packet dropping attack, or data forwarding misbehavior. In comparison to deliberately malicious behavior, in some cases nodes are unable to forward data packets because they are overloaded or have low battery reserves; alternatively the nodes may be selfish, for example saving their battery in order to process their own operations. Packet dropping attacks differ from black hole and grey hole attacks because there is no attempt to "capture" the routes in the network.

III. CONCLUSION

In this paper we review paper which is based on security problems and intrusion detection system for attacks in Manets. We observed that existing intrusion detection schemes have not included the fact that some misbehaving nodes can also indulge in improper use of shared media. We have focused on this part and we have also proposed IDS, which can detect if nodes are not getting their fair share of the transmission channel. However, history shows that intruders often find new ways to attack and cause damage to computer systems and networks .Therefore, we consider that enabling a protection mechanism to learn from experience and use the existing knowledge of attacks to infer and detect new intrusive activities is an important and potentially fruitful area of future research. We also believe that the development and deployment of network security policies are vital in networks with a dynamic environment such as are found in MANETs; this is a further potential area of research. Finally, the attacker may try to attack an existing protection scheme; therefore the protection mechanisms need to be robust enough to protect themselves and not introduce new vulnerabilities into the system.

REFERENCES

[1] Panayiotis Kotzannikolaou, Rosa Mavropodi, Christos Doulideris. (2005), "Secure Multipath routing for Mobile Ad hoc Networks", Proceedings of the second Annual conference on Wireless On demand Network System and services (WONS‟05), IEEE, pp 1-8

[2] Akarygiannis, E. Antonakakis and A. Apostolpoulos. (2006), "Detecting Critical Nodes for MANET Intrusion Detection systems", Proceddings of second international workshop on security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU‟06), IEEE, pp 1-9

[3] Neeraj Nehra, R.B. Patel, V.K. Bhat, "Routing with Load Balancing in Ad Hoc Network: A Mobile Agent Approch", 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 1007), 2007 IEEE

[4] Amir Darehshoorzadeh , Nastooh Taheri Javan, Mehdi Dehgan, Mohammad Khalili, "A New Load Balancing Multipath Routing Algorithm for Mobile Ad Hoc Networks", Proceedings of IEEE 2008 6th National Conference on Telecommunications and IEEE 2008 2nd Malaysia Conference on Photonics, 26-27 August 2008, Putrayaja, Malaysia, pp 344-349

[5] Zhang XiangBo, Ki ll Kim, "Load Aware Metric for Efficient Balancing on Multipath DSR Protocol in Mobile Ad Hoc Networks", 2008 International Conference on Advance Technologies for Communications, 2008 IEEE, pp 395-398.

[6]. Tameen Eissa, Shukor Abd Razak, Md Asri Ngadi ,"Enhancing MANET security using Sceret public Keys" International Conference on Future Networks, (2009)IEEE, pp 130-134.

[7] Marjan Kuchaki Rafsanjani, Ali Asghar Khavasi, Ali Movaghar, "An Efficient Method for Identifying IDS Agent Nodes by Discovering Compromised Nodes in MANET," 2009 IEEE Second International Conference on Computer and Electrical Engineering, PP 625-629 .

[8] Maysam Hedayati, Hamid reza hoseiny, Seyed Hossein Kamali, Reza Shakerian,"Traffic Load Estimation and Load Balancing in Multiple Routing Mobile Ad Hoc Network", 2010 International Conference on Mechanical and Electrical Technology(ICMET 2010), 2010 IEEE, pp 18-21

[9] Mehdi EffatParvar, MohammadReza EffatParvar, Amir Darehshoorzedeh, Mehdi Zarei, "Load Balancing and Route Stability in Mobile Ad Hoc Networks base on AODV Protocol", 2010 International Conference on Electronic Devices, System and Applications(ICEDSA2010), 2010 IEEE, pp 258-263.

[10] R.Balakrishna , U.Rajeswar Rao , N.Geethanjali N,"Performance Issues on AODV and AOMDV for Manets", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) ,2010, pp 38-43.

Mohamed Tekaya,Nabil Tabbane, Sami Tabbane, " Multiple Routing Mechanism with Load Balancing in Ad Hoc Networks",2010 IEEE, pp 67-72.

[12]. Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra. (2010), "Security issues in MANET: A Review", IEEE , pp 124-128 .

[13]. Husain Shahnawaz, Dr. S. C Gupta, Chand Mukesh, Dr. H.L. Mandoria , " A Proposed Model For Intrusion Detection System for Mobile Adhoc Network", International Conference on Computer and communication Technology (ICCCT"10), IEEE, pp 99-102

[14]. Peyman Kabiri and Mehran Aghaei. (2011), " Feature Analysis for Intrusion Detection in Mobile Adhoc Networks", International Journal of Network security , Vol 12, No 1 , pp 42-49 .

[15]. Nan Kang, Elhadi M. Shakshuki , Tarek R. sheltami. (2011), "Detecting forged Acknowledged in MANETs", International Conference on Advance Information Networking and Applications, IEEE , pp 488-494

[16]. S. Mangai and A. Tamilarasi. (2011), "Analysis of an efficient Scalable and secured Geographic Routing Protocol for MANETs," International Journal of Advanced Computing (IJAC), Vol 3, issue 2, pp 47-53 .

[18] Okoli Adaobi, Ejiro Igbesoko, Mona Ghassemian. (2012)," Evaluation of Security Problems and Intrusion Detection Systems forRouting Attacks in Wireless Self-organised Networks",IEEE www.olsr.org

[19] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay," Different Types of Attacks on Integrated MANET-Internet Communication,"International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp 265-274.

[20] Pradip M. Jawandhiya et. al., " International Journal of Engineering Science and Technology, " Vol. 2(9), 2010,"pp 4063-4071.

[21] Onkar V.Chandure, V.T.Gaikwad," Detection & Prevention of Gray Hole Attack in Mobile Ad Hoc Network using AODV Routing Protocol," International Journal of Computer Applications (0975 - 8887) Volume 41- No.5, March 2012,"pp 27-32 .

