International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-223 PAGE NO: 1391-1394
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

A SURVEY OF INTRUSION DETECTION SYSTEM IN MOBILE AD-HOC NETWORKS

V.Meenakumari[1], V.P.Muthukumar[2],
[1]M.Phil Full time Research Scholar, PG & Research Department of Computer Science[1]
[2]Head of the Department, PG & Research Department of Computer Applications[2]
Vivekanandha College of Arts & Sciences for Women (Autonomous)
Tiruchengode, Tamilnadu, Namakkal-637 205,
meenakumariv.94@gmail.com[1]
rajiperiasamy@gmail.com[2]

ABSTRACT- Mobile Ad-hoc Network (MANET) is an Emerging Technology, having features like dynamic topologyand self-configuring ability of nodes. Each device in a MANET is without free to move in any direction and its changes the connections to other devices frequently. Mobile Ad-hoc network is faces several challenges such as Energy, Routing, Security, Quality of services, Memory and etc.. The self –configuring ability of nods in MANET made it popular among the critical mission such as military use and emergency recovery. The main Intrusion Detection is one of the possible ways in recognizing possible attacks before the system could be penetrate. The encryption and authentication solution are consider as the first line of protection, are no longer enough to protect MANETs. In this paper, we focus on various intrusion-detection systems in MANETs.

Keywords: Mobile Ad-Hoc Network, Intrusion Detection System.

1.INTRODUCTION

Wireless networking is the platform for working with the current technology widely used in several applications. Mobile Ad-hoc Network (MANET) is a collection of wireless mobile node, consists of both wireless transmitters and receivers, which dynamically forming a temporary network and communication between transmitter and receiver is by using bi-directional link. Either directly, if nodes in MANET are within communication range or indirectly means transmitter node rely on intermediate node, for forwarding data to destination node. Various feature of MANET, overcomes the problem in contemporary application of wireless network such as dynamic topology and decentralized network feature of MANET, means all the nodes are free to move randomly.

The self-configuring ability of nodes in MANET, Minimal configuration and quick.Development makes MANET ready to be used in emergency condition, where an infrastructure is unavailable, or difficult to install network, in scenarios like natural disasters, military conflicts. Due to these various

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-223 PAGE NO: 1391-1394
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

unique characteristics, MANET is becoming popular among all other wireless application as well as widely implemented in industry.
There are several Applications used in Mobile Ad-Hoc Networks. These are,

- Commercial Environment,
- Location Aware Services,
- Personal Area Network
- Emergency Services

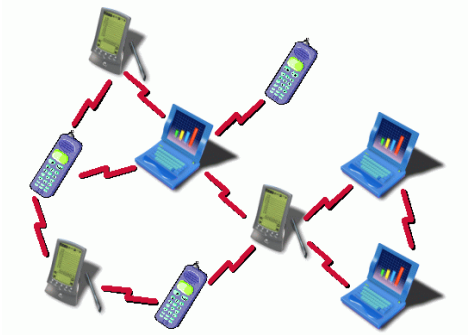

Fig1. Wireless MANET

1.1 ID'S IN MANETS:
Intrusion is any set of actions that attempt to comprise the integrity, confidentiality or availability and an intrusiondetection system (IDS) is a device or software application that monitors network traffic and if any suspicious activityfound then it alerts the system or network administrator. There are three main modules of IDS are Monitoring,Analyses, Response. The Monitoring Module is responsiblefor controlling the collection of data. Analyses Module isresponsible for deciding if the collected data indicated as anintrusion or not. Response Module is responsible formanage and using the response actions to the intrusion.
. To overcome this problem, intrusion-detection system (IDS) should be added to enhance the security level of MANETs.

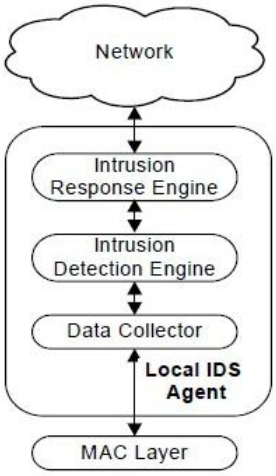

Fig2.Intrusion detection system

If MANET knows how to the detect the attackers as soon as they enters in the network, we will able to completely remove the potential damages caused by compromised nodes at the first time.

2. SECURITY THREATS FACED BY MANETS

Securing Mobile Ad-hoc Network is highly challenging task. The attacks in MANETs are secure communication in MANETs and for that reason secure transmission of information is necessary.
2.1 Active Attack

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-223 PAGE NO: 1391-1394
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

An active attack is the attacker try to bypass or break into secured systems. And it has done through worms, Trojan horses. Active attacks attempts to avoid or break protection features, to introduce malicious code, and take or modify information. Attacker gains the physical control link .It is detected to easily.

2.2 Passive Attack

A passive attackis monitoring unencrypted traffic and clear-text passwords and sensitive information that can be used in other types of attacks.The attacker cannot directly cooperate with the parties occupied, so attacker attempts to crack the system by observing the data. Identification of attack is very hard.

LAYERS	ATTACKS
Application Layer	Repudiation, Data corruption
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Warm hole, Block hole, Flooding
Data Link Layer	Traffic Analysis, Monitoring, WEP weakness
Physical Layer	Jamming, interception
Multi Layer Attack	Dos , Replay, Man in the Middle, impersonation

3. RELATED WORK

3.1 Routing misbehavior in mobile Ad-hoc networks (MANET)

Most of the routing protocols in MANET have limitations in transmission. Therefore, nodes in MANET assume thatother node always cooperate with each other, to reciprocation of packet this assumption, gives opportunities to attackers,

3.1.1 Watchdog

Watchdog serves as IDS for MANET. It is responsible for detecting malicious node misbehaviors by prominently listing to its next hop's broadcast. If Watchdog node overhears that, its next node fails to forward the packet within pre-defined time, it increase its failure counter.

3.1.2 Pathrater

Pathrater works as response system. Once Watchdog node identifies malicious node in the network, then the pathrater cooperator with the routing protocols to avoid the reported node in the future transmission. Many research studies have proved that, watchdog scheme is efficient. Nevertheless, as pointed out by Marti et watchdog scheme fails to detect malicious misbehaviors with presence of following: 1)ambiguous collisions; 2) receiver collisions; 3) limited transmissions; 4) false misbehavior report; 5)collusion; 6) partial dropping.

3.2 Acknowledgement Based Routing Misbehavior Detection in MANET:

To address six weakness of watchdog scheme, various new approaches proposed by many researches.In this paper Liu et al.[3] proposed a novel scheme called TWOACK. TWOACK is one of the most significant approaches among them. This TWOACK scheme is neither an enhancement nor Watchdog based scheme. Its aim is to overcome problems such as Receiver collision an limited transmission power in a watchdog.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 14, 2017 ISSN: 2348-6600
Reference ID: IJCS-223 PAGE NO: 1391-1394
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

3.3 Video Transmission Enhancement in presence of Misbehaving Nodes in MANETs.

In this paper, sheltami et al. [5] proposed a new novel intrusion detection system, called Adaptive Acknowledgement (AACK). AACK is an acknowledgement-based, scheme, which is considered as combination of TACK (identical to 2-ack) and end-to-end acknowledgement scheme (ACK). as compared to TWO-ACK with TACK packet. Hybrid scheme in AACK, significantly reduces RO. Both the TWO-ACK and AACK schemes are acknowledgment based scheme. Misbehaving nodes, that exhibit abnormal behaviors can disrupt thenetwork operation.

3.4 Detecting forged Acknowledgement in MANETs.

Nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attacker with the opportunities to drop the packet as well as to generate forge the acknowledgement packet,MANET suffers from the problem is it fails detect malicious node. In this paper, N.

In this secure-ACK scheme, the principle is to let every three consecutive node work in group, the third node required to send S-ACK packet to the first node as well as third node is required to sign packet with its own digital signature.

3.5 EAACK – A Secure intrusion-detection System forMANETs

As discussed in previous paper, both TWO-ACK and AACK solve two weakness of watchdog scheme, namely receiver collision and limited transmission power. But both of them, still suffer from problem that is to false misbehavior attack.

CONCLUSION

The Intrusion detection is the primary security problem in mobile ad hoc network. Intrusion detection are major detection in MANET, probably that need to be addressed in mobile ad hoc networks. Malicious attack has always been a major threat to the security in MANETs. In this paper, we have done literature survey for detecting the malicious nodes misbehaviors in Mobile Ad-hoc Network (MANET). Intrusion detection system (IDS) is one of the most active fields of protocol specially designed forMANETs. In this system, first send data packet; if it detects any misbehavior in the network it will find misbehavingnode and eliminate the node from the route.

REFERENCES

[1]. Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK- A Secure Intrusion Detection System for MANETs" IEEE trans. Vol.60, no.3, MAR, 2013.

[2]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265

[3]. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.