International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||09||Pages||7067-7073||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i9.17

Security attacks on Routing protocols and Intrusion Detection in MANET

R.M.Chamudeeswari[1], Dr.P.Sumathi[2]

Asst. Professor.
Department of Computer Applications
Asan Memorial College of Arts and Science
Chennai,
Asst. Professor
Department of Computer Science.
PG & Research, Department of Computer Science
Government Arts College, Coimbatore-18.

Abstract
The security for MANET is the major issue in the network area. Dynamic topology of wireless network sets a challenge to implement the real time application as compared to wired networks. MANET is a set of independent node can communicate with each other by active path of multi hop wireless medium. Mobile ad-hoc networks are vulnerable to security threats. Many Intrusion Detection Systems (IDS) have been inserted to distinguish the possible approaches in the MANET. An intrusion detection system is the capability to sense intruders and user actions in the organization in a competent and reasonable manner. An Intruder that collaborates a mobile node in MANET eliminates the communication between the nodes. By distribution fake routing information, provided that false link status information, and plentiful other nodes with superfluous routing traffic information. In this paper, our aim is to present a review of different strategies for MANET have been elaborated for a future research enhancement in the field of Intrusion Detection System.

Keywords: ANIDS, IDS, MANET, MIDS, ROUNTING PROTOCOLS

I Introduction

A Mobile Ad hoc Network (MANET) is a collection of autonomous nodes communicate with each other through wireless connections. The primary advantage of MANET is flexibility, adaptability, easily co-operation, efficient communication, infrastructure system and no cooperation. MANET is vulnerable to malicious attack because of open medium, dynamic topology, lack of centralized management and control points. Security of the network fall into two layers. One is prevention layer IE firewall an authority and coding, second is Intrusion detection, which detects the attack based on the audit data. Data is transmitted as store-and forward manner using multi hop routine with a wireless sender and receiver. Application of MANET's being used in military services, disaster relief, personal are networked.

Different characteristic of MANET includes communication via wireless means, No centralized controller, Dynamic topology, energy constraints, can be set up anywhere, limited security.

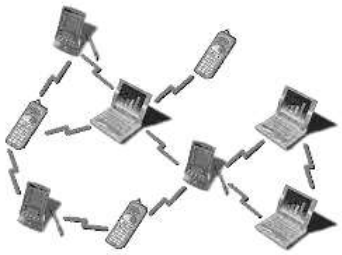

Figure 1. Mobile Ad-hoc network [1]

MANET can be classified into open- nodes, which shares resources with global connectivity, in some cases it turns down the connection to share the data called selfish or misbehaving nodes and closed –all clients are communicating by cooperating with each others. In wired networks, router performing routing task, but in MANET each node acts as router for forwarding packets, so it needed to set up anywhere in the global system. A firewall cannot provide the complete security against intrusion. The network based attacks can also be considered as some kind of intrusion. The intrusion can be specified as "any set of natural processes that attempt to compromise the integrity, confidentiality or availability of a resource". For controlling intrusion, intrusion detection systems

employ security in MANET plays major role in the network. Vulnerability is a weakness in security system. A particular scheme may be vulnerable to unauthorized data manipulation because the arrangement does not verify a user's identity before allowing information access. MANET is more vulnerable [2] than wired networks. Some of the vulnerabilities are as follows: - Lack of centralized management, Resource Availability, Scalability, Cooperativeness, Dynamic topology, power supply, Bandwidth constraint, Adversary inside the network, No predefined Boundary.

Issues and Challenges in MANET

Networks can contain a various collection of thousand of devices and its subcomponent may communicate through different technologies and protocols. Some challenges and issues are: [3]

IDS Components are able to communicate across sub- networks. MANET is infrastructureless network. There is no centralized management and control, difficult to detect and manage the faults. IDS monitor the activities and compare the activities against security rules and generate alarms. IDS suffer from false positive and negative alarm in the nature of Dynamic topology. Other challenges are reliability problems due to limited wireless transmission range. Other challenges in MANET are severe resource constraints and node mobility, Wireless channel is bandwidth constrains and new technologies with its own set of protocols among

II Adhoc Networks

2.1 **Challenges In Ad Hoc Wireless Networks**

Security involves a set of investments that are adequately funded. In a MANET, all networking functions [4], such as routing and packet forwarding, are performed by the nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is really challenging.

The goals to evaluate if mobile ad-hoc network is secure or not are as follows: [4]

Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

Confidentiality: Confidentiality ensures that computer-related assets are accessed exclusively by authorized parties. Confidentiality is sometimes called secrecy or concealment.

Integrity: Integrity means that assets can be changed only by authorized parties or only in authorized ways. Modification includes writing, changing position, deleting and making. Integrity ensures that a message being removed is never spoiled.

Authentication: Authentication enables a guest to ensure the identity of peer node it is communicating with. Authenticity is guaranteed because only the legitimate sender can get a message that will decrypt properly with the shared key.

Non repudiation: Non repudiation ensures that the transmitter and recipient of a message cannot disavow that they have ever committed or got such a message.

Anonymity: Anonymity means all information that can be used to identify the owner or current user of node should default be kept private and not be distributed by the node itself or the system software.

Authorization: This property assigns different access rights to different characters of users. For instance a network management can be performed by network administrator only.

2.2 Routing Protocols In Ad Hoc Wireless Networks

Routing is an important cognitive process, being the creation of data exchanging between wireless devices. Each wireless node acts as a router and participate in the routing protocol. Routing relies therefore on an implicit trust relationship among participating devices. Main routing responsibilities are exchanging the routing information, finding a feasible path between source and destination based on various metrics, and path maintenance.

The major requirements [5] of a routing protocol are (1) minimum route acquisition delay, (2) quick route reconfiguration in the case of path breaks, (3) loop-free routing, (3) distributed routing protocol, (4) low control overhead, (5) scalability with network size, (6) QoS support as demanded by the application, (7) support of time sensitive traffic, and (8) security and privacy.

Generally, current routing protocols for MANET can be categorized as:

Routing is the process of moving packets across a network from one host to another using suitable methods and algorithms to achieve high performance in the whole network [5].

Three types of Routing

1. Proactive routing
2. Reactive Routing
3. Hierarchical Routing

Proactive routing

A proactive routing protocol is also named "Table driven" routing protocol. Using a proactive routing protocol, nodes in a mobile ad hoc network continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. Thus, a source node can make a routing path immediately if it requires one.

- ✓ Optimized Link State Routing Protocol (OLSR)
- ✓ Wireless Routing Protocol (WRP)
- ✓ Destination Sequence Distance Vector (DSDV)

Reactive Routing

Reactive routing protocols for mobile ad hoc networks are also called "On-demand" routing protocols. In a reactive routing protocol, routing paths are sought only when required. A route discovery operation invokes a route-finding process

- ✓ Zone Routing Protocol (ZRP)
- ✓ Zone-based Hierarchical Link State routing (ZHLS)
- ✓ Hybrid Ad hoc Routing Protocol (HARP)

Hierarchical Routing

This type of routing protocol the choice of proactive and of reactive routing depends on the hierarchic level in which a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through the reactive flooding on the lower levels.

- ✓ Cluster Based Routing Protocol (CBRP)
- ✓ Fisheye State Routing protocol (FSR)

1.3 Attacks On Routing Protocols In Ad Hoc Wireless Networks

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the foremost step towards developing sound security solutions. Security of communication in MANET is important for secure transmission of information. [6] Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types: [4]

Active attacks can be divided into internal and external attacks.

i) External Attacks are carried by nodes that are not legitimately part of the network. Such attacks can be defended by using encryption, firewalls and source authentication. In external attacks, it is possible to disrupt the communication of an establishment from the parking lot in front of the company office.

ii) Internal Attacks are from compromised nodes that were once legitimate part of the network. Since the opponents are already part of the ad hoc wireless network as authorized nodes, they are much more dangerous and difficult to find when compared to outside approaches. Active attacks are **Passive or Active**

A. Passive Attacks

Passive attacks with the intent of keeping battery life for their own communications are seen to be selfish.

B. Active Attack

Active attacks with the purpose of damaging other nodes by doing a network outage are considered as malicious

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamic requests without a static part of routing. Schematics of various attacks as reported by Al-Shakib Khan on individual layer are as below:

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer : Sybil, Flooding, Black Hole, Gray Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure, etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal, External
- Physical : Interference, Traffic Jamming, Eavesdropping

MANET Attacks also can be classified into two broad categories .

i) **DATA traffic attack:** Black-Hole, Gray-Hole, Cooperative Black-Hole,

ii) **CONTROL traffic attack**: Jellyfish, Cache Poisoning, Rushing, Man in Middle, Registration , HELLO FloodBogus, Worm- Hole, Sybil , Cooperative Blackmail, Blackmail

III.Generic IDS

Due to the rapid growth of network and internet security IDS and multilayer are the two protection layer used. Intrusion detection is the process applied to identify intrusions. The main purpose is to serve alarm for the network. There are three modules, a monitoring module, controlling the collection of data, an analysis

module, identify if intrusion occurs or not, a Response module, managing the action.

Figure -2 IDS Basic Module [8]

3.1Classification of IDS

Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. IDS analyses network or system activities captured in audit data and uses patterns of well know attacks or normal profile to detect attacks. Classification of IDs based on i) Data collection techniques and ii) Data analysis techniques.

Data Collection Technique can be classified into Host based IDS and Network base IDS, whereas Data Analysis Techniques can be classified into three types[9]: Anomaly Detection, misuse or Signature Detection and specification based Detection.

Anomaly based IDS (ANIDS) models the normal usage of the network as a noise characterization. Anything differ from the noise is assumed to be an intrusion activity. E.g flooding a host with lots of packet. Strength is to identify the novel attacks. Detect any action that extensively deviates from the normal behavior. Merit is able to detect unknown attacks based on audit. Disadvantage is high false-alarm and limited by training data.

Misuse based IDS(MIDS) possess an attacked description that can be matched to sensed attack appearance. Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities. Based on known attack actions, feature extract from known intrusions and integrate the Human knowledge. Advantage is Accurately and generate much fewer false alarm . Disadvantage Can Detect any action that extensively deviates from the normal behavior to detect novel or unknown attacks .

Specification Based IDs(SIDs)is a hybrid of both signature and the anomaly based IDS and it is a set of constraints that describe the correct operation of a program or protocol. A mismatch is reported as an attack

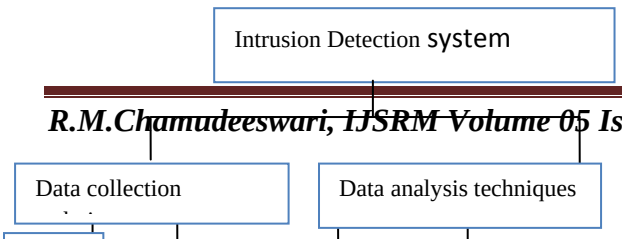

Figure 3. Classification of intrusion detection system

The major methods are active and passive intrusion detection, An Active Intrusion detection system is as well described as Intrusion Detection and Prevention System. This system is configured to repeatedly block if the attacks devoid of any interference required by an operator. This system has the gain of offering real time remedial action in response to an attack.

The Passive Intrusion detection is a system to ease the configuration to only monitor and evaluate network traffic activity and alert an operator to check for probable vulnerabilities and attacks. A passive intrusion detection system doesn't have any ability of performing defensive or remedial functions on its own.

3.2Intrusion Detection in MANETs

IDS in MANET can be based on the network infrastructure by flat or multilayer structure and its architecture on the network can be classified into [8] 1)standalone IDs 2)Distributed and collaborative IDS 3) Hierarchical IDS 4) Mobile Agent for IDS. more attention has been increased due to the usage of mobility network.

Stand-alone IDS In MANET the IDS is deployed in individual nodes unlike routers in wired networks. Decision is based on the individual nodes information of the network, because there is no exchange of information among the IDs nodes

Distributed and Cooperative IDS Every individual node has rule to take part the operation of intrusion and response via IDS agent The IDS agent is responsible for detecting and collecting local action to identify the intrusion .

Hierarchical IDS It is an enhanced version of distributed and cooperative IDS. Multilayered architecture is used where the network is divided into clusters. Cluster head is responsible for send packets, detecting intrusion and response them . Mobile Agent for IDS Mobile Agent for IDS architecture uses Mobile agents to perform specific task on behalf of the agent.

IV. Recent Ids Techniques For Manet

Intrusion detection is the progression of monitoring the events up in a computer organization or system. And to evaluates them for cryptogram of feasible incidents. In which are contravention or impending threats of contravention of computer security policies, suitable use policies, or usual security practices. An intrusion prevention system (IPS) is software that has all the ability of an intrusion detection scheme and can also effort to end probable incidents.

The release medium and broad distribution of nodes make MANET susceptible to malicious attacker In this case, it is vital to expand competent intrusion detection method to defend MANET from attacks. To familiar to such development, they strongly believed that it is very important to concentrate on its possible security concerns. As represented and executed a fresh intrusion detection [15] method Enhanced Adaptive Acknowledgment (EAACK) particularly intended for MANETs. EAACK established as elevated malicious behavior exposure rates in assured conditions as does not really influence the network performances.

The multimodal biometric expertise offered probable resolution for continuous user-to-device verification in elevated security mobile ad hoc networks (MANETs). The Multimodal biometric is position to occupation with Intrusion Detection Systems (IDS) to assuage the shortcomings of unimodal [16] biometric systems. The scheme chooses whether user verification is necessary and which biosensors must be elected, based on the security attitude. The resolution is complete in a completely dispersed manner by each verification device and IDS.

Multimodal biometrics[17] is position to exertion with intrusion detection systems. They are used to unimodal biometric system to avoid the shortcomings of the problem. Because all devices in the system have precise dimension and evaluation boundaries, more than one apparatus needs to be selected, and interpretation can be compound to amplify surveillance

Ad hoc Networks are imperfect with power and normally more respected to different attacks as evaluated to other types of system. Insider attacks are individual of the vigorous attacks transpire in Ad-hoc network. These attacks are extremely widespread in case of hasty protocols like Ad-hoc On Demand Distance Vector Protocol. The intrusion detection scheme determination is urbanized for discovery and separation of attacks. The MAC layer appliance determination is used for sense malicious behavior and determination spotlight on the verdict of attack progression in the system. They offered steady and effectual attack explanation which can be unswervingly appropriate to the genuine surroundings for Mobile Ad-hoc Devices.

The broadcasting technique is an appropriate for an extensive range of vehicular circumstances. Which only utilize limited information obtained via periodic beacon messages, hold acknowledgments of the [18] dispersed transmitted messages. Every vehicle chooses whether it go to a connected dominating set (CDS).

The Security is a significant problem in mobile ad hoc networks (MANETs). Nevertheless, security systems have important impacts on throughput. That is for the reason that 1) they required some transparency and use some network resources, thus reduce throughput accordingly; 2) The security and throughput disjointedly in manipulative a MANET, which can not accomplish an on the whole optimization of network recital

Intrusion detection is regularly used as a successive line of protection in Mobile Ad-hoc Networks. Sequentially to carry out they evaluate five supervised [19] categorization algorithms for intrusion exposures method. As they measured their recital on a dataset, illustrate in which consist of different traffic conditions and mobility model for multiple attacks. How categorization recital based on the difficulty cost matrix. As a result, inspect how the use of consistent versus weighted cost matrices influences classifier recital. Accordingly, we expand a chronological cross-validation system so that not all types of attacks determination essentially be current transversely all folds.

V Conclusion

MANET is collection of independent nodes which are communicated via radio waves. Many Intrusion Detection Systems (IDS) have been introduced to identify the possible attacks in the MANET. The proposed system present a review of different strategies for MANET has been elaborated for future research enhancement in the field of Intrusion Detection System.

References

1. Mukesh Kumar et al." **issues** and challenges Ofquality of service in mobile adhoc network" International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 1 No. 3
2. S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks"International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312
3. Sanjeev Gangwar,"Mobile Ad Hoc Newtwork:A Comprehensive study and survey on intrusion Detection" International Journal of Engineering Research and Applicatrion.,Vol.2,Issue 1,Feb-2012.
4. Priyanka Goyal,Vinti parmar, Rohul Rishi, MANET: Vulnerabilities, Challenges, Attacks, Application, a.IJCEM InternationalJournal of ComputationalEngineering & Management, Vol. 11, January 2011.
5. Perrig, R. Canetti, D. Tygar, and D. Song, The TESLA Broadcast Authentication Protocol, RSA Cryptobytes (RSA Laboratories), Vol 5,No 2, Summer/Fall 2002, pp. 2-13.
6. Y. -C. Hu, D. B. Johnson and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WM-CSA'02), Jun. 2002.
7. J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, Proc. of the 3rd Intl. Symp. on Information Processing in Sensor Networks, 2004.
8. Omkar Pattnaik et al, "Survey On Application Of IDS in MANET", ARPN Journal of Engineering and Applied Sciences, VOL. 7, NO. 12, DECEMBER 2012
9. Peng Ning and Sushil Jajodia, Intrusion Detection Technique.Fromhttp://discovery.csc.ncsu.edu/course/ csc774-S03/IDTechniques.pdf.
10. yogendra Kumar jain ,Rajesh Kumar Ahiwar, "Secure Mobile Agent Based IDS for MANET,(IJCSIT),vol.3(4),2012,4798-4805.
11. Mandala, Ngadi, M. A., & Abdullah, A. H. (2008). "A Survey on MANET Intrusion Detection"*International Journal of Computer Science and Security*, *2*(1), 1-11.
12. Prajeet Sharma, Niresh Sharma, Rajdeep Singhl, A Secure IDs against DDOS attack in wireless Mobile Ad-hoc Netwrok,Internation Journal of Computer Application (0975-8887) V0l.41, No21,March 2012.
13. Charile Obimbo,Lilina Maria Arboleda-Cobol, An Intrusion Detection on MANET, Journal of Communications in information science and Management Engineering,vol.2 No.3 2012, pp1-5.
14. Rohit Sharma, DR. Jatinder Singh,"Feature Analysis of Co-Operative Intrusion Detection System in Mobile Adhoc Network", International Journal of Software and Web Sciences 2 (1), Aug-Nov, 2012, pp. 25-29.
15. Parasakthi and sanjeev kumar, "Distributed Combined Authentication and Intrusion Detection in High-Security Mobile Ad Hoc Networks to reduce the computation complexity", National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012).
16. Lakshmi Narayanan and Fidal Castro "High Security for MANET Using Authentication and Intrusion Detection with Data Fusion", International Journal

of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518.

17. Shengrong Bu., F. Richard Yu., Xiaoping P. Liu., and Helen Tang., "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks," IEEE Transactions on Wireless Communications, Vol. 10, No. 9, September 2011.
18. Francisco Javier Ros, Pedro Miguel Ruiz and Ivan Stojmenovic, "Acknowledgment-Based Broadcast Protocol for Reliable and Efficient Data Dissemination in Vehicular Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 11, No. 1, January 2012.
19. Aikaterini Mitrokotsa, Christos Dimitrakakis "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", journal of Elsevier, 2012