IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 4 (Nov-Dec. 2012), PP 40-45
www.iosrjournals.org

A Study on Various protocols Developed under Intrusion Detection System in Adhoc Networks

[1] Jatinder Singh 2 Bobson Gandhi [3] Shailender Kumar
[1] Student CSE AIACTR, IPU Delhi, India [2]Student AIACTR, IPU Delhi, India
[3]Assistant Professor AIACTR, IPU Delhi, India

Abstract: *In Computer Networks a number of security techniques provide security consolation but not up to optimal security extent. There are massive attacks and efficient viruses travel across the network which incapacitates computer system and default configuration of the operating system. Preceding techniques can capture anomalous activities and previous known attacks but unknown Security attacks have learned to survive in a high secure precinct, it must be noticed that virus has an augmenting influence, so it is very difficult to detect unknown attacks at application layer on the run time.*

This paper presents some of the best well known Intrusion detection techniques and appropriate protocols which were proposed for intrusion detection and anomaly detection in the recent years under various parameters.

Keywords: *Security, Intrusion Detection, Attacks, Routing.*

I. Introduction

A mobile ad-hoc network or MANET is an autonomous system of mobile routers (and associated hosts) connected by wireless union of links which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily. Thus, the network's wireless topology may change rapidly and unproductively .Such a network is developed in 'Ad-hoc' basis without any pre-existing infrastructure and may operate in either stand alone fashion or may be connected to the Larger Internet.

The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not.

Passive attacks:

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated.Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, there by making it impossible for the attacker to get useful information from the data overhead.

Active attacks:

An active attack attempts to alter to destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network.Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks.

II. Security Attacks In Adhoc Networks

There are various types of attacks on ad hoc network which are described as follows [6]:

2.1 Wormhole

The wormhole is one of the challenging attacks in the ad hoc routing in which two malicious nodes forms a tunnel with high transmission connectivity referred as a wormhole tunnel. Wormhole tunnels can be established by means of a wired link, high quality wireless out-of-band link or a logical link via packet encapsulation.

After building a wormhole tunnel, one attacker receives and copies packets from its neighbors, and forwards them to the other colluding attacker through the wormhole tunnel. This latter node receives these tunneled packets and replays them into the network in its vicinity. In a wormhole attack using wired links or a high quality wireless out-of-band links, attackers are directly linked to each other, so they can communicate swiftly. However they need special hardware to support such communication.The solution to the wormhole attack is packet leashes.

2.2 Black Hole

Black hole attack is one such attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. The first solution for black hole is to find more than one route to the destination and the second solution for black hole is to exploit the packet sequence number included in any packet header.

2.3 Denial of Service

A Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of his/her network connection.Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' access to a service provider.Specific instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the anticipating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.They have numerous forms and they are hard to prevent.

2.4 Distributed Denial of Service

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. A DDoS attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded.

2.5 Rushing Attack

On demand routing protocols that use route discovery process are vulnerable to this type of attack. An attacker node which receives a “route request” packet from the source node floods the packet quickly through out the network before other nodes which also receive the same “route request” packet can react. Nodes that receive the legitimate “route request” packet assume those packets to be the duplicates of the packet already received through the attacker node and hence discard those packets. Any route discovered by the source node would contain the attacker node as one of the intermediate nodes. Hence the source node would not be able to find secure routes.

2.6 Gray hole attack

We now describe the gray hole attack on MANETS. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes.

III. Issues In Secure Routing

Computer network is the source of transmission between the machines, important information travels across the network and on the global network (Internet) but that information is accessible.Network has become very risky and unsecure, precarious security is provided but every internet user wants to secure concern network up to optimal and acceptable extend, any machine that is connected to the global network (Internet) directly or under another domain, it has security threats.

Firewalls and routers are used to detect massive kind of virus and worms but it is possible when the virus or worm is already defined in signatures and it can also be detected when the virus is already spread. In order to spot these suspicious actions we use Intrusion Detection Systems (IDSs) and Intrusion Detection System is usually categorized as misuse based system or anomaly based system.

Intrusion Detection System (IDS) is normally practiced for identifying malicious activities and their resources. Misuse based system maintains records for description of attacks and signatures that are used to detect the attacks where anomaly based system has feature of detecting previously unknown attacks.

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
- Statistical analysis of activity patterns based on the matching to known attacks
- Abnormal activity analysis
- Operating system audit

There are three main components to the Intrusion detection system

Network Intrusion Detection system (NIDS) – performs an analysis for a passing traffic on the entire subnet. Network Node Intrusion detection system (NNIDS) – performs the analysis of the traffic that is passed from the network to a specific host.Host Intrusion Detection System (HIDS) – takes a snap shot of your existing system files and matches it to the previous snap shot.

In all these attacks DoS (denial of service) is the most common attack. Under this attack various protocols will be compared in Intrusion Detection system which is the most widely used prevention technique under DoS(Denial of service).

IV. Literature Review

Dr Manish Shrivastva and Sneha Kumari proposed a technique in 2012 ,Secure energy efficient routing is very essential in MANET[3]. We have observed the different approaches used to bring secure energy efficiency in routing. These approaches make them efficient but then also it can't go beyond a limit. This makes us for the search of new innovative approaches. Secure energy efficient routing techniques play a significant role in saving the energy consumption of the network. There are many existing MANET routing protocols as described above, each one is having its own advantages as well as disadvantages. After looking through the existing protocol, we decided to design a secure energy efficient routing protocol which reduces the total energy consumption in the network and thus maximize the life time of the network. We proposed first efficient intrusion detection technique for security and secondly proposed a new energy efficient dynamic source routing protocol which is based on the minimum-hop fixed-transmit power version of DSR.

Prajeet Sharma, Niresh Sharma And RajdeepSingh 2012 proposed a mechanism protects the network through a self organized, fully distributed and localized procedure[4]. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

M. Kumar, Dr. M.Hanumanthappa & Dr. T. V.Suresh Kumar , 2011 proposed Positive Alert Reduction Technique for reducing the false positive alarm rate. According to author network Intrusion Detection System (IDS) is very susceptible for identifying and detecting network attacks but whenever Intrusion Detection System predict any intrusion, it activates alarm for security alert but there are thousands of activities running across the networks; Intrusion Detection System (IDS) generates thousands of alarm on scents of suspiciousness of any particular activity, it is fact that most of them are false. To avoid the discussed problems author has propose Alert Reduction Technique. In this technique it has been recommended to update the desired patches and updates the security signatures. Author has compared this technique with sensor level and log alert technique and suggested the proposed technique among previous contribution. The technique was proposed by identifying Spoofing attack, malicious use attack, known and unknown attacks. Weakness of this proposed technique is that, it cannot detect newly born unknown attacks as this attack was identified problem for proposed solution but the results are false in case of unknown attacks.

D.Md. Farid, N.H. Hoa, J.Darmont, N.Harbi& M.ZahidurRahman, 2010 proposed Self-AdaptiveNaïve Bayesian Tree (NBTree) which is used for anomalous based intrusion detection[7]. Author has presented a new learning algorithm for Naive Bayesian Tree by which the performance of Naive Bayesian Tree (NBTree) has been enhanced and the detection has been scales up for different types of known attacks,it has also recorded a decrease in the rate of false positive alarm. According to author the Naive Bayesian Tree (NBTree) provide similarity to traditional recursive partitioning schemes, Naive Bayesian Tree (NBTree) is a fusion and crossbreed approach that exploits the advantages of both decision trees and Naive Bayesian Classifier. This amalgamation of decision tree and Naive Bayesian Tree provide Improved Self-adaptive NBTree. The proposed solution takes datasets of analyzed information as input and as output it presents hybrid decision trees with Naive Bayesian classifier.

Pasquale Donadio, Antonio Cimmino and Giorgio Ventre 2010, Grid based Intrusion Detection System (G-IDS)[1] that uses the basic principles of the Grid computing and apply them to the intrusion detection mechanisms, in order to define a new process capable to protect networks characterized by the constantly changing of the topology. In this they used a distributed traffic analyzer that operates a real-time feedback sharing the results between the neighboring nodes of the network.

S Sen 2010, proposed a "grammatical evolution approach to intrusion detection on mobile ad hoc networks"[2]. They use artificial intelligence based learning technique to explore design space. The grammatical evolution technique inspired by natural evolution is explored to detect known attacks on MANETs such as DOS attacks and route disruption attacks. Intrusion detection programs are evolved for each attack and distributed to each node on the network.

Er. Shivani Sharma and Er. Tanupreet Singh 2009, have used a sensor network simulation based on the simulation package by the Naval Research Laboratory (NRL) running on NS2[11]. The package included a new routing protocol for the phenomenon broadcast packets called PHENOM routing protocol. Selected anomaly-based IDS is characterized into training and testing phases, defined below:

Training phase is such that the training data contains both normal and abnormal data. We assume that attack data will not occur frequently as normal data would.Testing phase analyses the traffic generated on the network based on the information gathered from the testing phase.

K.K.Gupta,B.Nath & Ramamohanarao 2007, proposed The conditional random field's technique, the technique is used in a toolkit (CRF++) as a model[8]. Author has anticipated the technique as best among the previous techniques, and defined the Conditional Random Fields (CRT) as a unique technique for task of intrusion detection. In the experiment among the other techniques it was recorded a very high rate of accurate results for intrusion detection. It is also one of the best feature in among other techniques that proposed technique can be used without client server environment, where number of other techniques are proposed for the client server environment (research labs etc.). The proposed technique is a directionless graphical model, it used for the task of sequence classification and labeling, unlike the other models which prefer joint distribution the Conditional Random Fields model favor conditional distribution.

TABLE 1 SUMMARY OF VARIOUS DISCUSSED TOOLS LITRATURE REVIEW

Author(s)	*Name of Proposed Protocol*	*Summary*	*Identified Problem(s)*	*Proposed Solution*	*Data used*	*Implemented*	*Limitations*
DrManish Shrivastvaand Sneha Kumari 2012	Secure Routing Protocol	Effectiveness of Energy Efficient Protocol Better than normal DSR protocol	How to provide maximum life and security to nodes (energy constraints)	New energy and efficient DSR protocol based On minimum hop fixed transit power	YES	YES	Invisible node attack is applicable to several proposed secure routing protocols
Prajeet Sharma Niresh Sharma And Rajdeep Singh 2012	Secure IDS technique in DDOS attack	Use of different Intrusion Detection parameter to increase security	Need for a centralized trusted authority which is not practical in ADHOC networks.	Protection of network through a self organization, fully distributed and localized procedure. Changing security parameters.	YES	YES	Routing load is very high , congestion may occur.
M. Kumar, Dr. M. Hanumanthappa & Dr. T. V. Suresh Kumar 2011	False Positive Alert Reduction Technique	A technique for false positive alert reduction on (SNORT) open source network intrusion prevention and detection system	Spoofing attack, malicious use attack, known & unknown attacks	To review the configurations and update the security patches for reducing the false positive security alert	YES	YES	Newly born unknown attacks can never be detected by proposed solution

D.Md. Farid, N. H. Hoa, J. Darmont, N. Harbi& M. ZahidurRahman 2010	adaptive naive Bayesian tree (NBTree)	An algorithm for anomaly based intrusion detection and implemented on naive Bayesian tree	Denial of service attack, user to root attack, remote to user attack and probing attack	A new learning algorithm to be apply (NBTree) for anomaly based intrusion detection of large volume of audit data	YES	NO	Masquerader attack, port based attack, unknown attacks, results are wrong.
S Sen 2010	Grammatical evolution	Artificial intelligence based learning technique to explore design space	DOS attacks and route disruption attacks	Intrusion detection programs are evolved for each attack and distributed to each node on the network	YES	YES	Fixed-length and fixed-integer rule encoding and the resulting issue of illegal genotypes being generated.
Pasquale Donadio, Antonio Cimmino and Giorgio Ventre 2010	Grid based Intrusion Detection System	Distributed traffic analyzer that operates a real-time feedback sharing the results between the neighboring nodes of the network	Network worm and DOS attacks	Basic principles of the Grid computing and apply them to protect networks characterized by the constantly changing of the topology	YES	NO	Exhibit legitimate but unseen behavior
Er. Shivani Sharma and Er. Tanupreet Singh 2009	PHENOM Routing Protocol		Performance of WSN under realistic situation	Correction and detection of the type of attack made by intruding node.	YES	YES	Challenging problems due to network device
K. K. Gupta, B. Nath& K. Ramamohanarao 2007	Conditional Random Fields	Using conditional Random Fields as a model in a toolkit (CRF++)	Malicious attack, denial of service attack, probing attack, R2L (unauthorized access from a remote machine) or U2R (unauthorized access to root) attack.	To use conditional Random Fields as a model in a toolkit (CRF++) for much robustness and effective result in intrusion detection.	YES	NO	Unknown Attacks cannot be detected by proposed model.

V. Conclusion And Future Work

The work presented is strong on the subject of how to make the intrusion detection system resistant to attack against itself.This paper discusses the nature of the attacks that the system could be subjected to, what assumptions have to be made about these attacks, and how the system counteracts them.

In order to achieve the goal of improving the design process for IDSs, various comparisons have been done.These namely include highly concise schemes for classifying protocols. Current techniques provide security for known attacks in a dedicated network environment and these schemes may serve as the basis for future conceptual work in the domain of ID; Future work will be contributed to standalone machines for further betterment and towards achievements.

References:

[1] Pasquale Donadio,Antonio Cimmino and Giorgio Ventre “Enhanced Intrusion Detection Systems in Ad Hoc Networks using a Grid Based Agnostic Middleware”.

[2] S.Sen and John Andrew Clark “A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad hoc Networks” March 2009, WiSec ’09: Proceedings of the Second ACM Conference on Wireless Network Security.

[3] Sneha Kumari1, Dr. Maneesh Shrivastava Secure DSR Protocol in MANET Using Energy Efficient Int.rusion Detection System Volume 1, No.1, July August- September 2012

[4] Prajeet Sharma Niresh Sharma And Rajdeep Singh A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network Volume 41– No.21, March 2012

[5] Intrusion Detection Technique in Mobile Adhoc Network based on Quantitative Approach Volume 37– No.8, January 2012

[6] Vikas Beniwl, Ashwani Garg A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks, Volume 2, Issue 9, September 2012

[7] D.Md Farid,N.HuuHoa,J.Darmount,N.Harbi, and M.ZahidurRahman, “scaling up detectionrates and reducing false positives in intrusion detection using NBTree”,ICDMKE April 2010

[8] K.KGupta,B.Nath,andK.Ramamohanarao ”Conditional Random Fields for Intrusion Detection”,In International Conference on Advanced Information Networking and Applications Workshops,IEEE,2007

[9] C.Kruegel,D.Mutz,W.Robertson, and F. Valeur,”Bayesian event classification for intrusion detection”,In Proc. Of the19th Annual Computer Security Applications Conference,Las Veges,nv,2003

[10] Amrita Anand* Brajesh Patel An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols Volume 2, Issue 8, August 2012

[11] Er. Shivani Sharma, Er. Tanupreet Singh An Efficient Intrusion Detection System for Routing Attacks in Manets: An Analytical Report ISSN: 2278-7844,2012

[12] Ms. Preetee K. Karmore A Survey on Intrusion in Ad Hoc Networks and its Detection Measures, 2011

[13] Jihye Kim, Gene Tsudik. “SRDP: Secure route discovery for dynamic source routing in MANET’s”. AdHoc Networks, Volume 7, Issue 6, Pages 1097-1109, August 2009.

[14] Nishu Garg, R.P.Mahapatra. “MANET Security Issues”. IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.