A Study and analysis of detection and countermeasures against the attack in MANET

Ms.S.R. chavan, Dr. S.S.Sherekar, Dr V.M.Thakre, Dr.N.B.Raut

Abstract- **Security is one of the most challenging issues in Mobile Ad hoc Network (MANET) due to the lack of centralized authority and limited resources. In our daily life Mobile Ad Hoc Networks are being used in more applications such as business application, remote areas, personal area networking and battlefield. Mobile Ad Hoc Network is easy to deploy and useful when the infrastructure is absent, destroyed or impractical. In mobile ad hoc networks nodes communicate with each other through insecure wireless link, security is very essential for this type of network. Mobile Ad Hoc Network is vulnerable to attacks, such as Distributed Denial of services (DOS) attack, Sybil attack, Blackhole attack, Grayhole attack, Wormhole attack and Spoofing attack. The paper discusses the detection techniques against attacks and Network attacks in mobile ad hoc network and their different classification. Various countermeasures are used to overcome the numerous attacks in mobile ad hoc networks.**

Keywords- **Attacks, MANET, Detection, Analysis, Classification, Countermeasures.**

I. INTRODUCTION

The Popularity of Wireless local Area Networks is increasing day by day. Wireless local area networks are widely used in both home and business computer networks. Wireless local area networks provide mobility advantage to their users so that they can access their information from many locations. A Mobile Ad Hoc Networks is a self organized and directions from web servers under the assailant's control [6]. Accordingly, distinguishing bots with electronic controlling is more unpredictable than bots with IRC-based controlling. In this study, we have experienced different systems for HTTP botnet discovery and techniques utilized in them.

Figure 1: The MANET Architecture

infrastructure less Networks. Mobile Ad Hoc Networks don't need any centralized control over the network to manage the communication. Nodes in a Mobile Ad Hoc Networks create dynamic topology to communicate with the other node. In this network, nodes can directly communicate with any other node laying in their communication range. If one node want to communicate with another node, which is not in the communication, range, this node uses the intermediate node to communicate the distance node. The MANET architecture is shown below in Figure 1. Mobile Ad Hoc Networks provides great flexibility to its users. Due to some fundamental characteristic, such as Dynamic topology, wireless medium, lack of centralized authority, limited Resources, limited Bandwidth, constrained battery life or Open medium. Mobile Ad Hoc Networks is vulnerable to various types of security attacks. Security is the most challenging issues in Mobile Ad Hoc Networks. In MANET security issues are included routing security, data forwarding security, link layer security, key management, and intrusion detection. In general five security goals are needed for reliable and secure communication in MANET, Confidentiality, availability authentication, integrity, and nonrepudiation [1, 2].

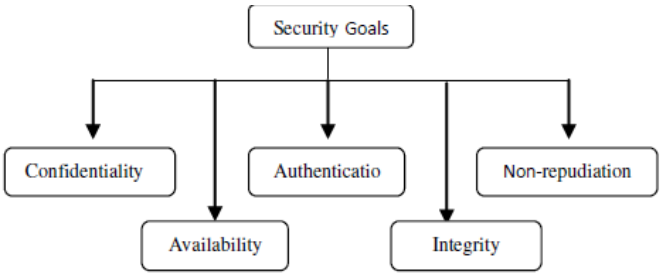

Figure 2: Types of Security Goals

Confidentiality means that data should be kept secret and only authorized person can be able to access the network data. Due to Multi hop communication, it is very difficult to keep data confidential. Availability means all the Resources through out the network should be accessible and available for authorized person when required. Data is authenticated when it is originally created, placed, or transferred. In Non-repudiation the sender should not be able to deny that it has transmitted the message and receiver should not be able to deny that it has received the message [2].

II. ATTACKS ON MANET

2.1 Phishing attack In phishing attack, a login environment is shown to the user and attacker can get the user name, password or some credit card information. The pages can be a complete duplicate of some banking website and attacker can get the user id and password easily by just one click.. Usually

email passwords are hacked by this method. An attachment when opened, the user gets the message of being logout and asked for re-login. Which is shown by a fake page duplicate of the original login page? A fake website is shown when users try to access a website. The website shown is similar to genuine website even having the images and also the logos shown in original [3].

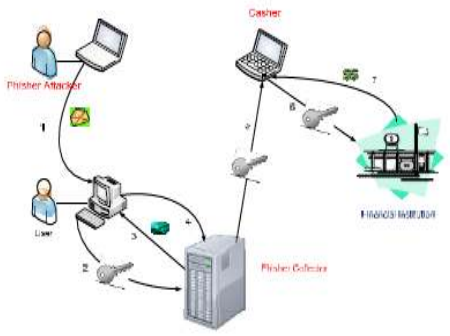

Figure 3: Phishing Attack

2.2 *DDOS attack* DDOS attack one of the most severe threats existing in the internet, refers to using a puppet host to consume the computing resources of its target and prevent the target from providing services for its users. In the early days of the Internet, DDOS attacks did not attract enough attention because of the smaller range of the network and the relatively smaller number of service providers. But with the rapid development of the Internet and its continuous expansion, especially in the rapid development of cloud computing, the representative of the emergence of new computing model, an attacker can implement DDOS attacks in a very short period of time, via a large number of virtual Machine rent with less money from cloud service provider [4].

2.3 Cloning attack Cloning attack is the malicious attack in Online Social Networks. While opening the face book or twitter, everyone will post photos and update the status. Attacker mostly creates fake identities like the real one and sends a friend request to their friends. If those have accepted the friend request they are visible to the attacker, they may get easily cloned by the attacker, and continue to send friend request to the people in the friend list. Another enhancement is that the user accepts the request; an attacker will easily collect more information about the person. Then the cloning account will be created using the detailed profile and showing genuine to others. Some traditional fake identities are easily identified by ordinary users such information like school, college, and date of birth [5].

2.4 Replay Attack social networking sites frequently suffer from security attacks, due to some popular features such as open access channel, dynamically changing topology and wireless system. In MANET Dynamically topology means that topology in the current network might not be present in the future. In Replay attack attacker continually retransmits valid information to the network that has been previously captured or hold information for some period of time and then resend [5].

2.5 Man In The Middle The Man-In-The-Middle (MITM) attack is one of the most well known attacks in computer security, representing one of the biggest concerns for security professionals. The effect of these attacks varies between sender and receivers that targets the actual information flows between them and the confidentiality and integrity of the data itself. MITM attack is also known as: Monkey-in-the middle attack, Session hijacking, TCP hijacking, TCP session hijacking. At the application layer these attack launched in the form of spoofing –based MITM in which the attacker captures actual information flows between two hosts while hosts are not aware of a middle man existence. MITM attack lunched on Transport and Network layer in the form of IP spoofing-based MITM. IP spoofing-based MITM is an attack where a malicious party intercepts a legitimate communication between two nonmalicious parties. At the data link layer MITM occurred in the form of ARP spoofing attacks. ARP spoofing attack may be worked in two ways, cheating the gateway, and cheating the host of the internal network [6].

2.6 Sybil attack In Sybil attack, attacker creates more than one identity on social networking sites; entities do not have any physical information about other entities. The only one manner to recognize them is by some informational abstractions called identities. In these types of system different entities have distinct identities. When an entity send data to multiple identities it can be detected as single entity with multiple identities. The additional identities are known as Sybil node. This fabrication of multiple identities is known as Sybil attack. It decreased the performance of the networks and disturbs the transmission process [7, 8].

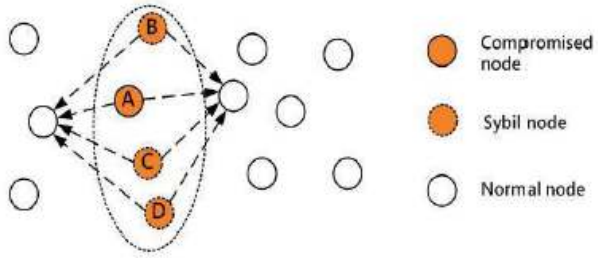

Figure 4: Sybil Attack

2.7 Packet dropping Attack A path between a source node and a destination node in a MANET is established using a route discovery process. 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 [9].

2.8 Flooding Attack Basically, this attack targets Reactive Routing Protocols (On Demand). In reactive routing protocol route is established by flooding method. But in flooding attack, attacker used flooding to disturb the transmission is called flooding attacks. In MANET flooding is making use of find the path in between the source to destination.

In Manet malicious nodes using flooding for mislead the communication between the nodes and try to exhaust resource of the node. The main aim of this attack is include: consume the resource of the node, consume bandwidth or battery power and disturb the transmission system. Due to this consumption of network resources performance of the server dirges [10].

2.8 Wormhole Attack MANET is becoming more popular for their easy deployment. These Networks are vulnerable to attackers due to high availability and the lack in security measure of their routing protocol. Wormhole Attack in the MANET works against two different types of Protocol; such as networking routing protocol and location based protocol. Wormhole attack is very serious thread in wireless network. In the wormhole Attack, attackers records packets at one location and tunnel them to another location in the network, and retransmit them there in to the network. During the transmission of the packet, attackers use the different path which does not exist in the actual network. Due to using the different path is very difficult to detect the wormhole attack in the MANET [11].

2.9 Blackhole Attack Blackhole is a very common attack in MANET. In Blackhole attack a malicious node can attract all packets by claiming itself of being the shortest and fresh route to the destination node and drop them without forwarding them to the destination. . Due to this, packet delivery ratio gets decreased and all resources utilizations wasted. In black hole attack. Malicious node fully utilizes the routing protocol [11].

III. DETECTION TECHNIQUES AGAINST ATTACKS ON MANET

In proposed a secure trust-based scheme against packet dropping attacks in MANETs. This scheme combines social and QoS trust. The main target of this proposed scheme is to mitigate nodes performing various packet forwarding misbehaviours. Basically four parameters calculated for trusts which are control forward ratio, data forward ratio, intimacy and residual energy. Then finally present adversary model of the packet dropping attack against which our trust-based scheme is evaluated [9, 10, 11]. In proposed security approach is to detect and mitigate wormhole attack. It is secured Ad hoc on demand distance vector (AODV) approach which efficiently finds wormhole attack present in a MANET and Digital signature is used to prevent it. This approach is based on a calculation of tunnelling time taken by tunnel to analyze the behaviour of wormhole. Afterward, it decides some static threshold value. Based upon this tunnelling time and threshold value, it decides whether given node is wormhole node or trustworthy node. This approach provides QoS up to a satisfactory level and removal of unwanted errors occurs in the wormhole detection are still open issues [11]. In proposed a RSS- based lightweight scheme to detect the new identities of ybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system. This scheme works on MAC layer using the 802.11 protocol .The concept of received signal strength (RSS) used to differentiate between the legitimate and Sybil identities. This scheme detects the Sybil attack identities with good accuracy by the help of simulations and real-world tested experiments [12]. In Novel Based strategy was proposed to detect the black hole attack in MANET. This approach decreased routing and computational overhead also. Using ADSN, black hole list and next hop information extracted from RREP, the D-CBH algorithm creates a list of collaborative black hole nodes [12]. In this paper, we propose a new approach to protect against phishing attacks with "bogus bites" on the basis of the two observations was mentioned. Bogus Biter is transparent to users, At a user's Web browser, Bogus Biter is turned on once a login Web page is classified as a phishing page by a Web browser. For a victim who is beguiled into divulging a real credential, Bogus Biter hides the real credential among a set of automatically generated bogus credentials, and then submits these credentials one by one to the phishing site. For a security conscious user who does not reveal a real credential, Bogus Biter also generates a set of bogus credentials, and then submits them to the phishing site. At the phishing site, a phisher will thus receive a much larger number of credentials than before, but the overwhelming majority are bogus credentials fed by Bogus Biter. Elaborating bogus credential generation and submission mechanisms, Bogus Biter makes it difficult for a phisher to distinguish who are real victims and which are real credentials. The only effective way for a phisher to sift out bogus credentials is to visit the legitimate Web site and verify whatever credentials have been collected from the phishing site[13]. A statistical approach was proposed to defence against RREQ flooding attacks in MANETs. This detection mechanism can be applied on AODV-based ad hoc networks and used real-time monitoring of received and generated RREQ messages of each node in the network.

S.NO.	Attacks	Mode of attack	Security Approach	Source of Data	Protocol	Simulator	Advantages	Limitations	Countermeasure
	Wormhole	Tunnel between malicious nodes	Angle Based Scheme	Tunnelling time and threshold Value	AODV	NS2	Successfully Defend against wormhole attacks	-	Algorithm using analytical hierarchy process (AHP) methodology
	Blackhole	Fake optimum route message	D-MBH Algorithm	Information extracted from RREP	AODV	-	Reduce computational and routing overhead	Storage overhead	Cluster Based Scheme
	Sybil	Creates multiple identity on a single device	lightweight scheme	RSS Value of the Node	802.11	NS2	High degree of accuracy& Does not required additional Hardware	Not Define	lightweight scheme
	Flooding	Mislead the communication between the nodes	noncryptographic security approach	RREQ messages of the node	AODV	NS2	Detect attacks in large networks	Not Define	SLICOTS Mechanism
	Packet Dropping	Drop the packets instead of forwarding them	Trust Based Scheme	Trust value of the node	AODV	NS2	Improve the packet delivery ratio	More Parameters are Required for improvement of the result	Accurate Algorithm
	Phishing	Bogus biter creates fake identity	Trust Based (DTD) detection Scheme	Trust value of the node	AODV	NS2	Not Define	Not Define	DTD algorithm

K.S. Arathy, C.N. Sminesh was analyzed the computational, routing and storage overhead of the Black hole attack detection D-MBH Algorithms with the existing Fidelity, DRI and Trust based schemes and found that this approach reduced the computational and routing overhead. But there is no substantial improvement in storage overhead compared to the existing schemes. T. N. D. Pham and C. K. Yeo was proposed destination sequence number based SNBDS detection scheme for AODV protocol to counter grayhole attack during route discovery phase. Performance of the scheme analyzed under three grayhole adversary models taking different mode of operations. Simulation result with various network parameters show that the proposed scheme improves the network performance To detect the Sybil attack,S. Abbas, M. Merabti, D. Llewellyn-Jones used Network Simulator NS-2.30 in which it used the parameters like Speed, accuracy, area ect.They proposed lightweight scheme for detection of the attack. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and D. Gaiti proposed the non cryptographic security approach for detecting Sybil attack using NS2 network simulator. To detect Packet Dropping attack T. Shu and M. Krunz was proposed Trust based scheme which is simulated using NS2.

V. CONCLUSION

Mobile Ad Hoc Networks have vast potential and the ability to establish networks on the fly in a harsh environment, still there are many challenges left to overcome. Security is an essential feature for deployment of MANET. This paper introduces the fundamental Characteristics and Security Goals of Mobile Ad Hoc Network. In this paper, we discuss about various attacks and classified as an active or passive attacks or the other classification is clear that how different layer protocols become vulnerable to attacks. We examined that Active attacks are more dangerous as compared to Passive attacks because they disturb the normal operation of the MANET. Different detection and Prevention techniques are introduced for the mitigation of attacks. It can also Outlined countermeasure used to protect mobile ad hoc network from various attacks. Analyzed different detection techniques against the network attacks and discuss their advantages and limitation, mode of attack, security approach, protocol, and simulator. Elimination of these limitations enhances the accuracy of detection methods and improves performance of the Mobile Ad Hoc Network.

REFERENCES

1. H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra, "Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET",10th International Conference on Sensing Technology (ICST), Nanjing, 2016, pp. 1-6. 2. N.

2. Alomar, M. Alsaleh and A. Alarifi, "Social Authentication Applications, Attacks, Defense
Strategies and Future Research Directions: A Systematic Review," in IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1080-1111, Second quarter 2017.
3. A. Waheed, M. Ali Shah and A. Khan, "Secure login
protocols: An analysis on modern attacks and solutions," 2016 22nd International Conference on Automation and Computing (ICAC), Colchester, 2016, pp. 535-541.
4. . B. Meng, W. Andi, X. Jian and Z. Fucai, "DDOS
Attack Detection System Based on Analysis of Users'
Behaviors for Application Layer," 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, 2017, pp. 596 599.
5. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato
and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", in IEEE Wireless Communications, vol. 14, no. 5, pp. 85-91, October 2007
6. . M. Conti, N. Dragoni and V. Lesyk, "A Survey of
Man in the Middle Attacks", in IEEE Communications
Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051,
third quarter 2016.
7. S. Abbas, M. Merabti, D. Llewellyn-Jones and K
Kifayat, "Lightweight Sybil Attack Detection in MANETs", in IEEE Systems Journal, vol. 7, no. 2, pp. 236-248, June 2013
8. J. Zhang, R. Zhang, J. Sun, Y. Zhang and C. Zhang,
"TrueTop: A Sybil-Resilient System for User Influence Measurement on Twitter", in IEEE/ACM Transactions on Networking, vol. 24, no. 5, pp. 2834-2846, October 2016.
9. T. Shu and M. Krunz, "Privacy-Preserving and
Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", in IEEE Transactions on Mobile Computing, vol. 14, no. 4, pp. 813-828, 1 April 2015.
10. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and D. Gaiti, "Flooding attacks detection in MANETs", 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, 2015, pp. 1-6.
11. T. N. D. Pham and C. K. Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks", in IEEE Transactions on Mobile Computing, vol. 15, no. 5, pp. 1116-1129, 1 May 2016.
12. K.S. Arathy, C.N. Sminesh,"A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET", in Procedia Technology,Volume 25 ,Pages 264-271,ISSN 2212-0173,2016
13. Chuan Yue, Haining Wang," ACM Transactions on
Internet Technology (TOIT)",in ACM New York, NY, USA, Volume 10 Issue 2, May 2010, ISSN: 1533-5399 EISSN: 1557-6051.