IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A Survey on MANET Attacks and Prevention Schemes

Archie Goel[1], Vimlesh Kumar[2]

School of Information and Communication Technology,Gautam Buddha University, Greater Noida[1,2]

Abstract: Mobile Ad hoc Network (MANET), a wireless network is mainly deployed over a restricted or remote area. The decentralized, self-organized & infrastructure-less design make them more susceptible to various security hazards. One of them is malignant node or selfish node attack. In this paper, a survey is done on several techniques to lessen these attacks by making network more secure and enhancing the overall performance of the network.

Keywords: MANET, survey, security services, attacks, defense mechanisms.

I. INTRODUCTION

The formation of wireless mobile networks by some well-equipped devices like PDAs, Laptops, GPS receivers, etc. is done which makes the network ubiquitous & more attractive. Due to their highly dynamic & mobile nature, the network is independent of any fixed infrastructure.
MANETs are temporal network of mobile inter-connected through wireless links.

In MANET, nodes ensure their role as both Server and Router with finite resources which is a challenging task. This resource constrained operation increase its vulnerability towards attacks.

The networks without central administration are an easy prey for the attackers. A survey is done on the various security hacks inferring the MANET & their techniques proposed.

A. Security Services

For securing MANET, some goals [1] are need to be met. A tradeoff between these goals or services must be provided which depends on network application, i.e., if one service assures without taking note of other services, the security system will break down.

1. Confidentiality- This service is very broad and encloses whole message or a part (digest) of a message making it confidential against traffic analysis attack. Due to lack of central administration in MANET key distribution is a bit challenging as this service is provided using Encryption methods.
2. Availability- The information (data & services) must be accessed by authorized nodes only in the network. This is ensured by the availability service of MANET. The time required for a node to access information is the Accessing time which is one of the security parameters.
3. Authentication- This service provides realistic communication between two nodes. The identity of nodes should be known to other communicating nodes. The traditional way to provide this service is by issuing certificate which is a bit challenging in absence of any central authority.

   Authors presented a way to public the certificate keys based on Trust & Clustering model [2]. This approach is better than traditional PGP but clustering in MANET is a major drawback due to its dynamic topology and mobile nature of nodes.
4. Integrity- To protect data from modification, deletion, insertion & replaying type of attacks from any adversary Data Integrity services is designed. The adversary captures the data packet in between route and then modifies or removes the packet from the transmitted data.
5. Non-Repudiation- This service protects the data against repudiation by either sender or receiver i.e. the sender or receiver should not refuse a transmitted message.

B. Security Attacks

Before ensuring security for MANET or any other wireless network it is essential to summarize probable kind of attacks.

MANETs are mainly subjected to two types of attack [3]:

1. Internal: As the name suggests, the attack is done internally within the network affecting directly nodes and the interfacing link between them.

Here the attack is performed by a selfish or compromised node, the node may misroute other nodes in the network. The fake or false routing information developed by the malicious node is challenging to detect. As the attacks are conducted through trusted and authorized nodes makes internal attacks more challenging.

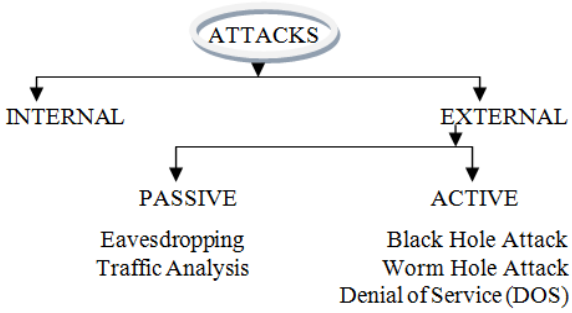
2. External: Nodes performing attack to the network externally is known as external attack. The attacking node does not belong to the communicating network or is not authorized to access to it.

External attacks interrupt the network from usual communication and introduce supplementary overheads.

External Attack maybe subdivided into two categories:

- Passive Attacks
- Active Attacks

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016



MANETs are highly sensitive to Passive Attacks. The attacker eavesdrop the data traffic of the network externally by constantly listening the information. Attacker does not modify data but analyzes to extract information important to the attacker for future use. These types of attacks are challenging to spot. These attacks threaten the confidentiality of MANET.

a) Eavesdropping: The word eavesdrop means overhearing confidentially where a passive node attacks either internally or externally in order to extract useful information by analyzing communicated data. The eavesdropped message or data may be modified or intercepted without disturbing the communication in the network.

b) Traffic Analysis: It is another type of passive attack. The attacker senses the communication pattern between the communicating nodes of the network. Traffic analysis in MANET disclose these information:

i. Current Position of nodes.
ii. Network topology during communication.
iii. The present source and sink of network.
iv. The function performed by the nodes.

Active Attacks another type of external attack that controls the operation of the network by masquerading as one of the communicating node. Active attacks can be done externally by outside node or internally by selfish or malicious nodes which are present in the network but behave selfishly. Active attacks such as DOS (Denial of service), modification of data packets, misrouting, etc. are mostly carried out by selfish or malignant node.

a) Black Hole Attack: The selfish or malicious node affects routing protocols by flooding direct and shortest route through it to extract useful packet. Two types of Black hole attack are discussed.Single Black hole Attack, within the communication range there will be only one malicious or selfish node. Whereas, in Collaborative Black hole Attack there may be multiple nodes creating a malicious group [4].

Black hole Attack possesses two properties:

i. Malignant node affects mostly the reactive routing protocols, such as AODV.
ii. The malignant node ingests the extracted packets without redirecting.

b) Worm hole Attack: Malignant node collects data packets from different point without the network and tunnels them to some other point affecting the routing protocols. The tunnel created between two or more intriguing attackers is termed as Worm hole.

c) (DOS) Denial of Service: The objective of DOS is to threaten the availability of a particular node or the whole network [5]. Thus, the services will become inaccessible.
The paper consists of following sections:

Section I: Introduction of paper followed by
- Security Services
- Security Attacks

Section II: Related work
Section III: MANET vulnerabilities
Section IV: Conclusion of the survey paper

II. RELATED WORK

Malignant or misbehaving nodes deteriorate the potential of routing protocols [6], access control mechanism [7] and address assignment [8].

Previously, research done focus on thwarting malignant behavior [9] but they do not take in to account on securing network as they do not work in the manner spot and penalize the misbehavior of the entity. Some proposed schemes were based on monitoring the neighbors to spot the malicious or misbehaving node and distinguish it from the network.

Lal et al. [10] proposed a watchdog mechanism or protocol to notice the functioning and behavior. Each entity in the communication range is signed to examine the functioning of its next hop or neighboring node. An improved watchdog protocol is proposed titled as I-watchdog protocol based on two steps: 1. one node authenticates other node by using local information such as packet sending and storing period of the next hop; authentication of nodes is assured along with. Watchdog serves as efficient IDS for MANET but this mechanism fails in some of these conditions:

- Obscure collision in the network or at the sink.
- Confined transmission power.
- Partial dropping of packets.
- Fake malicious report generation.

Augustine et al. [11], a watchdog mechanism along with an acknowledgement scheme is proposed to detect Black Hole attack in MANET. Black hole attack is imported mostly in ON-Demand routing protocols like AODV. In the proposed scheme, when source sends a packet it waits for an acknowledgement packet from the sink.

If source receives an acknowledgement then the packet transmission is successful. If there is any assaulter in the network, it gets detected by watchdog and then alarm message is produced and flooded in the network.

Shamaei et al. [12] proposed a two-phase detection scheme to detect and prohibit wormhole attack. First phase ensures that if there is any wormhole tunnel in the selected path or not. If there is any, the second phase is activated to approve the presence of wormhole attack and diagnose malignant node. The source forwards data packets on the suspected path and waits for a pre-defined time period. If

DOI 10.17148/IJARCCE.2016.5415

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

this time expires, the suspected path is assumed to be safe and all node lying on the path disables the abandoned node meanwhile all nodes lying in the suspected path buffers the IP header of the received packet if the transmitted packet header by the abandoned node does not match with buffered one during that period then it is considered as wormhole node. A tradeoff is maintained for considering the value of time period, as to small value may increase the false positive rate. Otherwise, energy consumption and delay will increase.

In another paper Shiyu et al. [13] proposed, Firstly a centralized algorithm is proposed to identify the wormholes leveraging a centric node in the network. Then DAWN is proposed, a Distributed detection Algorithm against Worm hole for the distributed wireless network coding systems DAWN do not depend on any position report, global synchronization assumption or specific hardware or middleware. It only depends on local information that can be collected from network coding protocols. In DAWN, meanwhile usual data transmission each and every node files the anomalous influx of new envelopes and split this information in the network. Due to DAWN based on less assumptions it is more efficient. This solution though practical and efficient but is expensive and overheads can be problematic if the network is highly dense.

To mitigate the effect of DOS attacks Nadeem et al. [14] proposed an anomaly based intrusion detection system that uses a combination of chi-square test and control chart to detect intrusion and then identifying the intruder. In AIDP, control packet overheads are reduced and throughput of the network is increased gradually. The limitation of AIDP mechanism is that it does not take into account other factors related to include or cover other routing attacks.
Mamatha et al. [15] proposed as IDS based on anomaly intrusion detection that checks the behavior of the nodes and for that Data Transmission Quality function is used. The DTQ for absolute nodes will be constant or slightly change but will diminish for malignant node. High detection rate is achieved even in the presence of more malicious node. But this IDS is limited for internal attacks only.

Fernandes et al. [16] A Controller-node based Access-Control mechanism for Ad hoc network (ACACIA) is proposed, a self-organized and de-centralized or distributed access control mechanism controlling the authentication of nodes and eject the malignant nodes. The controller nodes acculturate to the network changes by altering ACACIA parameters. The nodes performing ACACIA are randomly chosen. The scheme also uses a neighborhood watch mechanism which invariably induces accusation packets to the randomly selected controller nodes. Then, these nodes evaluate a reputation value to the nodes which depend on the arriving number of accusation packets and ejects the nodes with less or low reputation. The drawback of this scheme is the large control message overhead and the inflexibility towards different network status as low reputation accuracy was calculated for different neighbors generating different reputation values.

Ferraz et al. [17] proposed the Trust-based Exclusion Access-control Mechanism (TEAM). TEAM uses a two-level trust and reputation system motivated by jury trial which is self-coordinated and robust. The system performs the following function:

- Controls node access to the network.
- Monitors neighboring nodes and their behavior.
- Ejects misbehaving ones.

TEAM extends the ACACIA and only well-being nodes are allowed to access network. A trust model [18] is used to assign nodes behavior a trust value and ejecting the ones having value below a certain threshold more precisely and efficiently. Control overheads are also reduced as the decision made is Global by jury set which are randomly chosen. TEAM distributes its access control in two-level context: Local context concerning the vicinity of nodes and the global context concerning whole network. Local context monitors the neighboring nodes and sends evidences to the jury this is done by three modules namely: monitor, trust and evidence. Global context consists of dynamic jury which is self-organized based on voting scheme to eject the misbehaving nodes.

Name of Attack	Description of attack	Defense mechanism	Description	Drawbacks
Eavesdropping	Overhearing of data packets	I-watchdog	1.Authentication of nodes 2.Observes action of neighboring nodes	1.In presence of obscure collision 2.Partial dropping of packets
Black hole attack	Malignant node extract packet by re directing shortest route through it	Watchdog with acknowledgement scheme	Alarm message is flooded if acknowledgement is not receive and gets detected by watchdog	Additional delay and overheads
Worm hole attack	Two disunite rivalries underpasses the data packets	1.Two-phase detection system 2.DAWN	1.1st phase detects wormhole in the suspected path then 2nd phase diagnose malignant node 2.Each node files the anomalous influx of new envelopes	1.Tradeoff for predefining the value of time period 2.Expensive and overheads in highly dense network
DOS(Denial of Service)	Users are deprived of services	1.Adaptive Intrusion Detection System(AIDP) 2.Enhanced IDS	1.Combination of Chi-square test and control chart detects intrusion 2.DTQ function is used	1.Other routing attacks are not considered 2. Limited to internal attacks only
Malignant Node		1.ACACIA 2.TEAM	1.Controller nodes handles node's access to the network and eject malignant nodes 2.Two-level trust and reputation based malignant node exclusion mechanism	1.Low accuracy

Table 1. Comparison of Attacks and their defense mechanisms

III. MANET VULNERABILITIES

Vulnerability means exposure to problems. MANET are highly vulnerable than cabled networks. The following vulnerabilities of MANET [19] are weakness in security system.

1. De-centralized administration: Due to their dynamic nature MANET are independent of any central administration. The absence makes the attack detection a bit difficult as it is not simple to monitor the traffic.
2. Resource scarcity: Resource scarcity is one of the primary concerns in MANET like power supply, Band-width. Dynamic topology and resource constraint leads to the development of self-organized and managed security schemes or mechanisms.
3. Scalability: MANET are also known as open network due to boundary less topology changing all the time. Security mechanism has to be capable enough of bearing topology changes.
4. Cooperativeness: For MANET to work properly and effectively the nodes has to be collegial and non-malignant. But malignant attacker may rattle network operation by non-following the protocol.

DOI 10.17148/IJARCCE.2016.5415

5. Lack of clear line of defense: Attacks can be possible either externally or internally. Due to lack of clear line of defense it's easy for the attacker to attack in any order.

IV.CONCLUSION

This paper a survey is conducted to highlight some of the security hacks which may infer the working of MANET. Looking forward to the MANET's vulnerabilities towards security concerns several defense mechanisms are also introduced to mitigate the effects of these attacks. A range of these defense mechanisms have been discussed with their drawbacks. Still research is being carried out to classify new threats to MANET and defense against them.

REFERENCES

[1]. Priya, S. Banu, and C. Theebendra. "A STUDY ON SECURITY CHALLENGES IN MOBILE ADHOC NETWORKS." (2016).
[2]. E.C.H.Ngai and L.M.R," Trust and clustering-based Authentication Services in Mobile AdHoc networks, "presented at the proceeding of the 24th international conference on Distributed Computing systems Workshops 2004.
[3]. Navaneethan, T., and M. Lalli. "Security Attacks in Mobile Ad-hoc Networks–A Literature Survey." T. Navaneethan et al, International Journal of Computer Science and Mobile Applications 2, no. 4 (2014): 1-7.
[4]. Kumar, Jaspal, M. Kulkarni, and Daya Gupta. "Effect of Black hole Attack on MANET routing protocols." International Journal of Computer Network and Information Security 5, no. 5 (2013): 64.
[5]. Aggarwal, Ruchi, and Simmy Rana. "A Comparitative Survey on Malicious Nodes and Their Attacks in MANET." IOSR Journals (IOSR Journal of Computer Engineering) 1, no. 16: 93-101.
[6]. R.P. Laufer, P.B. Velloso, L.F. Vieira, L. Kleinrock, Plasma: a new routing paradigm for wireless multihop networks, in: IEEE INFOCOM'12, 2012.
[7]. S. Zhu, S. Xu, S. Setia, S. Jajodia, LHAP: a lightweight network access control protocol for ad hoc networks, Ad Hoc Netw.4 (2006) 567–585.
[8]. Fernandes, Natalia Castro, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte. "An efficient filter-based addressing protocol for autoconfiguration of mobile ad hoc networks." In INFOCOM 2009, IEEE, pp. 2464-2472. IEEE, 2009.
[9]. Mahendran, S. K. "Perfect Malicious Node Avoiding Mechanism for Mobile Ad-Hoc Networks." (2014).
[10]. Lal, Nidhi, Shishupal Kumar, Aditya Saxena, and Vijay Km Chaurasiya. "Detection of Malicious Node Behaviour via I-Watchdog Protocol in Mobile Ad Hoc Network with DSDV Routing Scheme." Procedia Computer Science 49 (2015): 264-273.
[11]. Alfy Augustine and Manju JamesS, Black Hole Detection using Watchdog IJCET, Vol.5, No.4 (Aug 2015).
[12]. Shamaei, Shiva, and Ali Movaghar. "A Two-Phase Wormhole Attack Detection Scheme in MANETs." The ISC International Journal of Information Security 6, no. 2 (2015): 183-191.
[13]. Ji, Shiyu, Tingting Chen, and Sheng Zhong. "Wormhole attack detection algorithms in wireless network coding systems." Mobile Computing, IEEE Transactions on 14, no. 3 (2015): 660-674.
[14]. Nadeem, Adnan, and Michael Howarth. "Adaptive intrusion detection & prevention of denial of service attacks in MANETs." In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, pp. 926-930. ACM, 2009.
[15]. Mamatha, S., and A. Damodaram. "Enhanced Intrusion Detection System for Malicious Node Detection in Mobile Ad hoc Networks using Data Transmission Quality of Nodes." International Journal of Computer Network and Information Security 6, no. 10 (2014): 32.
[16]. Natalia Castro Fernandes, Marcelo Duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte, A Self-Organized Mechanism for Thwarting Malicious Access in Ad Hoc Networks in: IEEE INFOCOM'10, 2010.
[17]. Lyno Henrique G. Ferraz, Perdo B. Velloso, Otto Carlos M.B. Duarte, An accurate and precise malicious node exclusion mechanisms for ad hoc networks, Ad hoc networks 19 (2014) 142-155.
[18]. P.B. Velloso, R.P. Laufer, D. de O Cunha, O.C.M.B. Duarte, G. Pujolle, Trust management in mobile ad hoc networks using a scalable maturity-based model, IEEE Trans. Netw. Serv. Manage. 7 (3) (2010) 172–185.
[19]. Goyal, Priyanka, Vinti Parmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." IJCEM International Journal of Computational Engineering & Management 11, no. 2011 (2011): 32-37.