British Journal of Mathematics & Computer Science
8(1): 25-38, 2015, Article no.BJMCS.2015.142
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Survey of Mobile Ad hoc Networks Attacks and a New Classification Scheme

Noureldien A. Noureldien[1], Saeed K. Saeed[1*], M. Ahmed Salih[1] and Alsawi M. Ahmed[1]

[1]Department of Computer Science, University of Science and Technology, Omdurman, Sudan.

Article Information

DOI: 10.9734/BJMCS/2015/15393
Editor(s):
(1) Yilun Shang, Department of Computer Science and Institute for Cyber Security, University of Texas at San Antonio, USA.
(2) Doina Bein, Applied Research Laboratory, The Pennsylvania State University, USA.
Reviewers:
(1) Anonymous, India.
(2) Niranjan Panda, Computer Science & Engineering, Siksha 'O' Anusandhan University, Odisha, India.
(3) Anitha Vijaya Kumar, Electronics and Communication Engineering, Visvesvaraya Technological University, India.
(4) Sherin Zafar, Manav Rachna International University, Faridabad And Faculty of Engineering, Jamia Milia Islamia, India.
(5) Yueran Gao, Southern Illinois University Carbondale, USA.
(6) Natarajan Meghanathan, Department of Computer Science, Jackson State University, USA.
(7) Anonymous, South Korea.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=1030&id=6&aid=8450

Original Research Article

Received: 24 November 2014
Accepted: 28 January 2015
Published: 14 March 2015

Abstract

Mobile Ad Hoc Networks (MANETs) is a growing technology which magnetizes many useful applications because nodes can communicate with each other and join and leave network without any predetermined network infrastructure.
This behavior of MANETs makes it vulnerable to various different types of attack, so security solutions must be implemented for such environment. Developing adequate countermeasures requires understanding and classification of these attacks.
In this paper a comprehensive survey of MANET attacks is performed, and a new classification scheme that is based on the security service targeted by the attack, namely, confidentiality, integrity and availability is proposed.
This new classification will provide a better understanding to MANETs attacks that can aid in developing a security service oriented detection and prevention techniques.

Keywords: MANETs; security; attack; classification; scheme.

1 Introduction

A mobile ad hoc network (MANET) is an infrastructure less network, which consist of a collection of equal nodes with no any centralized control; these nodes communicate with each other over the wireless media and have the mobility and the self configuration ability without need of central

**Corresponding author: saeed_kl@hotmail.com;*

administration. The nodes can be interconnected to the network and leave it dynamically and freely. This makes MANET topology highly dynamic and random.

For MANET nodes to communicate, they must set up paths among one another, and the routing process will rely on the collaboration between the interconnected mobile nodes [1]. Therefore, to provide effective functionality, the traditional routing protocols were modified to meet these special needs and new routing protocols, such as Ad hoc On Demand Distance Vector routing protocol (OADV) are implemented.

The special features of MANETs, such as, lack of centralization, limitation of resources, non secure boundaries, scalability, cooperativeness, dynamic and random topology, make it highly susceptible to many security challenges and vulnerabilities [2].

Due to these vulnerabilities, MANETs has been targeted by a huge number of attacks and each of which has its own malicious effects. In order to understand the behavior and similarity of these attacks, many classification schemes have been proposed.

Authors of [3,4,5,6,7,8] propose classifying attacks based on the layer of the networking stack in which they occur. In [9] a classification based on the types of the packets targeted by the attackers was proposed. On the other hand, in [10] MANET attacks are classified into passive and active attacks and in [11] as internal and external attacks. In [12] the authors classified the attacks against AODV according to the security goals targeted by the attack.

However, it is obvious that any attack targets to compromise one of the general network security requirements, i.e. confidentiality, integrity, or availability. Thus, it seems reasonable to classify attacks based on the security service compromised by the attack.

In this paper a survey of MANET attacks is carried out, and a classification of these attacks, based on security requirements is performed.

The rest of this paper is organized as follows: section 2 is dedicated to MANET attacks. Section 3 reviews the previous classifications of MANET attacks. Section 4 is introducing the proposed classification and in section 5 conclusions are given.

2 Manet Attacks

As mentioned above MANETs are vulnerable to numerous types of attacks due to its nature and characteristics. This section describes these attacks and their effects.

2.1 Wormhole Attack

In this attack, two or more malicious nodes collude to control the network by making a tunnel between them, this tunnel is used to forward the packets that are sent in the network to make malicious behavior [13,14]. The wormhole attack could prevent, discover routes other than the tunnel, thus the malicious nodes will be able to capture any packet sent on the network, which will allow the possibility of disclosure, modification or dropping of packets. For example, in Fig. 1 the malicious nodes M1 and M2 initiate tunnel between them and this tunnel is used later to achieve selfish behaviors.

2.2 Eavesdropping Attack

This attack can target confidentiality by capturing plain data packets that must be secured and confidant [3,15], for example, it can be used to pick secret information such as passwords and keys or any secret information during communication.

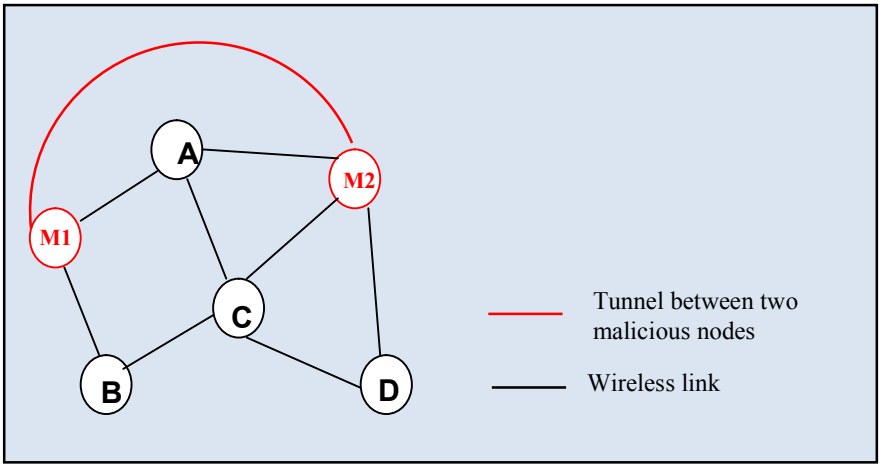

Fig. 1. Wormhole attack

2.3 Traffic Monitoring and Analysis Attacks

In this attack the adversary monitors the packet traffic to collect information such as the source of transmission, destination and packet size that can help in planning further attacks that may compromise any of the three security services in the network [16,3].

2.4 Location Disclosure Attack

The location disclosure attack tries to gather information about the nodes location or the network topology to make further attacks; the adversary gathers information such as a route map and knows which nodes are located on this route which will help to do any future malicious behavior, also the attacker tracks all the changes in traffic to achieve a smart attack [3]. Different attacks that can compromise security services can be launched based on the gathered information.

2.5 IP Spoofing Attack

When a new node wants to connect to the network it chooses a random address and then broadcasts a conflicted IP address detection packet, if this address is not assigned previously to another node, then the node can connect successfully. An adversary can get this packet and impersonate the same address to stop and prevent the new node to connect [17], so this attack results in a denial of service.

For example, Fig. 2 shows IP spoofing attack, as shown the new node N wants to connect to the network so it broadcasts to detect the neighbors whom have the same address to avoid confliction. The malicious node M argues that it has neighbor with same address $N^{\backslash}$ to prevent N from connecting.

2.6 Sybil Attack

In this attack the malicious node impersonate nonexistent nodes appearing as multi normal nodes, these malicious nodes work together and when a new node wants to be configured and using some configuration information such as an IP address, this information will seem to be used by another node. Thus preventing a new node from communication with other nodes [18], so this attack works when the cooperation is available and it deny recourse access.

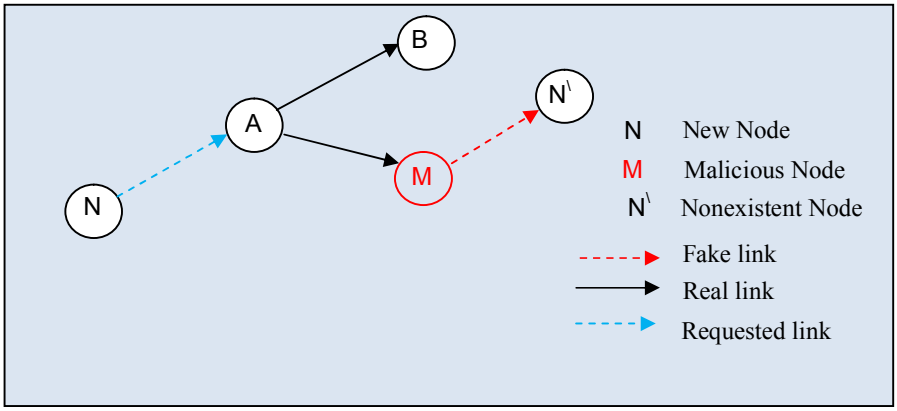

Fig. 2. IP spoofing attack

2.7 Modification Attack

Modification includes writing, changing status and deleting from data packets in an unauthorized manner by the malicious nodes that participate in the packet forwarding process [16,3,15]. This type of attack endangers clearly the integrity of the packets in the networks. For example, in Fig. 3 node S want to send data packet to destination D and it has discovered route to D through [S, M, C, D] when malicious node M receives the data packet, it modified and then forwards it to node C, node C forwards the modifies packet to destination D.

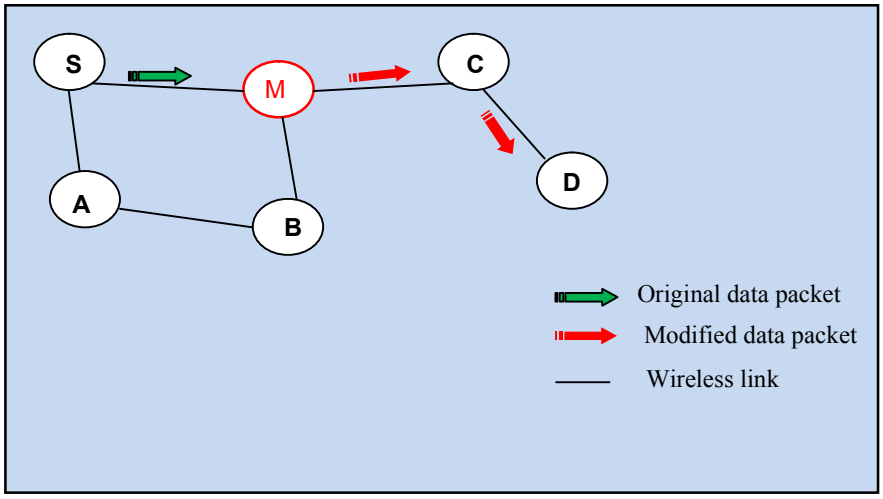

Fig. 3. Example for modification attack

2.8 Fabrication Attack

In this attack malicious nodes fabricate their own packets and inject it into the networks [3,15], for example the attacker may fabricate routing error messages, which claim that a neighbor can no longer be connected. Fabrication attack produces incorrect data that will hurt the integrity of data.

2.9 State Pollution Attack

In this attack, at the routing discovery operation a malicious node gives incorrect parameters in the route reply message [3]. This can result in modification of the normal routing information which leads to a significant damage in packet routing operation, which cause a form of denial of service.

2.10 Data Corruption Attack

This attack targets data integrity and availability as its result in packet corruption due to a malicious activity on the network or due to radio propagation failure [16].

2.11 Replay Attack

In replay attack the adversary node records legitimate packets and resend them back later to make an unauthorized effect [3], that compromise integrity, confidentiality or availability of information or the network. For example, a malicious node can record a route advertisement message and then rebroadcast it later, this message may carry stale information about paths, when other nodes receive this advertisement and updates their routing information accordingly, this can cause a denial of service.

2.12 Jamming Attack

The jamming attack occurs when a jammer prevents the legitimate users from exchanging messages by interfering the signals over the transmission media, leading to a denial of service [19,20].

2.13 Black-hole Attack

This attack [21] has two phases: in the first phase the attacker claim to have a valid route to the destination even though the route is a fake, and in the second phase the attacker drops the packets instead of forwarding them to that destination and this can make pull down effect on availability in the network.

For example, in Fig. 4, node S wants to send data to the destination node D, node S broadcast RREQ and when the malicious node M receives this RREQ, it sends RREP message to node S and its claims it has a valid route to destination D. When S receives this message, it begins forwarding data throw node M and when the data arrives to malicious node M; M instead of forwarding data to node D; it simply drops this data.

2.14 Gray-hole Attack

This attack is similar to black-hole attack since the attacker drops all the packets, but in the gray-hole the attacker selectively drops the packet depending on special expectation which makes it more difficult to detect the black-hole attack. So the attack targets availability.

2.15 Resource Consumption Attack

In this attack the malicious node tries to consume the victim resources [22,23], storage capacity, power, …etc., in order to render it unresponsive. For example the attacker can sink the target node by sending a storm of RREQ for fake destination, consuming their resource and this lead to pull down or disable the victim nodes. Thus, these attacks target availability.

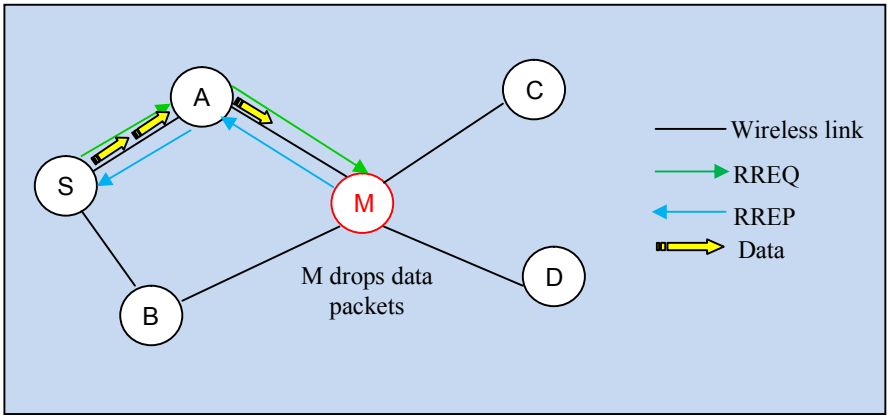

Fig. 4. Black-hole attack

2.16 SYN Flooding Attack

As mentioned early the resources in the MANET are limited and the SYN Flooding attack [24,25,17] exploit this limitation to drop down the victim by sending a huge number of half-opened TCP connections, without completing the three way handshake operation, and this selfish behavior makes the victim node unable to deal with the other legitimate requests to opening a connection. This attack is a famous denial of service attack.

For example, in Fig. 5 the malicious node M sinks the target node T with storm of half TCP connection without accomplishing the connection, node T has limited space for storing routing information after this limited space is full with selfish TCP connection requests from M the legitimate nodes N2, N3 and N4 they try to open a connection with T but this legitimate request cannot be accepted by node T because there is no free space can be used to store the new connection entry.

2.17 Byzantine Attack

Byzantine attacks targeting availability, in such attacks, the attacker compromised an intermediate node or a set of nodes works alone or in collusion to carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services [23].

2.18 Flooding Attack

The flooding attack is a denial-of-service attack. The attacker sends a large number of packets to the other nodes [22]; these packets may be either data packets or routing control packets. In data packet flooding, the attacker sends a huge amount of useless data packets to all other nodes in the network. In routing control packet flooding, for example the attacker floods the RREQ to a destination node that does not exist in the network, so these RREQs packets will reach to all of the other nodes in the network which makes a routing loop.

The flooding process takes a lot of the network resources such as bandwidth, processing or power resources, also flooding disrupts the routing operation. For example, in Fig. 6 the malicious node M sends a RREQ to nonexistent node to her neighbors B and A, nodes A and B forward this RREQ for their one hop neighbors and this flood is continued until reaches the whole network.

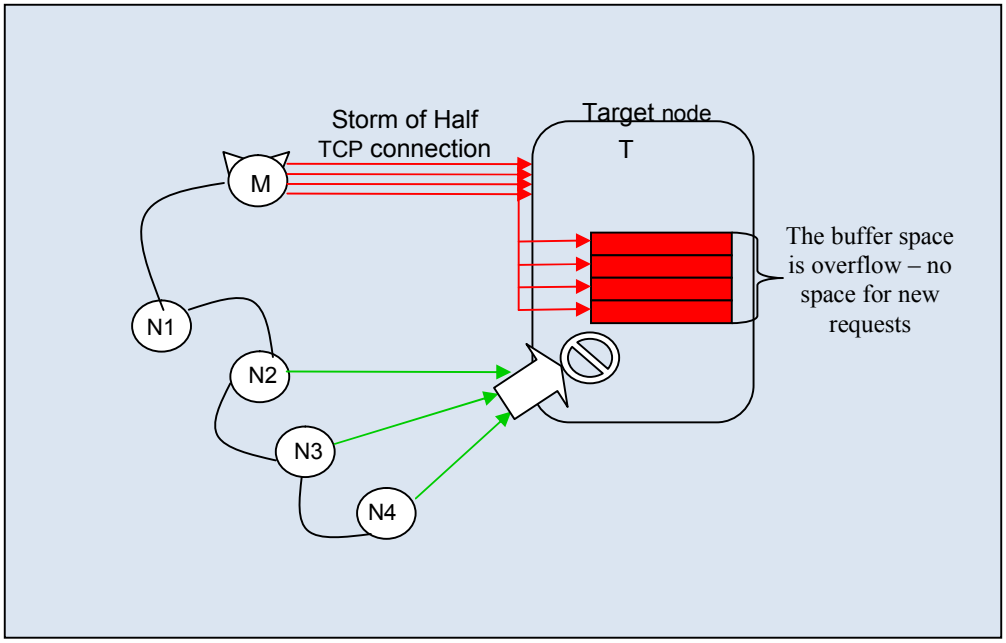

Fig. 5. SYN flooding attack

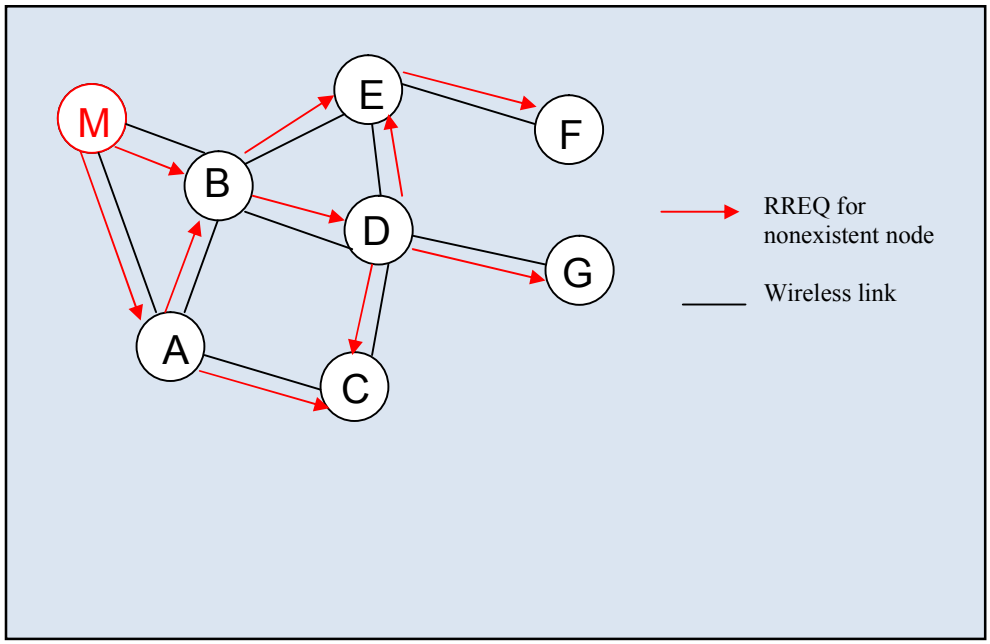

Fig. 6. Flooding process

2.19 Jellyfish Attack

In this attack a malicious node makes unreasonable delay for all the packets that were received for some amount of time before forwarding it [26]. Jellyfish attacker aims to increase end-to-end delay

and make high delay, jitter, which affects the normal performance of the network. Obviously this is a denial of service attack.

2.20 Rushing Attack

There are some on-demand routing protocols that use the duplicate suppression technique. In this technique during the route discovery process if any node receives the same route request packet (RREQ) more than one time, it automatically discards this duplicate packet. The attacking node exploits this vulnerable technique by flooding the network quickly by the route request it receives so as to reach the destination before the same route request reaches the destination through other nodes. As a result the destination will discard the later legitimate request rather than process it [27].

The attacker this way will be on the route that will be used by the source to transmit its packets to the destination. And therefore any possible malicious act can be carried out, such as dropping packets, delaying forwarding, revealing or modifying packets.

2.21 Link Withholding Attack

In the link state routing protocols [28], each node provides information about the state of the links with its neighbors. In this attack the malicious node pays no attention for the provision of information about a specific link, this leads to lose the link and will affect the routing operation seriously as well as prevent the availability of the network services [29].

2.22 Colluding Misrelay Attack

In this attack multiple malicious nodes work together to affect the routing operation by modifying or dropping the routing packets [30].

2.23 Nodes Isolation Attack

Here the attacker attempts to isolate the target node from communicating with other nodes in the network by preventing its routing information to be disclosed [31]. Any node in the network doesn't have any information about the target node to interact with it because the attacker drops all routing information that belongs to the target node. Thus, this attack targets availability.

2.24 Blackmail Attack

This attack attempts to exploit the vulnerability in some routing protocols that use a mechanism to keep track of malicious nodes in the network by maintaining a black list in any node that records any malicious node in the network. Any node that detects a malicious node, it propagates a message in the network and other nodes in the network update its own blacklist of records the new malicious node.

The attacker use this property in the routing protocol to propagate a fake message to claim that a legitimate target node is a malicious node and due to this message all nodes in the network records this target node in their blacklist as malicious node, and thus the target node is isolated from the network [30] and becomes unavailable.

2.25 Cloning Attack

This attack is also called node replication attack in Wireless Sensor Networks. In clone attack the attacker just targets only some nodes to replicate them and then places many numbers of replicas

all over the network [31] that means there are many copies from one node in the network. The difficulty is to differentiate between a clone node and the original node since they are typical and they have the same information. This will result in delays in reaching the correct node or even losing the way they reach the correct node.

2.26 Desynchronization Attack

In any transmission operation there is a possibility of losing some of packets due to network failure or any network error, in this case, nodes which participate in the connection send a request for retransmission of the missed packets. In this attack, the attacker target availability by constantly passes messages to one or both of the end nodes [31]. Thus, these messages will be transmitted again and if the attacker keeps the timing properly, it can prevent the participating nodes from exchanging the data. This will lead to resource consumption of these nodes and damage the transmission operation.

2.27 Routing Information Attacks

There are many attacks that can be classified as routing information attacks, any one of them can target the routing operation attributes which affect the availability of the service, or data integrity by providing incorrect routing parameters such attacks include; Routing Table Overflow [32], Routing Table Poisoning, Route Cache Poisoning [32] and Link Spoofing Attack [28,33,29].

2.28 Session Hijacking Attack

The connection oriented transport protocol TCP, protects communications by providing credentials such as the IP address only in the setup of the session and assign a sequence number to any packet during the transmission operation. In this attack the adversary impersonates the victim node by spoofing the victim's IP address, determines the correct sequence number that is expected by the target. So the attacker can gain access to confidential information.

2.29 Botnet Attack

In botnet attacks [34,35,36], the goal of a Botnet based DDoS attack is to cause damage on the victim side. The attacker controlled a single machine using a malware code. The infected machine can be used further to discover and infect another machine connected and so on. The attacker, thus gradually prepares an attack network called a botnet.

Depending upon the attacking code the compromised machines are called Masters/Handlers or zombies. Hackers send control instructions to masters, which in turn control zombies. The zombies under the control of masters/handlers transmit attack packets which converge at the victim to exhaust its resources.

3 Previous MANET Attacks Classifications

In [5,6] the authors have discussed the issue of misbehavior of nodes at the Medium Access Control (MAC) layer and made an attempt to classify attacks at that layer. Also [7,8] classify attacks on the application layer. In [4,3] attacks are classified according to TCP/IP layers application, transport, network, data link and physical.

In [9], the authors have classified attacks based on the types of attack packets into data traffic attacks and control traffic attacks. Attacks under the first category targeting the data packets, such

as black hole attack which drop the data packets, but the attacks under the second category target the control packets used in the different routing operations.

In [10], security attacks classified as passive attacks and active attacks, the passive attacker tries to analyze, monitor or use the information and do not involve any alteration of the data so it is very difficult to detect. The active attack attempts to involve some modification or fake date and it is subdivided into four categories: modification of messages, masquerade, replay, and denial of service.

In [11], attacks are classified as internal and external attacks. External attacks are typically active attacks that are targeted to cause congestion, propagate incorrect routing information, prevent services from working properly, or shut them down completely.

Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as authorized parties and are thus protected by the security mechanisms in the network and its services offer. Thus, such malicious insiders, who may even operate in a group, may use the standard security means to actually protect their attacks.

In [12], the authors classified attacks against ad hoc routing protocols, in particular, against AODV, according to goals for a secure ad hoc network, i.e. authentication, non-repudiation, availability, integrity, confidentiality and privacy.

4 Attacks Classification Based on Targeted Security Service

There are three main security services that should be achieved to provide a secure environment which is defined by NIST in FIPS 199 [37], namely, confidentiality, integrity and availability, which represent the key security objectives for any information systems.

Due to the nature of MANET that was discussed in section 1, and the existence of a large number of attacks as discussed in section 2, it is very difficult to achieve these security objectives.

In order to achieve security services in a MANET environment, it may be adequate to classify attacks, according to the security service the attacks compromise. Accordingly, we propose to classify attacks to three classes; confidentiality attacks, integrity attacks and availability attacks.

4.1Confidentiality Attacks

Confidentiality is defined as “preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information” [37].

Based on confidentiality definition we classify numerous attacks which target disclosure of information as confidential attacks. Based on the description of attacks in section 2, Table 1 shows the attacks that are classified as confidential attacks.

4.2 Integrity Attacks

Integrity is defined as “guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity” [37]. Based on the description of attacks in section 2, Table 1 shows attacks that are classified as integrity attacks.

Table 1. Classification table

Attack name	Confidentiality	Integrity	Availability
Wormhole	√	√	√
Eavesdropping	√	X	X
Traffic monitoring and analysis	√	√	√
Location disclosure	√	√	√
IP spoofing	X	X	√
Sybil	X	X	√
Modification	X	√	X
Fabrication	X	√	X
State pollution	X	X	√
Data corruption	X	√	√
Replay	√	√	√
Jamming	X	X	√
Black-hole	X	X	√
Grey-hole	X	X	√
Resource consumption	X	X	√
SYN flooding	X	X	√
Byzantine	X	X	√
Flooding	X	X	√
Jellyfish	X	X	√
Rushing	√	√	√
Link withholding	X	X	√
Colluding misrelay	X	√	√
Node isolation	X	X	√
Black mail	X	X	√
Cloning	X	X	√
Desynchronization	X	X	√
Routing	X	√	√
Session hijacking	√	X	X
Botnet	X	X	√

4.3 Availability Attacks

Availability is defined as **"**ensuring timely and reliable access to and use of information" [37]. So any attack that aims to prevent or reduce the availability of information or services is an availability attack or a denial of services (DoS) attack. Based on the description of attacks in section 2, Table 1 shows the attacks that are classified as availability attacks.

5 Conclusion and Future Work

In this paper a brief introduction to the characteristics of mobile ad hoc networks (MANETs) is presented and a comprehensive survey for MANETs attacks is given. Based on the network security services targeted by attacks, a new classification scheme has been proposed.

The proposed classification will make it easier for MANETs security administrators understand the common features of attacks that target a specific security requirement, that is, confidentiality, integrity and availability and to counter theses attacks classes to achieve the desired security requirement.

Our future work is to determine the inherent relationships between attacks of each class and to define the features of the corresponding detection techniques.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Perkins C. Ad Hoc Networks: Addison-Wesley; 2001.

[2] Chlamtac I, Conti M, and Liu J. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks Journal, Elsevier. 2003;1(1):13–64.

[3] Wu B, Chen J, Wu J, and Cardei M. A survey on attacks and countermeasures in mobile Ad Hoc Networks. Springer; 2006.

[4] Al. Kh. Pathan. Security of self organizing networks MANET, WSN, WMN, VANET. CRC Press; 2010.

[5] Guang L, Assi C. On the resiliency of mobile ad hoc networks to MAC layer misbehavior. In Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Warless Ad Hoc, Sensor and Ubiquitous Networks. Montreal, QC, Canada; 2005.

[6] Cardenas A, Radosavac S, Baras J. Performance comparison of detection schemes for MAC layer misbehavior. In Proceedings of 26th IEEE International Conference on Computer Communication. Anchorage, AK; 2007.

[7] Leinmuller T, Schoch E, Kargl F, Maihofer C. Improved security in geographical Ad Hoc routing through autonomous position verification. In Proceedings of the ACM Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, USA. 2006;57-66.

[8] Yang Y, zhu S, and Cao G. Improving sensor network immunity under worm attacks: A software diversity approach. In Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing. Hong Kong SAR, China. 2008;149-158.

[9] Bhattacharyya A, Banerjee A, Bose D. Different types of attacks in mobile ADHOC network: Prevention and mitigation techniques. Department of Computer Science & Engineering, Institute of Engineering & Management Saltlake.

[10] William Stallings. Cryptography and Network security principles and practice. 5th Ed. Pearson Education; 2011.

[11] Mohammad Ilyas. The handbook of ad hoc wireless. CRC Press LLC; 2003.

[12] Vigna G, Gwalani S, Srinivasan K, Belding-Royer E, Kemmerer R. An intrusion detection tool for AODV-based Ad hoc Wireless Networks. University of California, Santa Barbara.

[13] Rutvij H, Ashish D, Jatin D, and Bhavin I. MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security. 2010;10(4).

[14] Hu YC, Perrig A, Johnson D. Wormhole attacks in wireless networks. IEEE JSAC. 2006;24(2).

[15] Hoang Lan, Uyen Trang Nguyen. Study of different types of attacks on multicast in mobile Ad hoc networks. Proceedings of IEEE ICNICONSMCL; 2006.

[16] Borisov N, Goldberg I, Wagner D. Interception mobile communications: The insecurity of 802.11. Conference of Mobile Computing and Networking; 2001.

[17] Computer Emergency Response Advisory Team. TCP SYN Flooding and IP Spoofing Attacks. CA. 1996;21.

[18] John R, Douceur. The Sybil attack. Revised Papers from the First International Workshop on Peer-to-Peer Systems. 2002;251-260.

[19] Manjeet Singh, Gaganpreet Kaur. A survey of attacks in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 2013;3(6).

[20] Hung-Min Sun, Shih-Pu Hsu, Chien-Ming Chen. Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks. Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops. 2007;1:457-462.

[21] Al-Shurman M, Yoo S, Park S. Black hole attack in mobile Ad Hoc networks. ACM Southeast Regional Conference; 2004.

[22] Ruchita M, Seema L. Review paper on flooding attack in MANET, Int. Journal of Engineering Research and Applications. 2014;4(1).

[23] Awerbuch B, Holmer D, Nita-Rotaru C, Rubens H. An on-demand secure routing protocol resilient to Byzantine failures. Proceedings of the ACM Workshop on Wireless Security. 2002;21-30.

[24] Network Working Group. TCP SYN Flooding Attacks and Common Mitigations. Request for Comments: 4987; 2007.

[25] Haining W, Danlu Z, Kang G. Detecting SYN flooding attacks. IEEE INFOCOM, New York City; 2002.

[26] Purohit N, Sinha R, Maurya. Simulation study of black hole and Jellyfish attack on MANET using NS3. IEEE International Conference on Current Trends in Technology; 2011.

[27] Hu Y, Perrig A, Johnson D. Rushing attack and defense in wireless Ad Hoc network routing protocols. Proc. of the ACM Workshop on Wireless Security (WiSe). 2003;30-40.

[28] Cédric A, Emmanuel B, Philippe J. Link state routing in wireless Ad-Hoc networks. Institute National De Recherche En Informatique Et En Automatique; 2003.

[29] Bounpadith K, Hidehisa N, Yoshiaki N, Nei K. A survey of routing attacks in mobile Ad Hoc networks. IEEE Wireless Communications; 2007.

[30] Rishabh J, Charul D, Meenakshi. A survey of protocols and attacks in MANET Routing. International Journal of Computer Science and Management Studies. 2012;12(3).

[31] Rajani M, Lisa A. Jamming attack detection and countermeasures in wireless sensor network using the ant system. Wireless Sensing and Processing Conf; 2006.

[32] Mbarusimana C, Shahrabi A. Comparative study of reactive and proactive routing protocols performance in mobile Ad Hoc networks. Advanced Information Networking and Applications Workshops, 21st International Conference. 2007;(2):21-23.

[33] Clausen T, Jacquet P, Optimized Link State Routing Protocol (OLSR), RFC 3626. Available: https://www.ietf.org/rfc/rfc3626.txt

[34] Shang Y. Optimal attack strategies in a dynamic botnet defense model. Applied Mathematics and Information Sciences. 2012;6:29-33.

[35] Lavanya A, Saravanan K. Areview of DDoS attacks in mobile Ad-Hoc networks. International Journal of Societal Applications of Computer Science. 2012;1(1).

[36] Alomari E, Manickam S, Gupta BB, Karuppayah S, Alfaris R. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. International Journal of Computer Applications. 2012;49:24-32.

[37] Standards for Security Categorization of Federal Information and Information Systems. Federal Information Processing Standards Publication; 2004.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=1030&id=6&aid=8450