Available online at www.elixirpublishers.com (Elixir International Journal)

Adoc Network

Elixir Adoc Network 88 (2015) 36629-36633

ISSN: 2229-712X

An Efficient Intrusion Detection System for Routing Attacks in Manets: AN Analytical Report

Shivani Sharma[1], Tanupreet Singh[1] and Sachin Khurana[2]

[1]Department of Computer Science & Engineering. Amritsar College of Engineering & Technology, Amritsar, India

[2]Department of Management Studies & Computer Applications, Amritsar College of Engineering & Technology, Amritsar, India.

ARTICLE INFO

Article history:

Received: 22 September 2012;

Received in revised form:

20 November 2015;

Accepted: 25 November 2015;

Keywords

MANETS,

IDS,

Security Attacks.

ABSTRACT

Mobile Ad hoc Networks is a collection of wireless mobile nodes, which form temporary networks without relying on any existing infrastructure or centralized administration or standard support services regularly available in wide area networks to which the host may normally be connected. In this paper we review the security attacks on mobile adhoc networks like black hole, grey hole attacks etc. the study on security attacks and intrusion detection system has led us to illustrate some of the particular security issues.

Introduction

Mobile Ad hoc Networks is a collection of wireless mobile nodes, which form temporary networks without relying on any existing infrastructure or centralized administration or standard support services regularly available in wide area networks to which the host may normally be connected [3]. MANET is one of the most important technologies that have gained interest due to recent advantages in both hardware and software techniques. MANET technology allows a set of mobile uses equipped with radio interfaces (Mobile nodes) to discover each other and dynamically form a communication network. MANET incorporates routing functionality into mobile nodes so that they become capable of forwarding packets on behalf of other nodes and thus effectively become the infrastructure. Providing multiple routing paths between any source-destination pair of nodes has proved to be very useful in the context of wired networks [7].

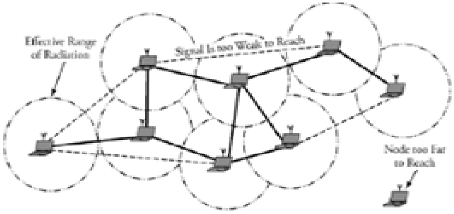


Figure 1: Typical Mobile ad-hoc network Diagram [9]

Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense [1]. Most of the routing protocols for MANETs are thus vulnerable to various types of attacks**.** Security is a main concern in the establishment of MANETs. Literature is abundant in defining protocol extensions to provide more secure MANET communications. Also many techniques have been developed to identify different types of network attacks, such as the wormhole attack, for example. However, all these security solutions are designed for specific routing protocols [6]. In the absence of generic security architecture, nodes from different MANET domains cannot cooperate and benefit from security advantages across the entire network, such as secured inter-domain routing, etc. A lot of challenges come with implementing these networks [15].

Zhang proposed a scheme for intrusion detection in MANET. They proposed distributed and cooperative framework to detect the attack. Every node in the MANET participates in the process of intrusion detection. It detects the sign of intrusion locally and independently and also propagates this information to other nodes in the network [11]. Intrusion Detection is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system and are abusing their privileges. The system protected is used to denote an information system being monitored by the Intrusion Detection system. The Intrusion Detection system (IDS) is a computer system that dynamically monitors the system and user actions in the network and computer system in order.

Attacks On Mobile Ad Hoc Networks [19][20][21]

MANETs like other wireless networks are liable to active and passive attacks. In the passive attacks, only eavesdropping of data happens; while in the active attacks, operations such as repetition, changing, or deletion of data are necessitated. Certain nodes in MANETS can produce attacks which cause congestion, distribution of incorrect routing information, services preventing proper operation, or disable them [7].

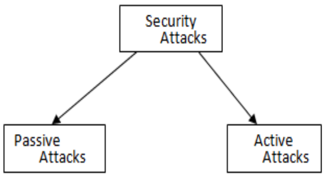
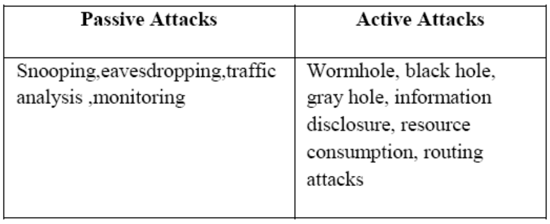


Figure 2: Attacks on Mobile Adhoc Network

Tele:

E-mail addresses: er.sharma04@gmail.com



Passive Attacks	Active Attacks
Snooping,eavesdropping,traffic analysis ,monitoring	Wormhole, black hole, gray hole, information disclosure, resource consumption, routing attacks

Table 1: Network Security Attacks against MANETS

A. Passive Attacks [19]

A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard. There is an attack which is specific to the passive attack a brief description about it is given below:

Snooping

Snooping is unauthorized access to another person's data. It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.

Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

B. Active Attacks [20]

An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.

Wormhole Attack

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

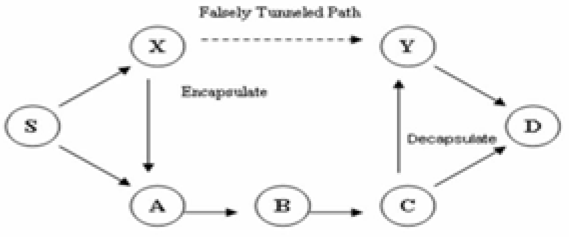


Figure 3: Wormhole attack

Black hole Attack

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

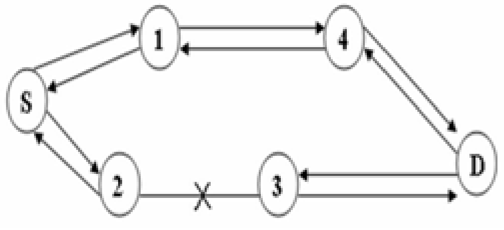


Figure 4: Black hole attack

Gray Hole Attack [21]

Gray Hole attack is the attack on the adhoc network. Gray Hole attack can be act as a slow poison in the network side means we can't said that probability of losing the data. In Gray Hole Attack [6] a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node , When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in its routing table. Otherwise, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination. We now describe the gray hole attack on MANET'S .The gray hole attack has two important stages , In first stage, a malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interrupting or corrupting packets, event though route is spurious. In second stage, nodes drop the interrupted packets with a creation probability. Detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack. A variation of black hole attack s is the gray hole attack, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). Both types of gray hole attacks seek to disrupt the network without being detected by the security measures in place.

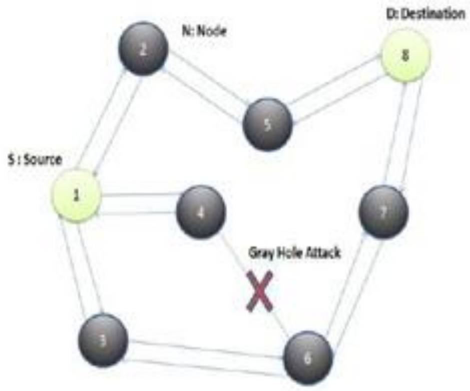


Figure 5: Gray Hole Attack in Mobile Adhoc Network

Analysis Of Anomaly Based Intrusion Detection System [17]

To start with the analysis of the accuracy of the IDS under investigation, we have run preliminary tests to investigate the performance of a WSN under a realistic situation by investigating the network performance with the presence of a phenomenon. We have used a sensor network simulation based on the simulation package by the Naval Research Laboratory (NRL) [14] running on NS2. The package included a new routing protocol for the phenomenon broadcast packets called PHENOM routing protocol.

Simulation Scenario

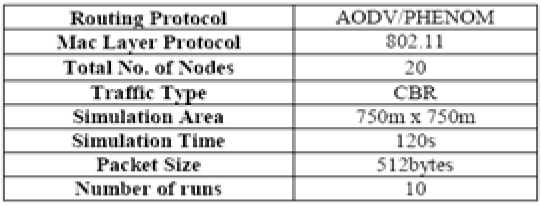
Our simulation scenarios consist of a total of 20 nodes. We configured 18 nodes as sensor nodes, one node as a phenomenon node moving through the network and emitting carbon monoxide (CO), and one sink node which is the data collection point where all the sensor nodes periodically send their sensor report when they sense the phenomenon. The movement of the phenomenon node was randomly generated with speed ranging from 1m/s to 20m/s and an average pause time of 1.0s. Each simulation carried out was done over a time period of 120s. We assumed in our analysis that each sensor node has enough power to operate communication as well as intrusion detection functions. For testing the IDS system, the operation of our approach has been described from the perspective of a set of nodes referred to as the Monitoring Nodes. Nonetheless, all nodes in the network have IDS capabilities and can potentially be monitoring nodes too. Our 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. Hence, less than x% of data is anomalous.

➢Testing phase analyses the traffic generated on the network based on the information gathered from the testing phase.

Simulation Parameters & Results

The common simulation metric definitions used in this paper are given below:



Routing Protocol	AODV/PHENOM
Mac Layer Protocol	802.11
Total No. of Nodes	20
Traffic Type	CBR
Simulation Area	750m x 750m
Simulation Time	120s
Packet Size	512bytes
Number of runs	10

Table 2: Simulation parameters

(a). Packet Delivery ratio (PDR) - The packet delivery ratio is the ratio between the number of packets originated by the "application layer" Constant Bit Rate (CBR) sources and the number of packets received by the CBR.

(b). Packet drop - The number of packets originated by the source but fails to reach the destination node.

Scenario 1 show the average of ten simulation runs with varying seed values. The sensor network performs optimally under normal condition.

Scenario 2 (No attack-STL) was simulated such that five instances were considered with the five pulse rates.

We observed that the higher the pulse rate, the lower the network performance

Scenario 3 (Attack-STL) was implemented with all the configurations in scenario 2. However, three malicious nodes were set to perform DoS attack on the network.

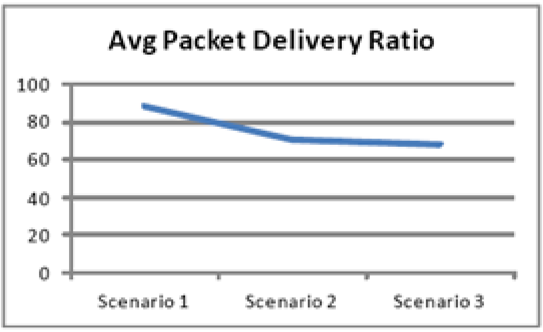


Figure 6: Average Packet delivery Ratio.

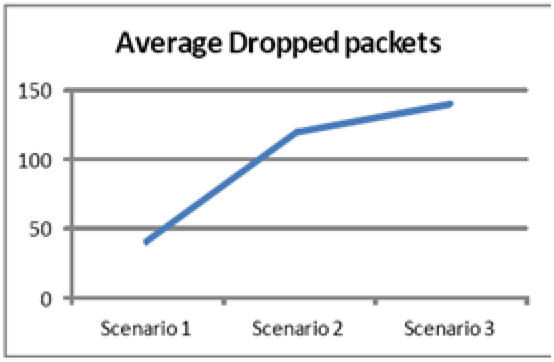


Figure 7: Average number of packets drops

Analysis Of Identification If Ids Agents Nodes [7]

IDS agents in intrusion detection systems must collect and analyze all packets in the communication area. So, it uses the extra resources and energy. In the most of the existing intrusion detection systems for MANETs IDS agents in order to detect intrusions load and run on all the nodes. Since, battery power of the nodes in MANETs are limited, there is a need for an efficient method of utilizing these resources to construct intrusion detection systems. The network lifetime is the time that the first node failure happens due to decrease of the battery. So, in order to improve the network lifetime, an effective method in selecting an IDS agent node is needed so that a required level of detection intrusion in MANETs would be provided.

Therefore, in the proposed method, after the compromised nodes are detected, then, from among them, the nodes which have higher battery power would be selected as the IDS agent nodes.

Simulation Parameters & Results

GloMoSim 2.03 simulator is used to simulate our method. We choose On Demand Multicast Routing Protocol (ODMRP) as the routing protocol. The channel capacity of mobile hosts is set to 2Mbps. Our network topology covers the area 1000 m by 1000 m with 15 mobile nodes that 5 nodes of them are compromised. The minimal speed is 0 m/s, maximal speed is 10 m/s, and pause time is 60s. The battery power of nodes is set randomly between 50W and 150W. The mobility model is the random waypoint model.

Fig.8 shows the number of nodes that fail due to decrease of the battery power (less than 15W) for AD and our method. We carried out simulation for different durations (15, 30, 60, 90 minutes).

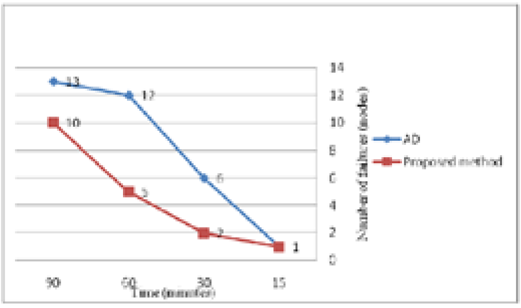


Figure 8: Comparison of number of failures

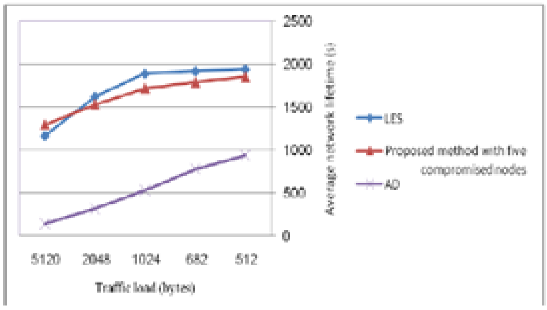


Figure 9: Comparison of the average network lifetime

Fig.9 illustrates the comparison of network lifetime among our method, AD (Anomaly Detection) and LES (Lifetime Enhancing Monitoring node selection). In AD, every node should participate in intrusion detection. So that, IDS agents are loaded on all the network nodes. In LES scheme, the nodes that have maximum remaining battery power between adjacent mobile nodes are selected as monitoring nodes for intrusion detection, but in this scheme every node can be compromised.

Conclusion

In this paper we review two different papers which is based on security problems and intrusion detection system for routing attacks in Manets. In this paper we compare following parameters like packet delivery ratio, average packet drop rate, number of failures, average network life time using NS2 Simulator and GloMoSim Simulators. In Future we propose a new routing algorithm that will detect and correct the type of attack made by intruding nodes and to implement the behavior of above said algorithm in NS-2 Simulator.

References

[1] Panayiotis Kotzannikolaou, Rosa Mavropodi, Christos Doulideris. (2005), 'Secure Multipath routing for Mobile Ad hoc Networks' , Proceedings of the second Annual conference on Wireless On demand Network System and services (WONS'05), IEEE, pp 1-8

[2] Akarygiannis, E. Antonakakis and A. Apostolpoulos. (2006), 'Detecting Critical Nodes for MANET Intrusion Detection systems', Proceddings of second international workshop on security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06), IEEE, pp 1-9

[3] Neeraj Nehra, R.B. Patel, V.K. Bhat, 'Routing with Load Balancing in Ad Hoc Network: A Mobile Agent Approch', 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 1007), 2007 IEEE

[4] Amir Darehshoorzadeh , Nastooh Taheri Javan, Mehdi Dehgan, Mohammad Khalili, 'A New Load Balancing Multipath Routing Algorithm for Mobile Ad Hoc Networks', Proceedings of IEEE 2008 6th National Conference on Telecommunications and IEEE 2008 2nd Malaysia Conference on Photonics, 26-27 August 2008, Putrayaja, Malaysia, pp 344-349

[5] Zhang XiangBo, Ki ll Kim, 'Load Aware Metric for Efficient Balancing on Multipath DSR Protocol in Mobile Ad Hoc Networks', 2008 International Conference on Advance Technologies for Communications, 2008 IEEE, pp 395-398

[6]. Tameen Eissa, Shukor Abd Razak, Md Asri Ngadi. (2009),'Enhancing MANET security using Sceret public Keys', International Conference on Future Networks,IEEE, pp 130-134

[7]. Marjan Kuchaki Rafsanjani, Ali Asghar Khavasi, Ali Movaghar, 'An Efficient Method for Identifying IDS Agent Nodes by Discovering Compromised Nodes in MANET,' 2009 IEEE Second International Conference on Computer and Electrical Engineering,' PP 625-629

[8] Maysam Hedayati, Hamid reza hoseiny, Seyed Hossein Kamali, Reza Shakerian, " Traffic Load Estimation and Load Balancing in Multiple Routing Mobile Ad Hoc Networks", 2010 International Conference on Mechanical and Electrical Technology(ICMET 2010), 2010 IEEE, pp 18-21

[9] Mehdi EffatParvar, MohammadReza EffatParvar, Amir Darehshoorzedeh, Mehdi Zarei, "Load Balancing and Route Stability in Mobile Ad Hoc Networks base on AODV Protocol", 2010 International Conference on Electronic Devices, System and Applications(ICEDSA2010), 2010 IEEE, pp 258-263

[10] R.Balakrishna , U.Rajeswar Rao , N.Geethanjali N," Performance Issues on AODV and AOMDV for Manets", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) ,2010, pp 38-43

[11] Mohamed Tekaya,Nabil Tabbane, Sami Tabbane, " Multiple Routing Mechanism with Load Balancing in Ad Hoc Networks",2010 IEEE, pp 67-72

[12]. Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra. (2010), 'Security issues in MANET: A Review', IEEE , pp 124-128

[13]. Husain Shahnawaz, Dr. S. C Gupta, Chand Mukesh, Dr. H.L. Mandoria. (2010), ' A Proposed Model For Intrusion Detection System for Mobile Adhoc Network', International Conference on Computer and communication Technology (ICCCT'10), IEEE, pp 99-102

[14]. Peyman Kabiri and Mehran Aghaei. (2011),' Feature Analysis for Intrusion Detection in Mobile Adhoc Networks', International Journal of Network security , Vol 12, No 1 , pp 42-49

[15]. Nan Kang, Elhadi M. Shakshuki , Tarek R. sheltami. (2011),'Detecting forged Acknowledged in MANETs', International Conference on Advance Information Networking and Applications, IEEE , pp 488-494

[16]. S. Mangai and A. Tamilarasi. (2011), ‘Analysis of an efficient Scalable and secured Geographic Routing Protocol for MANETs’, International Journal of Advanced Computing (IJAC), Vol 3, issue 2, pp 47-53

[17]. Okoli Adaobi, Ejiro Igbesoko, Mona Ghassemian. (2012),’ Evaluation of Security Problems and Intrusion Detection Systems forRouting Attacks in Wireless Self-organised Networks’,IEEE

[18] www.olsr.org

[19] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay,’ Different Types of Attacks on Integrated MANET-Internet Communication,’ International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp 265-274

[20] Pradip M. Jawandhiya et. al. ,’ International Journal of Engineering Science and Technology ,’ Vol. 2(9), 2010,’ pp 4063-4071

[21] Onkar V.Chandure, V.T.Gaikwad,’ Detection & Prevention of Gray Hole Attack in Mobile Ad Hoc Network using AODV Routing Protocol,’ International Journal of Computer Applications (0975 - 8887) Volume 41- No.5, March 2012,’ pp 27-32