 ISSN: 2321-8169
04 – 08

Multi Layer Attacks on MANET

Mrs. Rinki S. Jain
Research Scholar
SGB Amravati University,
Amravati, India
Email: rinki.jain013@gmail.com

Prof. S. S. Sherekar
Department of CSE,
SGB Amravati University,
Amravati, India
Email:ss_sherekar@rediffmail.com

Prof. V. M. Thakare
Department of CSE,
SGB Amravati University,
Amravati, India
Email:vilthakare@yahoo.co.in

Abstract: Security is an essential service for wired and wireless network communications. The success of mobile ad hoc network (MANET) will depend on people's confidence in its security. However, the characteristics of MANET pose both challenges and opportunities in achieving security goals. In OSI model each layer is prone to various attacks, which halts the performance of a Network. This paper focuses on Multi-layer attacks on MANET.
In this paper several attacks on different layers of OSI model are discussed and described security mechanism to prevent attack in Multi-layer. Discuss about various attacks in Multi-layer, their detection, prevention mechanism and also discuss their countermeasure.

Keywords: *Attacks, MANET, OSI layer, Multi-layer*

*****

I. INTRODUCTION

Mobile ad-hoc networking is a multi-layer architecture that normally involves the physical, medium access layer (MAC), network layer, application layer, data link layer andtransport layer. In MANET node are arranging in self organization manner. Self organization behavior of node includes the task route discovery and topology organization and reorganizations. MANETs are vulnerable in their functionality: attackers can compromise the operation of the network by attacking at any of the physical, MAC or network layers. Due to dynamic wireless networksMobile ad hoc network are very useful in various field such as: emergency search and rescue operation, meeting or conventions in which person wish to quickly share information.Becauseof the dynamic nature, openness of mobile node and no fixed infrastructure for the networkrequired the very high security mechanism to prevent these types of networks [1, 2].

This Paper arraigning as follows: In II section of this paper discuss various types of attacks on MANET at different layers of OSI Model.SectionIII focuses on Multi-layer attacks and their brief description. Section IV discusses detection Methods against multi layer attacks. In section V studyof prevention Methods against multi layer attacks. Section VI various types of defense mechanism to counter these attacks. In section VII focus Analysis and discussion. Finally, conclusion presented in the section VIII.

II. ATTACKS ON VARIOUS LAYER OF MANET

In MANET many types of attacks are possible. MANET is vulnerable to various types of attack. There are lots of attacks which can fall down the security of Mobile ad hoc network. These attacks can be occurred on different layers of the network but some attacks can be occurred on any layer of MANET and others are on a particular layer [3]. Various types of attacks on different layers in MANET areshown in Table I.

Table I.MANET-layered type of attacks

LAYER	ATTACKS
Multi-layer	DoS, impersonation, replay, man-in-the-middle
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, Blackhole Byzantine, flooding,resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping

III. MULTI LAYER ATTACKS

Multi Layer attacks can be launched from several layers instead of a single layer. Examples of multi-layer attacks are denial of service attacks, man-in-the-middle attacks, replay attack and impersonation attack,are given as follows:

A. Denial of service attack

Denial of service attackscould be occurred on several layers. Due to salient characteristics, MANETs are vulnerable to Denial of Service attacks. DoSattack is any event that reduces or eradicates a network's capacity to perform its expected function. In DoS attack attackers, pretense threats to larger websites such as flipkart, Snapdeal and amazon. DoS attacks are very effective attacks in MANET such as they temporarily stopped service availability or permanently deforming information in the network. DoS attacks disturb normal communication by employing signal jamming at the physical layer. DoS attacks are lunched against Network layerby changing routing information or modifying system configuration, selective dropping,table overflow, or poisoning.At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks[4].

B. Man-In-The-Middle Attack

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. [5]

C. Replay Attack

MANETs 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 attackattacker continually retransmits valid information to the network that has been previously captured or hold information for some period of time and then resend.Replay attack can be abused to pose a specific node or simply to disturb the routing operation in a MANET[6].

D. Impersonation Attack

Impersonation attacks are just the first step for most attacks, and are used to launchfurther sophisticated attacks. For example, a malicious node can precede an attack by changing its MAC or IPaddress. In this type of attack, nodes may be able to enter in to the network quietly, or send fake routing information, masquerading as some other trusted node. Sybil and trust attacks are two types of impersonation attack. In Sybil attacks, a malicious node claims a large number of client identities, either by impersonating other legal nodes or claiming false identities.[7]

IV. DETECTION AGAINST MULTILAYER ATTACKS

To detect the dos attack Echchaachoui et al. used the trust based model. This model is based on observation and detection of doubtful traffic. In [8], proposed method use the law of inferential statistics to harvest information on the number of received packets of the neighbor nodes. On the basis of this information each node can be detect and observe the malicious node in the network, which floods the network with a huge number of packets. After detecting the malicious node, the network should estimate through probabilistic theory, the real behavior of the malicious node and then decide to deny or permit packets from this node.

Benjamin Aziz and Geoff Hamilton [9], proposed a static analysis algorithm for the detection of man-in-the-middle attacks in mobile processes using a solution based on precise timing. A static analysis for detecting MITM attacks in real-time systems using precise timing. The analysis, designed for a stochastic process algebraic language, captures name substitutions occurring among processes as a result of their communications. The results of the analysis are then used to define a name integrity property and a notion of MITM attacks. This approach follows from earlier, well-established, works on security analyses for mobile systems and cryptographic systems. The results of the analysis are used to define a name integrity property, which itself forms the basis for defining a MITM attack property.

In [10] L. Li, D. Kidston et al., proposed a detection method for reply attack based on cross-layer management architecture. This method target to minimize messaging overhead, the scheme leverages the network statistics and observations available at different layers at each node. The approach focuses on implementing protection in the one-hop neighborhood of each network node, employing local information primarily from the physical and MAC layers.

In [11], describes the Generalized Detection Model (GADE), to detect presence of an attack in the network. This integrated system can detect impersonation attacks, determine the number of attackers, and localize multiple adversaries.Additionally, this approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

V. PREVENTION AGAINST MULTILAYER ATTACKS

To prevent MANET from one major DoS attack against routing protocol, here proposed a new Denial Contradictions with Fictitious Node Mechanism (DCFM) mitigation method. DCFM Method dependson the internal information acquired by each node during routine routing, and augmentation ofvirtual (fictitious) nodes. DCFM Method utilizes the same techniques used by the attack in order to prevent it.As size of the network increases, the overhead of the additional virtual nodes diminishes, which is reliable with general claim that OLSR functions best on large networks [12].

In [13], P. Patil et al.proposed a solution to prevent Man in the Middle attack in Manet using ALERT Protocol with Hash function and SHA-1 algorithm. This approach will be based on single path strategy andalso uses ACK for successful delivery of packets. According to this solution hash value given at Source side is checked at destination, when attacker node tries toalter data packet in Manet. If hash value of data packet's different from its source side hash value, attack is detected. So it sends negative acknowledgment (NACK) tosend packets again by finding malicious node in network &uses alternative path for routing.

In [14], discuss the solution to protect a MANET from a replay attack by using a time stamp with the use of an asymmetric key. This solution prevents the replay attack by comparing the current time and time stamp contained in the received message. If the time stamp is too far from the current time, the message is judged to be suspicious and is rejected.Although this solution works well against the replay attack, it is still vulnerable to a wormhole attack where two colluding attackers use a high speed network to replay messages in a far-away location with almost no delay.

In [15], introduces a framework for multi-factor identification and authentication to prevent impersonation attack in MANET, which allows mobile nodes in MANET to identify and authenticate each other by examining a wide range of characteristics.A key element to the proposed framework is that it combines well-known cryptographic mechanisms (such as digital certificates and signatures), with different sources of identification information. This information comes in the form of attributes describing physical node characteristics, much like the biometrical characteristics examined during human identification and authentication.

VI. COUNTERMEASURE FOR MULTILAYER ATTACKS IN MANET

Security is very challenging factor due to self organization environment of MANET. The characteristics and nature of MANET need the strict contribution of participating mobile hosts. A number of security mechanisms have been invented and a list of security protocols has been proposed to impose cooperation and prevent misbehavior. These Mechanisms can be classified into two categories: proactive and Reactive.Proactive mechanism is also known as prevention method. Proactive mechanism provide first line of defense through various cryptographic algorithms such as hash functions, threshold cryptography, digital signature, asymmetric and symmetric key cryptography etc.Reactive mechanisms attempt to identified threats first and then react accordingly. It consists of detecting routing misbehavior with the help of intrusion detection system and cooperation enforcement reducing selfish node misbehavior.In practice, both approaches can be combined to be more effective to counter malicious attacks.

Here, focused on Multilayer attacks and their corresponding security countermeasure. Multiple layers can be targeted by the DoS attacks, impersonation attacks, man in the middle attacks, reply attacks and many other attacks in the MANET.

Commonly two types of DoS attacks occurred in Manet. First one is occurring at the routing layer and second is occur at the MAC layer.End to end authentication may prevent from these two types of attacks[16].

In [11], proposed defense mechanism against DoS and Man in the Middle Attack and introduces ALERT Protocol based on single path strategy.

MANET is also susceptible to replay attacks. In this case the authentication system can be improved

and made stronger by extending the AODV protocol. This method of improving the security of Ad Hoc networks increases the security of the network with a small amount of overhead.

ARAN can be used to defend against impersonation and repudiation attacks. ARAN provides authentication and non-repudiation services using predetermined cryptographic certificates for end-to-end authentication. In ARAN, each node requests a certificate from a trusted certificate server. Route discovery is accomplished by broadcasting a route discovery message RDPfrom the source node. The reply message REPis unicasts from the destination to the source. The routing messages are authenticated at each intermediate hop in both directions.

In [17], various types of defense solution have been proposed to counter security attacks. Thesesolutions based on newly

 ISSN: 2321-8169
04 – 08

invented protocol or combination of security techniques into presentedprotocol such as AODV and OLSR.The preventing mechanism instigated from the conventional mechanism such as authentication, access control, hash, encryption, and digital signature. Reactive mechanism combination of intrusion detection systems, reputation and cooperation systems, and trust management systems provide a second line of defense against security attacks and reduce selfish behaviors.

VII. ANALYSIS AND DISCUSSION

The Various security approaches against Multi layer attacks are studies and analyze in the following table.

S.NO.	Author	Attacks	Attack Type	Prevention Method	Routing Protocol	Advantages	Limitation	Countermeasure
1	N. Schweitzer et al.	**DoS**	Active	DCFM Method	OLSR	Increase the Routing Efficiency	Required additional space in the network	End to end authentication
2	P. Patil et al.	**MITM**	Active	ALERT Protocol with hash and SHA-1 algorithm	ALERT	Low cost and easy to Implement	High Route discovery latency& vulnerable to misuse	ALERT Protocol based on single path strategy
3	B. Kannhavong et al.	**Reply**	Active	Time stamping Method	OLSR	Works well against the attack	Vulnerable to other attack	AODV Protocol Based authentication system
4	D. Glynos et al.	**Impersonation**	Active	Multi factor authentication Method	-	Deal with several types of impersonation attack	Requires additional sensing capabilities from the MANET nodes	ARAN Protocol Based End to end authentication

In [12], N. Schweitzer et al. proposed DCFM method for DoSattack increases the routing efficiencyand successfully prevent the dos attack. This Method based on OLSR routing protocol. But the limitation of this method is required additional space in the network. Countermeasure for active type of dos attack is end to end authentication. In [13], ALERT Protocol with hash and SHA-1 algorithm presented for the MITM attack is easy to implement. This provide secure route but main drawback of this method, it takes more time for route discoveryprocess. For MIMT attack ALERT Protocol Based on single path strategy is given as countermeasure. In [14], For Reply attacktimestamping method was implemented. This solution well work for replay attack, it is still vulnerable to other attack.AODV Protocol Based authentication system is successfully improving security of the ad hoc network. In [15], Multi factor authentication method is fully protected and deals with several types of impersonation attack. This method requires additional sensing capabilities from theMANET nodes.ARAN Protocol Based End to end authentication is implemented to count this type of attack.Multi layer of OSI Model are vulnerable to DoS, MITM, Reply and Impersonation attacks, which are most prominent attacks.

VIII. CONCLUSION

In this paper, various types of security attacks on different layers are classified, which produces lots of trouble in the MANET operations. Different security technologies are introduced for prevention and detection of attacks in such type of network. Attacks like DoS, impersonation and Reply have proved their effectiveness against almost all MANET routing protocols.All these attacks are very prominent attacks on Multilayer therefore paper focuses on the currently used security countermeasures to defend against these attacks. A lot of research is still need to be carried out to identify new security threats to ad-hoc networks & securing them.

REFERENCES

[1] A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2027-2045, Fourth Quarter 2013.

[2] J. Swain, B. K. Pattanayak and B. Pati, "Study and analysis of routing issues in MANET," 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, pp. 506-509,2017.

ISSN: 2321-8169
04 – 08

[3] M. M. Alani, "MANET security: A survey,″ Control System, Computing and Engineering (ICCSCE), 2014 IEEE International Conference on, BatuFerringhi, pp. 559-564, 2014

[4] B. Joshi and N. K. Singh, "Mitigating dynamic DoS attacks in mobile ad hoc network," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, pp. 1-7,2016.

[5] 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, thirdquarter 2016.

[6] M. Khatkar, N. Phogat and B. Kumar, "Reliable data transmission in Anonymous Location Aided Routing in MANET by preventing replay attack," Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization, Noida, pp. 1-6, 2014.

[7] Shikha Sharma, Manish Mahajan, "A Study of Attacks at Different Layers in Mobile Ad-Hoc Network," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, Issue 6,June 2016.

[8] Echchaachoui, A. Kobbane and M. Elkoutbi, "A new trust model to secure routing protocols against DoS attacks in MANETs," 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA), Rabat, pp. 1-6, 2015.

[9] B. Aziz and G. Hamilton, "Detecting Man-in-the-Middle Attacks by Precise Timing," 2009 Third International Conference on Emerging Security Information, Systems and Technologies, Athens, Glyfada, pp. 81-86, 2009.

[10] L. Li, D. Kidston, P. Vigneron and P. C. Mason, "Replay attacks and detection in tactical MANETs," Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Victoria, BC, pp. 226-231, 2011.

[11] B.Lakshmi, LB Sanmuga, R Karthikeyan, " Detection and Prevention of Impersonation Attack in Wireless networks ", International Journal of Advanced Research inComputer Science & Technology, Vol. 2 Issue Special 1, Jan-March 2014

[12] N. Schweitzer, A. Stulman, A. Shabtai and R. D. Margalit, "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes," in IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 163-172, Jan. 1 2016.

[13] P. Patil, N. Marathe and V. Jethani, "Preventing DOS & MITM Attacks in "anonymous location based efficient routing protocol" in MANET," 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, pp. 16-20, 2016.

[14] 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.

[15] D. Glynos, P. Kotzanikolaou and C. Douligeris, "Preventing impersonation attacks in MANET with multi-factor authentication," Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05), pp. 59-64, 2005.

[16] B Wu, J Chen, J Wu, M Cardei , " A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" Wireless network security, Springer-2007.

[17] A. K. Abdelaziz, M. Nafaa and G. Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks,″ 2013 UKSim 15th International Conference on Computer Modelling and Simulation, Cambridge, pp. 693-698, 2013.