International Journal of Computing and Business Research
(IJCBR)
ISSN (Online) : 2229-6166
Volume 4 Issue 1 January 2013

A comprehensive study of latest security models for MANETs: Covering Intrusion Detection and Denial of Service Attacks

Deepak Verma, Renu Jain
Dept of Comp. Sci. & Engg., UIET, CSJM University, Kanpur, {deepak300572,jainrenu}@gmail.com
Ashwani Kush
Dept of Comp. Sci., University College, Kurukshetra University, akush@kuk.ac.in

Abstract
Mobile Ad Hoc Networks (MANETs) are self organizing devices with no infrastructure control. Concept of security is major concern because of changing topology and no centralized control. Since MANET's are prone to many kind of vulnerabilities it is not necessary that any one kind of attack may be active at a moment hence there is a need to have a security system which could take into consideration many possibilities at the same time. The problem of intrusion detection and denial of service attack have been discussed in this paper. The objective of the paper is to present the recent work that is being done for intrusion detection and denial of service attack and also to emphasize on the fact that there is a need of work to be done to provide a comprehensive solution for intrusion detection and denial of service attack prevention, which are the two most prominent vulnerabilities of MANETs.

1.0 Introduction

Mobile Ad hoc Networks are Nodes (generally Hand held devices) which communicate with each other in the limited area forming a network for the purpose of sharing information. The network is short lived and does not require any wired links. Such a network generally does not have any central authority to authenticate the nodes or to manage the routing. Every node has the responsibility of routing as well. Due to its distributed nature in terms of authentication and open air access the security aspects in terms of confidentiality, authentication, integrity, availability, access control and non repudiation become more important. The usefulness of MANET's is due to its ease of deployment which leads to the only possibility in case of disaster management, military operations and situations where there is urgent and short lived need of a network.

2.0 Security Aspects

In case of Mobile Ad hoc networks security is the most important factor to be addressed apart from other issues like resource constraint, power constraint etc. some of the key issues are:

Confidentiality is to make sure that the information sent to the destination node is not read by any unauthorized user or node throughout the path.

Authentication is to be able to identify a node or a user so as to prevent impersonation.

Integrity is to keep the message safe from being altered or destroyed on the path.

Non-repudiation is making sure that if an entity has sent a message it cannot deny from the fact.

Availability is to ensure that the resources or services provided by the systems in the network are made available to the genuine user.

2.1 Attack Classifications

Broadly an attack can be in any one of the following category:

- **Passive Attacks:** Such kind of attacks involves probing into the data being exchanged without altering it; these attacks do not disturb the normal functioning of the network.
- **Active Attacks:** Such kind of attacks involves altering or destroying the data being exchanged thereby disturbing the normal functioning of the network. These attacks could be externally initiated or internally initiated by malicious nodes.

Some of the attacks in these categories that are of major concern are:

2.2 Denial of Service attacks: Such attacks attempt to hamper the service availability or attempt to prevent the rightful user from accessing the network. DoS attacks are performed by consumption of scarce, limited resources or by destructing or altering of configuration related information or by physically mishandling the network components. DoS attacks exploit flaws in operating systems, network interfaces, network protocols or software's being used. Examples are like injecting large amount of junk packets into the network or forcing the routing table to overflow.

2.3 Intrusion Detection: is the means to find such malicious nodes in the network which (a) May not be legitimate member of the network i.e. it pretends to be part of the network (b) May be a legitimate node of the network but its activities are against the expected normal behavior.

Intrusion detection techniques could be: (i) Signature based intrusion detection which uses pre-known attack scenarios (or signatures) and compare them with incoming packets traffic (ii) Anomaly based intrusion detection which attempts to detect activities that differ from the normal expected system behavior.

3.0 Recent Studies:

Researchers have tried to secure MANET's against intrusion and denial of service attacks in many ways. The study shows that solutions for these attacks on MANET's have been attempted separately but solutions that could cater to more than one kind of attacks are seldom available. Some of the important contributions have been discussed in this section.

R. Nakkerran et al. [1] in their work have incorporated agents and data mining techniques to prevent anomaly intrusion in mobile ad hoc networks.

Different modules in the proposed system are home agent, cross feature analysis for classifier sub model construction, local integration and global integration. As depicted in the proposed system architecture Figure 1 .

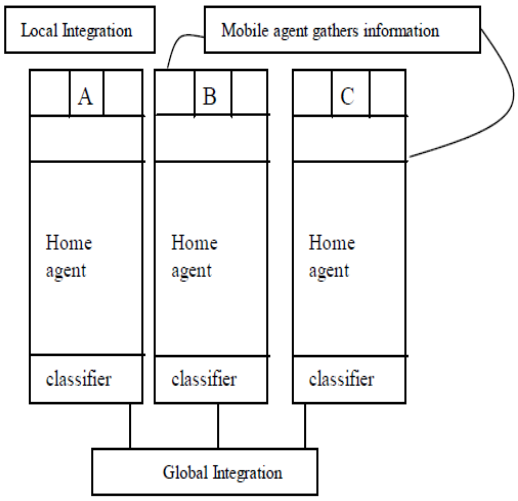

Fig 1: Proposed System Architecture.

Home agents present in each system, collect the data from its own system and use data mining techniques to observe the local anomalies. The Mobile agents monitor the neighboring nodes and collect the information from neighboring home agents to determine the correlation among the observed patterns before it will send the data. Their system was able to stop all the attacks successfully in an ad hoc network and reduce the false alarm positives. The system is cooperative and distributive; it considers the anomaly detection result from the neighbor node(s) and sends the current working node's result to its neighbor node(s). The implementation has been done considering DSR protocol. This system has not been tested for scalability, where the control traffic would increase drastically reducing the efficiency of the solution.

Peyman Kabiri et al. [2] have analyzed network features using principal component analysis. Their work purposes a neighbor monitoring intrusion detection based on the traffic profile of the node, where feature selection is used to improve its performance. The proposed approach uses the anomaly based intrusion detection method. In the reported work 16 features in the network traffic are monitored. The paper, intends to show the difference between the normal operating state of a network and the operating state of the network once it experiences a DoS attack. In the anomaly based intrusion detection, the profile of the network in its normal state of operation is initially extracted. Later on this profile is compared with the current state of the network. On detecting any deviation from the normal state of operation in the network, system will produce an alarm message to show the anomalous behavior. Their work intends to reduce the dimensionality of the network features so as to increase in intrusion detection speed. Network features such as movement and number of the nodes are also considered in the reported work. PCA (principal component analysis) is used to analyze results of the scenario based Adhoc network simulations. The network features that are addressed by the author are as follows: My address, Destination address, Route REQuest (RREQ) from node-I, Route REPly

(RREP) from node-I, Route error from node-I, Total packet received from node-I, My received sent packet, ACK packet from node-I, Traffic sent from node-I, Total received RREQ, Total RREP, Total received (Route Request ERror) RRER, Total Traffic received, Total ACK received, Timestamp and DSR header. Author has considered only traffic related features for intrusion detection.

Farhan Abdel-Fattah et al. [3] presented dynamic intrusion detection method for mobile ad hoc network by combining two anomaly methods namely conformal predictor k-nearest neighbor and distance based outlier detection (CPDOD) algorithm.

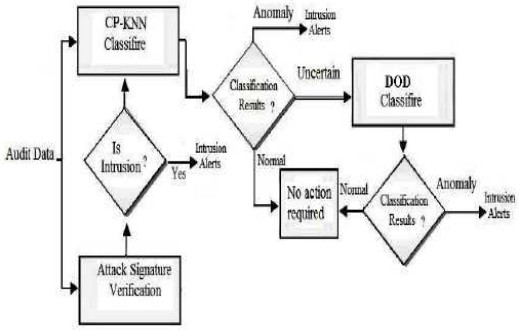

Fig. 2 Structure of CPDOD algorithm.

Proposed algorithm as in Figure 2 above employs two different metrics to improve detection ability. The nonconformity metric measures whether the unknown instance is more similar to known normal instances or abnormal instances. The Outlier Factor LDOF metric identifies the similarity to normal classes and detects abnormal attacks. The algorithm has been tested for resource consumption attack, dropping routing traffic attack and black hole attack. Since the algorithm used is commonly used machine learning and data mining technique its time of convergence for intrusion detection has to be considered.

Ningrinla Marchang et al. [4] have implemented collaborative techniques for intrusion detection. In this paper authors have proposed two intrusion detection techniques which use collaborative efforts of nodes in a neighborhood to detect a malicious node in that neighborhood. The first algorithm is for detection in a clique this technique is designed for detection of malicious nodes in a neighborhood of nodes in which each pair of nodes in the neighborhood are within radio range of each other. Such a neighborhood of nodes is known as a clique. The second algorithm is for detection in a cluster this technique is designed for detection of malicious nodes in a neighborhood of nodes, in which each pair of nodes may not be in radio range of each other but where there is a node among them which has all the other nodes in its one hop vicinity. Both techniques use message passing between the nodes. A node called the monitor node initiates the detection process. Based on the messages that it receives during the detection process, each node determines the nodes it suspects to be malicious and send votes to the monitor node. Node that initiates the algorithm is referred to as monitor node. The monitor node upon inspecting the votes determines the malicious nodes from among the suspected nodes. Proposed intrusion detection system is independent of any routing protocol.

The algorithm has been mainly checked for reliable channel. Algorithm works well for unreliable channel where the percentage of collision is around 5%.

Lawan A. et al. [5] describes some of the major vulnerabilities associated with wireless networks, demonstrates different methods of achieving denial of service (DoS) attacks and proposes different countermeasures so as to minimize the attacks. Authors has concentrated on IEEE 802.11 technology to achieve DoS attacks and have proposed the general intrusion detection/prevention architecture Fig. 3. The paper discusses vulnerabilities in wireless networks like highway war driving attack, packet capturing, flaws in link layer encryption algorithm associated with WEP, ARP poisoning, MAC spoofing, WEB spoofing, ICMP flooding etc.

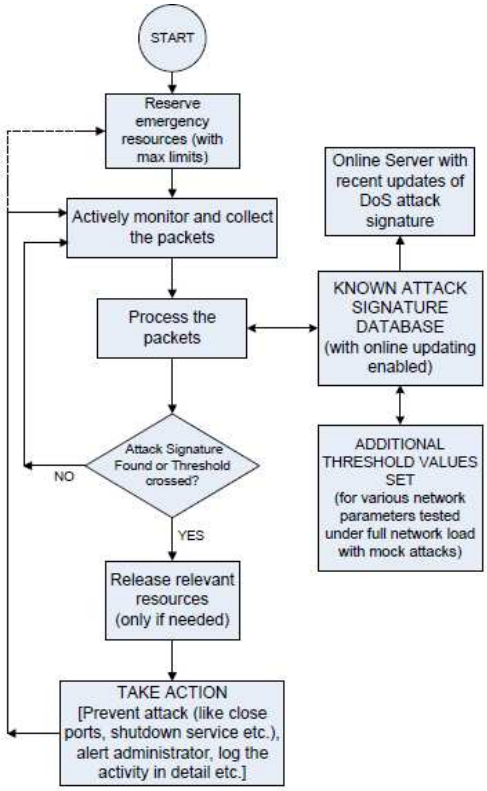

Fig. 3 General intrusion architecture flow chart.

Some of the proposed solutions by the authors are as follows: against spoofing use network switches that have MAC binding features that store the first MAC address that appears on a port and do not allow this mapping to be altered without authentication. Another alternative proposal is to make ARP negotiation centralized. Making ARP request unicast can save lot of congestion. Adding authentication to know the identity of the sender or against packet tampering makes it secure. ARP request packets can be sent to a central server which has the IP-MAC address mapping and the server can sent the ARP response with a strong

digital signature using a collision free one way hash function to the requested host. This can protect against tampering or injection of forged ARP packets. Host can send an encrypted acknowledgement with the timestamp of the server response. Related to flooding attack author proposes a general architecture for an intrusion detection or prevention system, especially against flooding attacks or other variants. There can be fine tuning done with the ability for self-learning and correcting false decisions through statistical/AI approaches as it lives longer in the network. Initially test installation can be done and a variety of mock DoS attacks can be performed. During the test period the suspicious attacks may only be alerted to the administrator. When satisfactory attack reaction results are obtained, it can be installed and made active. The attack signature database may be updated online in regular intervals to keep it up-to-date. Administrator can set threshold values. Once the threshold values are crossed, some specific action may be taken. To avoid false positives, the system must be trained and the optimal values should be set. Author has tried to present the shortcomings of IEEE 802.11 technology.

Kemal Bicakci et al. [6] presented a systematic survey of DoS attacks, which exploits MAC and Physical layer vulnerabilities of IEEE 802.11 networks. Authors discuss and compare available countermeasures against DoS attacks. A security extension model is proposed Fig. 4 in which the central entity coordinates the security countermeasures against DoS attacks.

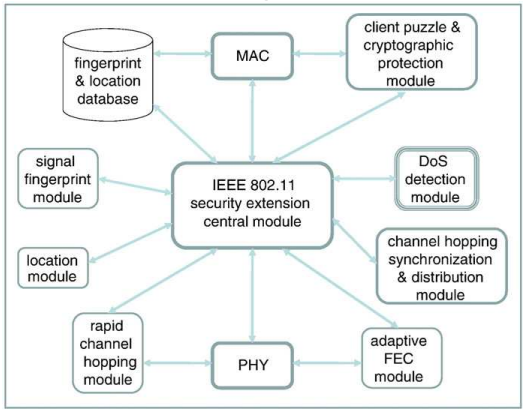

Fig. 4 proposed security extension.

This module is positioned in between MAC and PHY layers. It continuously monitors the data coming from other modules and decides whether an attack is in progress or not. Location and signal fingerprint modules are used for determination of the positions and signal fingerprints of neighboring nodes and the data coming from these modules are merged in a central entity called the fingerprint and location database. MAC address spoofing based attacks can be identified more robustly by using the data kept in this database e.g. MAC address, associated signal fingerprint vector and associated location information. Client puzzle and cryptographic protection module communicates with the central module to parameterize DoS countermeasures in the MAC layer. Rapid channel hopping and adaptive FEC modules are used as a countermeasure when an ongoing jamming operation is detected. The coordination necessary for the channel hopping of the stations and APs is provided by the channel hopping

synchronization and distribution module. Author has discussed mainly attacks at MAC and physical layer.

Ibrahim, M.M et al. [7] have worked on AODV based networks to prevent flooding attack using real time host intrusion detection. Authors propose a algorithm REHIDAN (i.e. Real-time Host Intrusion Detection for Ad hoc Networks) which identifies the flooding attacker nodes. It also takes the appropriate countermeasures to minimize the effectiveness of the attack and maintain the network performance within the accepted limits. The solution reduces the effect of the flooding attack by reducing the ratio of end-to-end delay and routing overhead.

Osathanunkul, K. et al. [8] present a countermeasure to black hole attacks in mobile ad hoc networks. Authors describe a solution to counter black hole attacks on the Expected Transmission Count (ETX) which is a common routing metric in MANETs. The solution is called the Secure ETX (SETX) protocol. The protocol allows nodes to measure neighbors' delivery ratios directly. The proposed protocol without incurring much overhead can improve the network performance even in the presence of black hole attacks.

4.0 Conclusion

A survey has been conducted for various intrusion detection schemes and denial of service attacks and their countermeasures. Major features have been highlighted in both the cases. It was found that no one scheme is able to remove all the attacks at one time. Either independent schemes will be used to achieve different categories of security or a multi-fence security system will be required. In future course of action majorly protocols will be analyzed such as SAODV, SAR, ARAN etc.

References

1. R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai, "Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks", IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010
2. Peyman Kabiri and Mehran Aghaei, "Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks", International Journal of Network Security, Vol.12, No.1, PP.42-49, Jan. 2011
3. Farhan Abdel-Fattah, Zulkhairi Md. Dahalin and Shaidah Jusoh. "Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010
4. Ningrinla Marchang and Raja Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks", Science Direct Ad hoc Networks 6 (2008) 508-523
5. Lawan A. Mohammed and Biju Issac, "Detailed DoS Attacks in Wireless Networks and Countermeasures", International Journal of Ad Hoc and Ubiquitous Computing, Vol. 2, No. 1, 2006
6. Kemal Bicakci and Bulent Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", Computer Standards & Interfaces 31 (2009) 931–941
7. Ibrahim, M.M., Sadek, N. and El-Banna, M, "Prevention of flooding attack in wireless ad-hoc AODV-based networks using Real-time Host Intrusion Detection", WOCN'09 proceedings of sixth international conference on Wireless and Optical Communications Networks, 2009. 424-428
8. Osathanunkul K. and Ning Zhang, "A countermeasure to black hole attacks in

mobile ad hoc networks", IEEE International Conference on Networking, Sensing and Control (ICNSC), 2011