A Detailed Survey On Attacks And Intrusion Detection in MANETs

G. Vetrichelvi*, Dr. G. Mohankumar**

** Associate professor,Department ofECE, PARK college of Engineering and Technology, Coimbatore.*
***Principal, PARK college of Engineering and Technology, Coimbatore.*

Abstract

Ensuring security in Mobile ad hoc networks (MANET) is very crucial Adhoc Network security is different from traditional network security. In recent years, the security issues on MANET have become one of the basic concerns. The MANET is more vulnerable to be attacked than wired network. These vulnerabilities are environment of the MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised to develop these vulnerabilities and to cripple the MANET operation. In many simple IDS implementation, several category are combined in a single device for improved efficiency. Intrusion Detection system (IDS) is another way to provide security and privacy in MANET. In this paper we have surveyed the various issues related with MANET and the use of Intrusion Detection System in the Adhoc Networks and analyzed their fruitfulness.

Keywords

Intrusion Detection, Network Security, Simulation Software, MANETS.

"1." Introduction

Mobile Ah-hoc Networks (MANETs) are networks that are made of mobile and power controlled nodes infrastructure less self-organizing, all the nodes share the same functions with respect to the network operation, (i.e. there is no node that is in charge for authentication or security services). It is vulnerable to security attacks due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring, management point, and lack of a clear line of defense.

"2." Detailed Discussion Of Manet Features

The characteristics of MANET can be objectively classified if studied from these angles: device compatibility, connectivity while accommodating varying traffic profiles, security and survivability. This section deals with each in a little more detail.

"2.1" Device Compatibility

MANETs are mostly composed of devices with different hardware configurations, varying energy profiles, or running different versions of software. Thus, the first challenge in deploying an actual MANET is that of establishing communication between these heterogeneous components. However, within the scope of this research, it is assumed that all our nodes communicate seamlessly.

"2.2" Connectivity

MANETS are systems with constituent nodes in different locations. Each such node may have a different set of neighbors that it is able to communicate effectively with. This is the first reason connectivity in MANETs is different from that infrastructure based networks - neighbor set and knowledge of an entity managing communication. In wired networks, the concept of communication establishment and maintenance is statically centered around dedicated routers, switches or an equivalent gateway. In traditional wireless infrastructure based systems, the equivalent concept is that of a central mobile station which manages connection establishment and session maintenance. Of course, connectivity depends on various activities of the OSI layers (considering OSI as a standard of functionality definition), particularly the communication sub-layers viz the physical, data-link network layers. But, of particular interest to the scientific community is routing; this may be because the layers below may be approached with the same view as that of infrastructure based wireless systems. We shall thus view the first challenge as one of routing.

"2.2.1" Routing

The IETF MANET is standardizing much of the work done toward routing protocols in MANETS. There have even been efforts to empirically model connectivity in MANETs. This section is dedicated to exploring Routing.

Routing Protocols based on reactive or proactive functionality: One of the primary approaches to routing is to decide whether the calculation of routes is a proactive one or a demand-based operation. The former, called Proactive MANET Protocols, (PMP) continuously evaluate routes. When a node wants to transmit, a route is known and immediately available. On the other hand, Reactive MANET Protocols (RMP) do not maintain routes between all nodes at all times and adapt to the traffic pattern on a demand or need basis. The study introduces each of these protocols and proceeds to do a comparative analysis.

Proactive Routing Protocols: Some pro-active routing protocols are Destination Sequenced Distance Vector Routing (DSDV), Cluster Head Gateway Switch Routing (CGSR) and Wireless routing protocol. These are mostly table driven.

DSDV bases on the Bellman-Ford routing algorithm and relies on routes weighed by hop numbers, prioritized using sequence numbers, and periodic broadcasting to maintain relevance of routes. CGSR differs in that it manages addressing based on a hierarchy of clusters lead by a cluster head, the internal non-head nodes having to transmit only to the cluster heads. WRP is a path finding algorithm that performs consistency checks on neighbor information, thus providing faster recovery in case of link failures.

Reactive Routing Protocols: Some examples of reactive protocols are Adhoc On demand distance vector routing(or AODV) and Dynamic source routing (DSR). AODV is built on DSDV, but calculates routes only when the source needs to transmit. This minimizes the number of broadcasts as opposed to DSDV, thus utilizing lesser bandwidth. But, the flip side to demand based route calculations is a greater percentage of broken source-to-destination links. However, AODV avoids such additional delays by using distance vector routing. Nodes that are not on a particular path neither maintain routing information, nor participate in routing table updates.

DSR uses source routing, which means the sender knows the complete hop-by-hop route to the destination. The node maintains route caches containing the source routes it is aware of, and data packets carry the source route in the packet headers.

This excessive route data caching introduces delay and throughput penalties, but keeps routing load low, thus saving valuable bandwidth.

Energy Aware Routing protocols MANETs differ from wireless infrastructure networks in that they have the structure and characteristics of a low-power radio network. Thus, a novel approach to routing in MANETs determines routes based on the energy profiles of nodes rather than distance (number of hops) .

"2.2.2" Mobility

Mobility in MANETs is different from the concept of movement of IP Address. When a device with a specific IP Address temporarily moves somewhere else, the home agent translates it into a second address that represents the device's current actual topological location. The packet stream is now forwarded to this location. Ina MANET, the address is tied to the device, not a topological location, as there is no fixed network infrastructure. The node cannot be located in a specific region (viz IP addresses of 100.100.X.X are on the UT campus etc) based on their addresses, and the route must be recalculated. MANET routing solves a routing problem in a network where mobility is normal. When mobility is solved using routing, addressing-based solutions are irrelevant. Mobility is not an aspect of all MANETs or of all nodes. However, mobility determines which nodes are neighbors, and within communication range. This means that it has a direct impact on route calculations, and affects data throughput of the MANET. Technical paper

"2.2.3" Bandwidth usage

Bandwidth availability affects connectivity. In MANETs, bandwidth is used for connectivity establishment and maintenance and for data exchange. If all of the available bandwidth is used up by data communication/other connection establishment activities, newer connections may not be established, or existing connections may not be re-established when mobile nodes relocate themselves. Hence, as discussed earlier, routing activities must be optimized to use the least amount of bandwidth. Data communication itself can be optimized, and, again, as mentioned earlier, data aggregation is performed at a few nodes (say, cluster head) and a summary is transmitted, thus saving bandwidth.

"2.3" Survivability

Survivability is defined as the capability to fulfill its mission, in a timely manner, in the presence of intrusions, attacks, accidents and system failures. Survivability is more concerned with protecting individual network nodes. Apart from directly determining the lifetime of a MANET, survivability of nodes has slowly evolved as a useful metric for routing protocol performance itself. Identifying areas where power consumption can be reduced (data aggregation, task-based node identities to quote a few) assists in improving survivability.

"2.4" Security

Heterogeneity of nodes in MANETs increases the vulnerability of MANET nodes. The exposed nature of MANETs connective links makes it open to inspection or targeted data capture. Also, unwanted interactions, or interactions with unwarranted entities drains power, thus decreasing survivability. Thus, security deals with the survivability of the network as a whole. MANETs are susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass though several lines of defense at firewalls and gateways, attacks on a wireless network are easy to launch, since they involve power-based-distances and not spatial distance (viz physical territories or boundaries). Furthermore, it is easier to launch attacks on MANETs than on infrastructure based wireless networks because there is no central base controlling identity of participant nodes.

The requirements at the application layer require protection from eavesdropping and malignant code (viruses and worms) to maintain secrecy and integrity. Robust encryption is typically the first line of defense for any communications network. In the cases of both encryption and anti-virus or anti-worm techniques and technologies, these protections come at the cost of network performance and must be balanced against the relative threat level and the operational need for low latency and high bandwidth. They mainly deal with strengthening the route discovery process or introducing methods for efficient selection of a route from among many available routes to the same destination. Link and physical layer data protection layer and adhoc layers talk more about protecting the physical layers protocols by addressing features of these layers that make them vulnerable.

Most of the above approaches tend toward self-examination, i.e they attempt to improve the resistance of the network to attacks by examining the features that make themselves vulnerable. This often involves the overhead accompanying such processes(bandwidth consumption, complexity of data retrieval and usage of power in the process).Another approach would be monitoring other nodes and their activities - if malicious intent could be detected as soon as it enters the network, and eliminated communications with them severed, then this overhead could be avoided or at least alleviated."Intrusion detection" falls into this category.

"3." Types Of Attacks

Many types of attacks are cited in MANETs. The names that are often encountered are Selective forwarding, Black-hole attack, Sinkhole attack, Wormhole attack, or flooding attacks. These are mentioned here because models of such attacks are used to test the efficiency of our research idea.

The types are attacks mentioned are briefly defined here:

"3.1" Selective forwarding attack:

Selective forwarding attack occurs when a compromised node drops a packet that is bound for a particular destination. This way, an attacker can selectively filter traffic from a particular part of the network. selective forwarding are involve dropping a percentage or random number of packets.

"3.2" Flooding attacks:

Flooding attacks are those in which the network is bombarded with a huge number of messages, so that the nodes are choked out of resources. Denial of service attacks are the most common form of flooding attacks.

"3.3"Denial of service attacks:

In this attack malicious node floods irrelevant data to consume network bandwidth or to consume the resources (e.g. power, storage capacity or computation resource) of a particular node. With fixed infrastructure networks, we can control denial of service attack by using "Round Robin Scheduling", but with mobile ad hoc networks, this approach has to be extended to adapt to the lack of infrastructure, which requires the identification of neighbor nodes by using cryptographic tools, and cost is very high..

"3.4" Black-hole attacks:

Black hole attacks are those in which the malicious node fails to forward any message that arrives at the node en route to its destination.

"3.5" Sinkhole Attacks:

Sink hole attacks are similar to black-hole attacks, except that they aim to attract more data traffic by advertising themselves as the best path to other destinations. Sinkhole attacks can also act as a platform for launching other attacks. An example would be to combine it with a selective forwarding attack..

"3.6" Sybil attack:

Malicious nodes in a network may not only impersonate one node, they could assume the identity of several nodes, by doing so undermining(destroy) the redundancy(repeating) of many routing protocols. This attack is called the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for storage, routing mechanism, air resource allocation and misbehavior detection.

"3.7"Wormhole attack:

Wormhole attacks are malicious nodes that tunnel messages between two different parts of the network via a high speed link. This can make distant nodes appear "closer" in the network, which can be useful as part of a Sybil attack.

"4." Intrusion detection in MANETS

IDS can be defined as the protector system that automatically detects malicious actions within a host or a network, and consequently generates an alarm to alert the security tools at a location if intrusions are considered to be illegal on that host or network. Intrusion detection can be defined as a process of monitoring actions in a system, which can be a computer or network system. Which this is achieved is called an intrusion detection system.

(IDS). Intrusion detection provides the following:
•Monitoring and analysis of user and system activity,
•Auditing of system configurations and vulnerabilities,
•Assessing the integrity of critical system and data files,
•Numerical analysis of activity patterns based on the matching to known attacks
•Irregular activity analysis,
•Operating system audit

"4.1". Intrusion Response

The type of intrusion reply for wireless ad hoc networks depends on the type of intrusion, the network protocols applications in use, and the confidence (or certainty) in the evidence.

A few likely responses include:
• Reinitializing communication channels between.
• Identifying the compromised nodes and reorganizing the network to prevent the compromised Nodes.
• The IDS agent informing the end user, who may in turn do his/her own inquiry and take appropriate action.
• Initiating a re-authentication request to all nodes in the network to prompt the end users
To authenticate themselves (and hence their wireless nodes)using out-of-band mechanisms Only the re-authenticated nodes, which may collectively discuss a new communication channel, will recognize each other as legitimate. That is, the compromised/ malicious nodes can be excluded .Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

"4.2" Classification of IDS

There have been many approaches to intrusion detection in MANETs. The initial classification is based on authentication based schemes. These rely on the identification of nodes by a unique identifier. Use of encryption keys fall into this category, and they have been deeply studied. The second approach is behavioral based algorithms where intrusion is defined based on nodal activities, rather than its identifier. It is a better approach for the following reasons:

1. Node identities can be easily stolen. Behavior is tougher to replicate.
2. Identity based behavior involves storage of Identifier databases or logic
3. Each new node has to be given a unique identifier, making the process of deployment more expensive(time and cost).

IDS may be classified as either host-based or network based, depending on the data collection method.

"4.2.1Host-based IDS

Host based IDS operate on the operating system's audit trails, system and application logs, or assessment data generated by loadable-kernel modules that intercept system calls.

"4.2.2" Network-based IDS

Network-based IDS operate on packets captured from network traffic. In addition, IDS may be classified based on the detection procedure as described below:-

"4.2.2.1" Anomaly Detection

In such systems, a baseline profile of normal system activity is created. Any system activity that deviates from the baseline is treated as a possible intrusion. The problems with this approach are:
1. Anomalous activities that are not intrusive are flagged as intrusive (false positives)
2. Intrusive activities that behave in a non-anomalous manner are not detected (false negatives).
Anomaly detection for mobile computing may demand that the normal profile be periodically updated and the deviations from the normal profile computed. The periodic calculations can impose a heavy load on some resource constrained mobile devices. Every node in the network participates, and runs an IDS agent runs which performs local data collection and local detection, whereas cooperative detection and global intrusion response can be triggered when a node reports an anomaly. consider two attack scenarios separately - abnormal updates to routing tables, and detecting abnormal activities in layers other than the routing layer; these formed the definition of the anomaly.

"4.2.2.2" Misuse detection

In misuse detection, decisions are made on the basis of the signature of an intrusive process, and the traces it leaves in the observed system. Legal behavior is defined and observed behavior compared against it to recognize intrusions. Such a system tries to detect evidence of intrusive activity irrespective of any knowledge regarding the background traffic (i.e., the historical behavior of the system). They define misuse/attack signatures using variables in SNMP Management Information Bases (MIB) variables.

"4.2.2.3"Specification based detection

This defines a set of constraints that describe the correct operation of a program or protocol, and monitors the execution of the program with respect to the defined constraints. This technique may provide the capability to detect previously unknown attacks, while exhibiting a low false positive rate.Tseng; Balasubramanyam et al propose an IDS based on this approach. Their approach uses finite state machines to specify correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. Similar work for DSR has been done by P.Yi, Y.Jiang at al .

"4.2.2.4" Compound detection

An improvement over misuse and anomaly detection is compound detection, which is misuse inspired system that forms a compound decision based on both the normal behavior of the system and the intrusive behavior of the intruder. The detector operates by detecting the intrusion against the historical, normal traffic in the system. These detectors are said to have a greater accuracy in detecting undefined behavior. They would at the very least be able to qualify their decisions better.M.Alam, T Li et al, propose an IDS which uses a quantitative method of anomaly definition based on transmission characteristics, but factors in historical transmission behavior of the node.

"5.".ARCHITECTURES FOR IDS IN MANETS

The network infrastructures that MANETs can be configured to are either Flat or multi-layer, depending on the applications. Therefore, the optimal IDS architecture for a MANET may depend on the network infrastructure itself. In a flat network infrastructure, all nodes are considered equal, thus it may be suitable for applications such as virtual classrooms or conferences. And multi-layered network infrastructure, nodes may be partitioned into clusters with one cluster head for each cluster. To communicate within the cluster, nodes can communicate directly. However, communication across the clusters must be done through the cluster head. This infrastructure might be well suited for military applications.

There are four major architectures on the network, as follows:

"5.1" Stand-alone Intrusion Detection Systems:

Stand-alone intrusion detection system is run on each node independently to the determine intrusions. Every

decision made is based on information collected at its own node, since there is no collaboration among nodes in the network. So, data is not exchanged. In addition, nodes in the same network do not know anything about the situation on other nodes in the network as no prepared information is passed. Even though this architecture is not effective due to its limitations, this architecture is more suitable for smooth network infrastructure than for multi-layered network infrastructure.

"5.2" Distributed and Cooperative Intrusion Detection Systems:

An IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating an answer independently, this architecture is more suitable for flat network infrastructure.

"5.3" Hierarchical Intrusion Detection Systems:

This architecture [4] is an extended version of the distributed and cooperative IDS Architecture. This architecture proposes using multi-layered network infrastructures where the Network is divided into clusters. The architecture has cluster heads, in some sense, act as Control points which are similar to switches, gate ways, and routers in wired networks. It also aggregates information from the member nodes about malicious activities. Cluster-head detects attacks as member-nodes could potentially reroute, modify or drop packet in transmission. At the same time all cluster-heads can cooperate with central base station to form global IDS.

"5.4" Mobile Agent for Intrusion Detection Systems:

The mobile agent for IDS architecture uses mobile agents to perform specific task on a nodes Absence the owner of the agents. This architecture allows the distribution of the intrusion Detection tasks. There are several advantages using mobile agents for intrusion Detection. A flow model of intrusion detection architecture of CBID which consists of 4modules. These modules are linked with each other for valuable intrusion detection. The information collected during the training phase in the logging module is passed regularly to the intrusion information module to perceive threshold value for the usual traffic. This threshold value is further used for the traffic during the testing phase to check intrusive activity.

"6." SIMULATION SOFTWARE

"6.1" GloMoSim

This is a public domain simulator developed by UCLA. Parsec is a C-based simulation language, developed by the Parallel Computing Laboratory at UCLA, for sequential and parallel execution of discrete-event simulation models. GloMoSim currently supports protocols for a purely wireless network. It is built using a layered approach that is similar to the OSI seven layer network architecture. Standard APIs are used between the different simulation layers.GloMoSim has moved away from creating each of the OSI layers as a separate entity to representing each node as a single entity, with each layer being represented only by standard APIs to initialize, finalize etc. They claim that this not only allows sharing of memory areas that all OSI layers need to access , but also allows for better performance, scalability and ease of programming use. GloMoSim is thus perceived to be modular, easy to use and flexible while maintaining a high degree of detail. GloMoSim needs the Parsec compiler, and coding knowledge of C and Parsec (to a lower extent), as stated by the authors. Qualnet is the commercial flavor of GloMoSim, and has additional implementations of layers/modules and features like GUI based analysis tools.

"6.2" OPNET Modeler Wireless Suite

OPNET claims to be the fastest simulation engine among leading industry solutions. It has a wide variety of niche simulators for the wired/wireless areas. It also has many of wired/wireless protocol and vendor device models with source code, and allows Object-oriented modeling of components. It has a hierarchical modeling environment, and has a slightly more complex method of definition of nodes as finite state machines. They also have an optional System-in-the-Loop to interface simulations with live systems. The simulator is flexible, allows integration with other libraries and simulators. The setup, configuration can be done with help from a rich suite of integrated, GUI-based debuggers and analyzers. OPNET is available at special rates for universities.

"6.3"NS2

NS-2 is widely used in the research community. It has grown via contributions from the research community as well as DARPA, Xerox etc, and is available free. It is a object-oriented discrete event simulator that follows the layered approach, and is accompanied by a rich set of protocols. It is also an emulator, and can talk

to real networks. However, to its disadvantage, it has a large footprint, and is not very scalable. It also ranks low on the flexibility and ease of use fronts. Also, the process to include/implement new protocols is complex**.**

"6.4" OMNet++

OMNet++ is an open source, open architecture simulator. Its components are defined by nested hierarchical modules in a simple text based language which is easy to learn, while being very expressive. The behavior of these components can then be elaborated in C++. OMNet++ offers an easy to use GUI for graphical network editing, animation and configuring simulation runs. OMNet++ has a basic output analyzer, which can display collected statistics in graphical formats. It is well documented, and has discussion forums. It is scalable too. However, not many OSI/mobility related models are implemented. Nevertheless, its base infrastructure is very extensible, and it is easy to modify. This offsets the lack of implemented models this to a certain extent. Thus, OMNet++ is perceived to be a good choice when a lot of customization or development is expected.

"7." Conclusion

The paper deals with the entire details of MANETs and explains the features, attacks and role of intrusion detection in MANETs. It also explains the classifications of Intrusion Detection methods and the problems related with that. Various simulators that can be used in MANETs are discussed in this paper.

"8." References

[1] Joo B. D. Cabrera, Raman K. Mehra, and Carlos Gutirrez. Ensemble methods foranomaly detection and distributed intrusion detection in mobile ad-hoc networks.International Conference on Mobile Computing and Networks, 9(1), January 2008.

[2] Tao Li, Min Song, and Mansoor Alam. Compromized sensor node detection: A quantitative approach. IEEE International Conference on Distributed Computing Systems,pages352–357,2008.

[3] Crina Grosan, Sugata Sanyal, Bhavyesh Divecha, and Ajith Abraham. Impact of node mobility on MANET routing protocols models. Journal of Digital Information Management, February 2007.

[4] Carl Hartung, James Balasalle, and Richard Han. Node compromise in sensor networks: The need for secure systems. January 2005.

[5] Patrick Albers, Olivier Camp, Jean-Marc Percher1, Bernard Jouga, Ludovic Me, andRicardo Puttini. Security in ad hoc networks: a general intrusion detection architectureenhancing trust based approaches. 2005

[6] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha. Intrusion detection in wireless ad hoc networks. IEEE wireless communications, February 2004.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. Computer Networks,38(4):393–427,2002.

[8] Tracy Camp, Jeff Boleng, and Vanessa Davies. Wireless Communication and MobileComputing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trendsand Applications. IEEE International Conference on Distributed Computing Systems,2(5):483–502, September 2002

[9] Dharma Prakash Agrawal and Qing-An Zeng. Introduction to Wireless and Mobile systems. Nelson, a division of Thomson Canada Limited, http://www.nelson.com.

[10] Panagiotis Papadimitratos and Zygmunt J. Haasl. Secure Routing for Mobile Ad hoc Networks. IEEE Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January2002.

[11] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, and Lixia Zhang. Self-securing adhoc wireless networks. IEEE Symposium on Computers and Communications, February2002.