International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Intruder & Attack Detection over Mobile ad-hoc Network: A Review

Priyanka Yadav[1], Assistant Prof. Sandeep Rai[2]
[1,2]*Department of Computer Science & Engineering, TIT(E), Bhopal, Madhya Pradesh, India.*

***Abstract*--The Mobile Ad-hoc Network is a newly emerging approach in the world of communication. The communication take place between devices having the ability of communication. the most popular techniques involved the mobile ad-hoc network. There are various types of attack can possible in the network. This technology has many advantages but have the loophole. This paper is a brief discussion on Mobile ad-hoc Network. This paper also throws some light on the various types of attacks like and its classification and other techniques used to enhance the performance of network.**

Keywords: **MANET, Attacks, Routing, AODV, Vulnerabilities, Intrusion Detection**

I. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies which are composed of bandwidth constrained wireless links. To enable communication within a MANET, a routing protocol is required to establish routes between participating nodes. Because of limited transmission range, multiple network hops may be needed to enable data communication between two nodes in the network. Since MANET is an infrastructure less network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network.

Mobile ad-hoc networks (MANETs) aim to provide wireless communication in a limited geographical area. Compared with traditional networks, MANETs have fundamental characteristics of open medium, dynamic topology, lack of central authorities, distributed cooperation, and constrained capabilities. MANETs are especially attractive for use by the military, emergency service providers and commercial applications where user density is too spare or too temporary to justify the deployment of any infrastructure.

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.

In Latin, ***ad hoc*** literally means "for this," meaning "for this special purpose" and also, by extension, improvised or impromptu.

- Dynamic Topologies
- Bandwidth-constrained, variable capacity links
- Energy-constrained
- Limited Physical security
- Scalability

Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure. And it's an autonomous system in which mobile hosts connected by wireless links are free to be dynamically and some time act as routers at the same time, and we discuss in this paper the distinct characteristics of traditional wired networks, including network configuration may change at any time , there is no direction or limit the movement and so on, and thus needed a new optional path Agreement (Routing Protocol) to identify nodes for these actions communicate with each other path, An ideal choice way the agreement should not only be able to find the right path, and the Ad Hoc Network must be able to adapt to changing network of this type at any time. and we talk in details in this paper all the information of Mobile Ad Hoc Network which include the History of ad hoc, wireless ad hoc, wireless mobile approaches and types of mobile ad Hoc networks, and then we present more than 13 types of the routing Ad Hoc Networks protocols have been proposed. In this paper, the more representative of routing protocols, analysis of individual characteristics and advantages and disadvantages to collate and compare, and present the all applications or the Possible Service of Ad Hoc Networks. Wireless Sensor Networks (WSNs) consists of a set of sensor nodes that are deployed in a field and interconnected with a wireless communication network.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Each of these scattered sensor nodes have the capabilities to collect data, fuse that data and route the data back to the sink/base station. To collect data, each of these sensor nodes makes decision based on its observation of a part of the environment and on partial a-priori information. As larger amount of sensors are deployed in harsher environment, it is important that the distributed computation should be robust and fault-tolerant. The identification of event in a wireless sensor network should be done as fast as possible, thus the computations are done in parallel..

II. Mobile AD-HOC Network

A wireless infrastructure less network having dynamic topology is called the mobile ad-hoc network. Here mobile word use due to the mobility of the nodes in the network. Weather the ad-hoc word comes because of temporal establishment of network. The figure shown below is an example of the mobile ad-hoc network. In this scenario there is a source and destination node is available for communication.

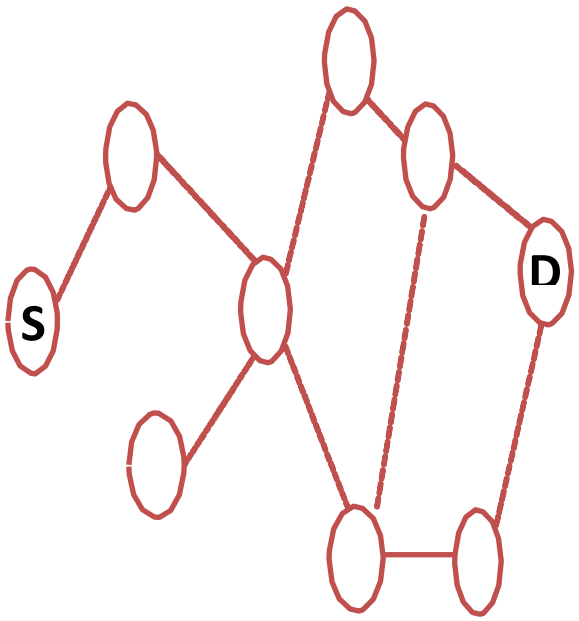

Figure 1 Mobile ad-hoc network

The characteristics of mobile ad hoc networks (MANETs) determine that the authentication approaches to protect routing and data packet transmission in MANETs should be lightweight and scalable.

In this paper, we propose a lightweight authentication protocol, which utilizes one-way hash chain to provide effective and efficient authentication for communications between neighboring nodes in MANETs. Delayed key disclosure scheme is used to prevent from in-the-middle attack on key release

Most of the previous mobile ad hoc network research has focused on routing protocols and communication methods in a trusted environment. However, applications such as emergency rescue operations, military and police networks, and safety-critical business operations such as oil drilling platforms or mining operations need secured communications.

III. Vulnerabilities Of Manets

- *Wireless Connection:* the wireless links are very helpful to connect the user with the network. The flexibility of this feature is helps the attacker to join the network.
- *Dynamic Topology:* this is a biggest advantage of MANET that nodes can leave and join the network freely. But this approach increased the complexity.
- *Cooperativeness:* Most of the routing approaches believe that the nodes which the moving in the network are not the malicious node. Even these nodes are cooperative.
- *Bandwidth:* here the bandwidth is limited due to large number of other activities in compare of wired network.

IV. Applications of MANET

The MANET is very popular because of its properties. It has lots of applications. Some of them are discussed below.

- Collaborative Work
- Disaster Management
- Military and intelligence
- Preserving Historical places
- Personal Area Network (PAN)
- Taxi or Cab Network
- Conference or Meeting room

V. Attacks

There are various attacks can possible in the mobile ad-hoc network. But there are two major classifications in this way.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Active and Passive attacks are the most common category. In active attack the attacker or the malicious node takes the part actively in the network. Here the attacker will modify or alter the data packet and send this packer into the network. In spite of altering the data packet attacker can also inject and drop the data packet. So that, such type of attacks very harmful for the end users.

On other hand the passive attack can happen without the tempering the data packet. In this type of attack the attacker only analyze the data.

The main goal of this type of attack is to break the confidentiality. Here the attacker tries to know the activities of the network. It focuses on the pattern to send in the network on the basis of which the attacker will take illegal action. Detection of passive attacks is very difficult since the operation of the network itself does not get affected.

The figure 2 shows the basic classification of the attacking approaches. As it shows the active and passive attack are the first criteria. It is possible to classify this by some other criteria.

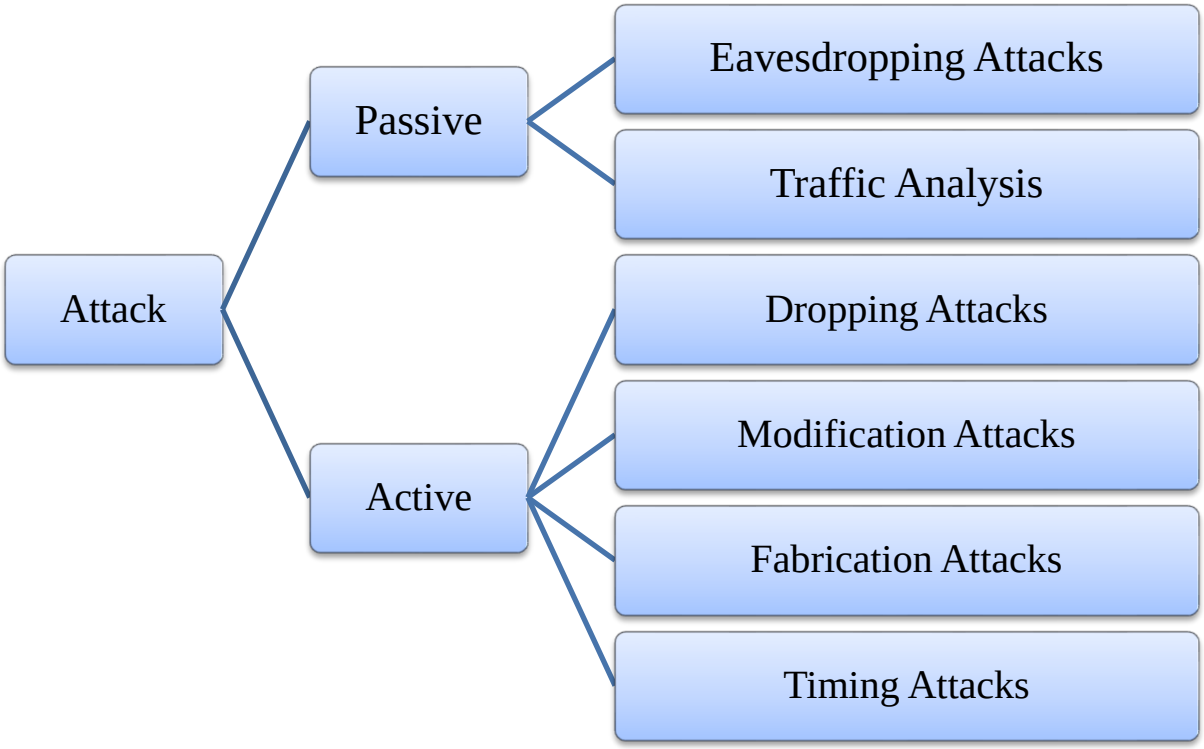

Figure 2 Classifications of Attacks

Types of Attacks on Protocol Stack

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

Layer	Attacks
Application Layer	Viruses and Worms
Transport Layer	TCP,UDP
Network Layer	Blackhole, Wormhole
Data Link Layer	Traffic Monitoring,
Physical Layer	EavesDropping

VI. Literature Review

Mobile ad-hoc network [1] is a collection of mobile nodes which forms an instant network without fixed topology and can be arranged dynamically. Energy saving and security are important issue in MANET. Network coding technique is used to reduce energy consumption by fewer transmissions in MANET. To achieve a security, there are many encryption scheme are available. Out of which p-coding technique is lightweight encryption scheme which provides confidentiality. P-coding is to let the source randomly permute the symbol of each packet. So eavesdropper can't obtain the meaningful information without knowing the permutation encryption function and coding vector.

Key management scheme [2] is a critical issue of Mobile Ad hoc Networks (MANETs). Malicious nodes may attack the legitimate nodes by eavesdropping. Data encryption is a solution to resolve this problem. Due to the restricted energy and computational capability of MANETs, it's necessary to design a lightweight and storage efficient key management scheme. In this paper, we propose a hop-by-hop authentication and routing-driven dynamic key management scheme. An improved Elliptic Curve Diffie-Hellman (ECDH) protocol with mutual authentication is used to generate pair-wise keys, and the pair-wise keys are stored in caches before their expiration. The simulation results and performance evaluation show that the proposed scheme can reduce more key storage space than other schemes. Furthermore, it increases the security level of MANETs.

In The paper [3] examines the lightweight cryptography primitives and proposes a novel integration mechanism of primitives to provide complete cryptography services for resource constraint Mobile Ad-Hoc Networks (MANETs). In this work, Tseng's protocol is modified to integrate primitives [30]. In order to evaluate the performance of secure MANETs, software; throughput, jitter & end to end delay; and hardware parameters; area consumption in terms of gate equivalents (GE); are taken into consideration. An integration proposal of these cryptography primitives has been proposed and it has been observed that these primitives can be clubbed with hardware cost of 36.5% of the total GE with maximum through and minimum delay using Destination Sequenced Distance Vector (DSDV) protocol.

In thepaper [4] introduces a lightweight and secure framework enabling the refreshing of private keys in identity-based public key infrastructures. The framework is applied to enable secure inter-operation between entities with different trusted authorities in dynamic coalition environments. The approach is particularly well-suited to coalition forming in computation and bandwidth-limited MANETs.

VII. Conclusion

This paper is review of mobile ad-hoc network and various approaches in this area. As the mobile ad-hoc network is a most user friendly scheme in the current scenario. It is highly need that performance of the network must enhanced. Securing the Mobile ad-hoc Network is becoming increasingly important in present scenario. The wireless network is area where there is needs to enhance the security. This paper has analyzed the attacks that MANET can be subjected to. This paper has discussed various types of attack which can happen in MANET.

It also shows the protocol which has used in mobile ad-hoc network. The worm hole is a major disadvantage of the MANET. There is a need to overcome this problem. This paper also throws some light on the classification of wormhole and previous work which has been done in this era.

REFERENCES

[1] S. Patel and F. Khatiwala, "A review paper of an encryption scheme using network coding for energy optimization in MANET," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, 2016, pp. 1054-1058.

[2] Dahai Du and Huagang Xiong, "A dynamic key management scheme for MANETs," *Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, Harbin, 2011, pp. 779-783.

[3] A Kumar, K. Gopal and A. Aggarwal, "A complete, efficient and lightweight cryptography solution for resource contrainst Mobile Ad-Hoc Networks," *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, Solan, 2012, pp. 854-860.

[4] S. Balfe, K. D. Boklan, Z. Klagsbrun and K. G. Paterson, "Key Refreshing in Identity-Based Cryptography and its Applications in MANETs," *MILCOM 2007 - IEEE Military Communications Conference*, Orlando, FL, USA, 2007, pp. 1-8.

[5] Zunnun Narmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[6] Sheikh, R. , Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review", IEEE 2010, pp 1-4.

[7] Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., " A survey of routing attacks in mobile ad hoc networks" IEEE 2007, pp 85-91.

[8] Verma, M.K. and Joshi, S. ; Doohan, N.V. "A survey on: An analysis of secure routing of volatile nodes in MANET", IEEE 2012, pp 1-3.

[9] P. Papadimitratos and Z. J. Haas, "Secure Routing For Mobile Ad Hoc Networks" in Proc. of CNDS, 2002.

[10] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol For Ad Hoc Networks" in Proc. of IEEE ICNP, 2002.

[11] C. E. Perkins, and E. M. Royer, "Ad-hoc on-demand distance vector routing," IEEE 1999, pp 25-26.

[12] Mahdi Nouri, Somayeh Abazari Aghdam and Sajjad Abazari Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in MANETs", IEEE 2011, pp 1-6.

[13] Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni and Naghmeh Niknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE 2011, pp 122-128.

[14] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[15] Jin Guo, Zhi-yong Lei, "A Kind of Wormhole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification", IEEE 2011, pp 564-568.