An Effective Intrusion Detection System for MANETs

T. Prasanna Venkatesan
PG Scholar, Dept. of IT
Anna University, RC
Coimbatore, India

P. Rajakumar
PG Scholar, Dept. of IT
Anna University, RC
Coimbatore, India

A. Pitchaikkannu
PG Scholar, Dept. of IT
Anna University, RC
Coimbatore, India

ABSTRACT

In the recent decades the mobile wireless communication becomes more attractive because of its applications in many fields. Moving from the wired communication to wireless communication, the security is the most important property to consider. Specifically in the mobile environment it has the vulnerability, because of its portability and scalability. The mobile ad hoc wireless communication has characteristics such as open medium, distributed environment and changing topology, it makes the network into most vulnerable to the attackers to make the intrusion. The attackers (intruders) can easily enter into the network and compromises the network to behave in the favors of his choice. The Mobile Ad hoc NETwork (MANET) should have the capability to detect such intrusion (attacks) and remove it. To survive the MANET from such intrusion, an Intrusion Detection System (IDS) should be enhanced to the MANET, which can efficiently identify the attacks of the intruders. In this paper it is discussed about various intrusion detection mechanisms and techniques for the MANET to detect the intrusion and intruders.

General Terms

Watchdog algorithm, Twoack, AACK

Keywords

Intrusion detection system, MANET, active attacks, passive attacks

1. INTRODUCTION

The set of actions that compromises confidentiality, availability, and integrity of a mobile node is called as Intrusion [1]. Someone who involved with the compromising networks and performs the intrusion is called intruder. The IDS can monitor the host computer, network equipment, a firewall, a router, a corporate network, or any information system. To detect the presence of intrusion in the network the intrusion detection system (IDS) is used. It is the kind of security technology that attempts to identify, those misbehaving actions of a network and those who have legitimate access to the system but are abusing their privileges [2]. The IDS inspects the network activity, identifies suspicious patterns and indicates the network attack, from someone attempting to break the network.

The IDS should dynamically monitor the network and user's actions in the network to detect intrusions. The network can suffer from various kinds of security vulnerabilities and attackers. It may cause both technically difficult and economically costly to build and maintain a network that is not susceptible to attacks in the mobile environment [3]. An IDS, by analyzing the system and users' operations, in search of undesirable and suspicious activities, may effectively monitor and protect against threats.

Generally, there are three types of intrusion detection methods such as misuse based detection, anomaly based detection and specification based detection [4]. The misuse based detection technique keeps the record on known attack signatures and system vulnerabilities and stores them in a large database for the analysis of the intrusion activities. If the IDS, find a match between current activities and signatures about the attacks that is already documented, an alarm is generated to indicate suspicious activity [5].

An anomaly based detection technique creates the profiles of system states or user behaviors and compares them with current activities of the user or the system. The profile of the system state includes state of the network's traffic load, breakdown, protocol, typical packet size, usage frequency of commands and CPU usage for programs. It also monitors the network segments to compare their states and look for anomalies. If a sufficient deviation is observed, the IDS raise an alarm about the intruders [6]. Anomaly detection can also capable of detecting the unknown attacks. For the detection of novel attacks the misuse detection technique is not as effective, it is because of the lack of corresponding signatures of attacks in network.

Specification based detection evaluates a set of constraints that describe the correct operation of a program or protocol in the network, and monitors the execution of the program with respect to the defined constraints. This detection technique provides the capability to detect previously unknown attacks, with the low false positive alarm rate. However, normal profile of system state is very difficult to build. In a MANET, mobility induced dynamics make it as the challenging task to differentiate the normality and anomaly [4]. It is more challenging to distinguish between false alarms and real intrusions.

An IDS can also be categorized as network-based IDS and host based IDS in the network based IDS, the individual packets flowing in the entire network is analyzed. It detects malicious packets by overlooking the firewall's filtering rules. In a host based system, the IDS examine the intrusion activity by traffic analysis on each individual mobile host. An IDS differs from firewall it only looks for intrusions in the network in order to stop them from happening [6]. The firewall limits the access between networks and does not alert about an attack from inside the network. But IDS evaluates a suspected intrusion, which is taken place in the network and alerts a signal on intrusion. It also overlooks for attacks that originate within a system.

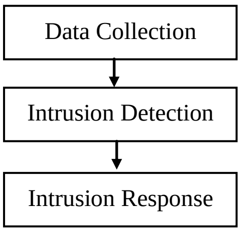

Fig 1: Components of IDS

The Intrusion Detection System has three main components as shown in Fig. 1, such as: data collection, intrusion detection, and intrusion response. The data collection component is responsible for the collection and preprocessing of data tasks. It is also responsible for transferring data to a common format, data storage and sending data to the intrusion detection module. IDS can collects data from different data sources and the inputs to the system such as: system logs, network packets. In the intrusion detection component data is analyzed to detect intrusion attempts or the malicious activity in the network. In this module there are several technologies are used for detection of accurate and low false positive rate of intrusion in the MANET [2]. The results of the intrusion detection are sent to intrusion response component. The intrusion response component collects the information from the intrusion detection module and finally it responds as the indication of presence of an intrusion in the MANET to the entire network.

In the following sections it is devoted about the different types of attacks in the MANET and various intrusion detection technologies applied for the MANETs to detect the existence of the intrusion or the intruders in network. Many researchers are devoted several intrusion detection system techniques that are suitable for the MANET.

2. ATTACKS IN MOBILE AD HOC NETWORKS

In this section it is briefly discussed about various types of passive attacks and active attacks occurring in the network layer, it is shown in Fig.2.

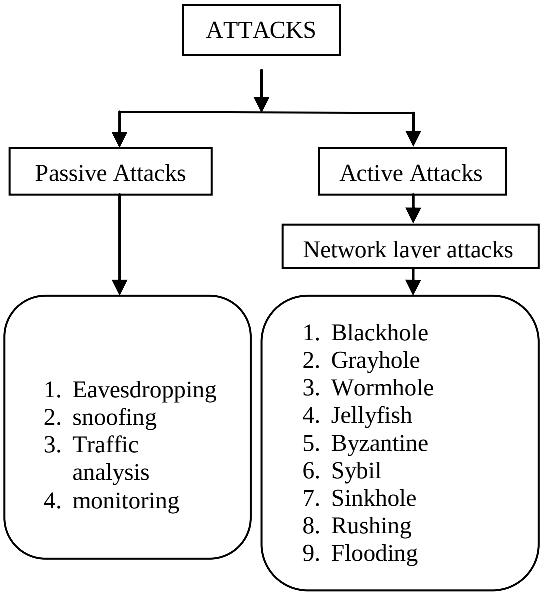

Fig 2: Types of attacks

The security issue in MANET is to protect network layer from the malicious attackers [7]. It is required to protect routing as well as data forwarding operations. First it is detailed about the passive attacks.

2.1 Passive attacks

A passive attack does not disrupt proper operation of the mobile nodes in the network. The attacker snoops the data exchanged in the network without altering it [7]. Fig. 3, shows the example of passive attack, where node 5 monitors/reads the data flow between the source and destination. This passive attack may be any of attack that is listed in the Fig. 2. Detection of passive attacks is very difficult since the operation of network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms. The different types of passive are listed in Fig. 2.

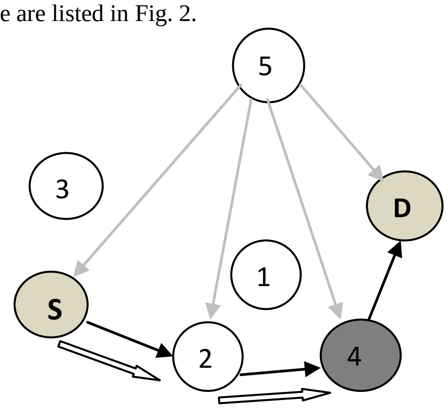

Fig 3: Passive attacks

2.1.1 Eavesdropping

Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers [7], [8]. A message sent by a node can be heard by every device equipped with a transceiver within the radio range, and if no encryption is used then the attacker can get useful information. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication.

2.1.2 Snooping

The snooping is the unauthorized interception of information in the form of disclosure. It is achieved by listening to (or reading) communications or browsing through files or system information. Wiretapping is a form of snooping in which a network is monitored [9].

2.1.3 Masquerading or Spoofing

Masquerading or spoofing, is an impersonation of one entity by another in the network, is a form of both deception and usurpation. It lures a victim into believing that the entity which it is communicating is a different entity in the network.

2.1.4 Modification or alteration

Modification or alteration is an unauthorized change of information. The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released [9].

2.2 Active attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. In active attacks, intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data of packets, resulting in various disruptions to the existing network. It can bring down the entire network or degrade performance significantly. The Fig. 2, shows the active attacks in the network layer of MANET [10]. The recent development and detection mechanism of blackhole, wormhole, and rushing attacks are briefed in the following subsequent sections of this paper.

2.2.1 Blackhole attack

MANET uses a reactive routing protocol such as Ad hoc On demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Secure Aware routing (SAR) for the routing of the data packets [11]. When the AODV routing protocol is used to discover the routes it works based on two types packets such as Route REQest (RREQ) packet and Route REPly (RREP) packet. The source node sends the RREQ packets to all other nodes to find the shortest route between the source and the destination in the network. The malicious node receives the RREQ packet and claim that it is having the shortest route or optimum path to the destination node. It is done sending the response by using the RREP packet that is having the shortest (fresh) route for the destination from the source. It is the fake RREP with extremely short route. Upon sending the fake RREP packet to the source node, the malicious node can able to place itself in the communicating network. It means that the transmitting packets are should be passed only by this malicious node only [12]. After sending the RREP packet, the malicious node receives the data packets from the source and does not forwards to the neighbor nodes or simply drops the packets that they received without sending to the destination node.

2.2.2 Wormhole attack

The colluding nodes creates an illusion [13] that two geographically separated (remote) nodes are directly connected and appears that the nodes as neighbors. But actually they are distinct from each other. The aim of the wormhole attack is to create the man in the middle attack and dropping the packets. The malicious node receives data packets at one node and tunnels them to another malicious node; this tunnel is called as wormhole. It makes the node as attractive and so that more packets are routed through these nodes. This type of attack prevents the discovery of any actual routes. It will disrupt the routing by short circuiting the network. This wormhole link becomes the lowest cost of path to the destination. Therefore these nodes are included for the transmission to the destination.

2.2.3 Grayhole attack

The grayhole attack is slight variation of the blackhole attack. If multiple paths exist between sender and destination then buffering packets with proper acknowledgement might detect active Gray-Hole attack in progress [7]. Dropping can occur by any of the following methods; it may drop all of the UDP packets while forwarding the TCP data packets; Dropping 50% of packets or uses the probabilistic computation. This type of attack simply drops the packets selectively or fully, based on certain scenario. The dropping is based the certain condition or it may be triggered. It may use any exponential computation and statistical manner for the dropping of the data packets.

2.2.4 Rushing attack

In AODV routing protocol, when source nodes flood the network with route discovery packets (RREQ, RREP) in order to find routes to the destinations, each intermediate node processes only the first non duplicate packet and discards any duplicate packets that arrive at a later time. A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets with a malicious RREP on behalf of some other node skipping any proper processing in order to gain access to the forwarding group [14]. In rushing attack, an intruder will rush (transmit early) the RREQ packet to suppress any later legitimate RREQs. Due to duplicate suppression, the actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker node, send packets to proper node after its own filtering is done, so from outside the network, the nodes behaves normally and nothing was happened. But it might increase the delay in packet delivering to destination node.

2.2.5 Byzantine attack

Byzantine attack is a compromised intermediate node or an asset of compromised intermediate nodes works to carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services [8]. This kind of failures is not easy for identification, since the network seems to be operating very normally. It may degrade the performance of the route discovery and data transmission process.

In this section it is briefly detailed about the active attacks on the network layer with the examples. From these researches on attack it is concluded that the attacks degrade the performance of the network as well as data packet transmission. In the next section it is discussed about various issues which are involved in the designing of the intrusion detection for the mobile ad hoc networks.

3. INTRUSION DETECTION IN MOBILE AD HOC NETWORKS

Intrusion detection for the MANETs is a complex, even difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points [15]. Conventional IDS are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. This section outlines the issues of intrusion detection for MANETs and reviews the main solutions proposed by the researchers.

For the mobile ad hoc networks, IDS provide solutions that should be self organized, collaborative and without centralized entity. Most of the MANET routing protocols have some limitations such that, nodes in network assumes all other nodes always cooperate with each other to relay data. This will cause the vulnerability to the attackers with the opportunities to do some intrusion or unwanted activities and also leave one or two compromised nodes. To address these problems, IDS should be added to enhance the security level of MANETs. If MANET can detect the attackers as soon as they enter into the network, it will be able to completely eliminate the potential damages caused by compromised nodes at the first time of the attack itself. An IDS act as the second layer for MANET and enables the overall security to the MANET.

A. Mishra et al (2004)., proposed [16] different intrusion detection schemes against attacks. Intrusion detection can be defined as the automated detection and subsequent generation of an alarm to alert the security apparatus at a location if intrusions have taken place or are taking place. An IDS is a defense system that detects hostile activities in a network and then tries to possibly prevent such activities that may compromise system security. IDSs achieve detection by continuously monitoring the network for unusual activity. The prevention part may involve issuing alerts as well as taking direct preventive measures such as blocking a suspected connection. In other words, intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the network and external ones. Unlike firewalls which are the first line of defense, IDSs come into the picture only after an intrusion has occurred and a node or network has been compromised. That is why IDSs are aptly called the second line of defense.

4. INTRUSION DETECTION TECHNIQUES FOR MOBILE AD HOC NETWORKS

Many researches are devoted their work for improving and developing the intrusion detection technologies for the MANET [1], [18]-[21]. In line these developments the different type ids for MANET such as watchdog algorithm, TWOACK algorithm, AACK scheme, intrusion detection techniques, and mission oriented intrusion detection are explained in this section.

4.1 Watchdog algorithm

Marti et al., (2000) proposed [17] a scheme named Watchdog algorithm aims to improve the throughput of network with the presence of malicious nodes in the network. In fact, the Watchdog scheme is consisted of two parts: Watchdog and Path rater. Watchdog serves as the IDS for MANETs. Watchdog node is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission in the entire network. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time then, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold value, Watchdog node reports it as the misbehaving node. However, compared to some other schemes, Watchdog algorithm is capable of detecting malicious nodes rather than links. Many MANET IDSs are developed as an improvement to the Watchdog algorithm. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: ambiguous collisions; receiver collisions; limited transmission power; false misbehavior report; collusion; partial dropping.

4.2 TWOACK Scheme

TWOACK algorithm was proposed [18] by Liu et al., (2007) is one of the most important approach in which the weaknesses of the Watchdog algorithm were to be solved. TWOACK is neither an enhancement nor a Watchdog based scheme. TWOACK algorithm is aiming to resolve the receiver collision and limited transmission power problems of Watchdog scheme. The TWOACK scheme detects misbehaving nodes by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination in network. It means that, each node required to send back an acknowledgment packet to the node that is two nodes away from it by using the same route.

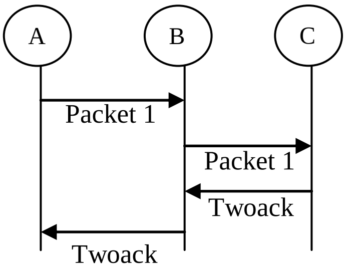

Fig 4: TWOACK scheme

TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) and on-demand routing protocols. The working process of TWOACK algorithm is shown in Fig. 4. In the Fig. 4, the Node A first forwards the Packet 1 to node B then, node B forwards it to node C.

When the node C receives Packet 1, as it is two hops away from the node A, node C is obliged to generate a TWOACK packet. The TWOACK packet contains the reverse route from the node A to node C, and sends it back to node A. The retrieval of this TWOACK packet at node A indicates that the transmission of Packet 1 from the node A to node C is successful. If the TWOACK packet is not received in a predefined time period, both nodes B and C are reported as malicious nodes. The same process applies to every three consecutive nodes along the rest of the route in the whole network. The TWOACK algorithm successfully solves the limited transmission, receiver collision and power problems of the Watchdog scheme. In TWOACK scheme, the acknowledgment process required in every packet transmission, this adds a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, this redundant transmission process can easily degrade the life span of the whole network.

4.3 AACK algorithm

Sheltami et al., (2009) proposed [19] a new scheme called AACK and this algorithm is based on the TWOACK. Similar to TWOACK, AACK scheme also an acknowledgment-based algorithm. It can be considered as a combination of a scheme called TWOACK and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, the AACK algorithm significantly reduces network overhead while still capable of maintaining and even surpassing the same network throughput in packet transmission. The end-to-end acknowledgment scheme is shown in Fig. 5.

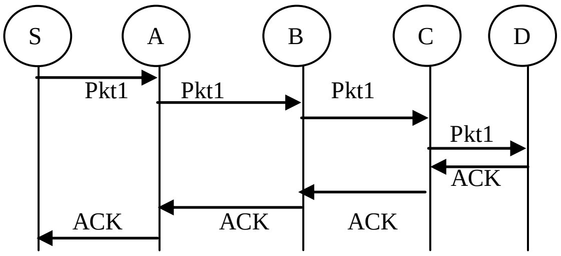

Fig 5: AACK scheme

In the ACK scheme shown in Fig. 5, the source node S first sends out Packet 1 without any overhead. All the intermediate nodes simply forward this packet to the neighbor nodes. When the destination node D receives Packet 1, it is required to send back an ACK packet to the source node S along the reverse order of the same route in the network. Within a predefined time period, if the source node S receives this ACK packet, then the packet transmission from node S to node D is successful. Otherwise, the source node S will switch to TWOACK scheme by sending out a TWOACK packet. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead. But both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes in the network with the presence of false misbehavior report and forged acknowledgment packets.

4.4 Intrusion Detection Techniques

B. Sun et al (2007) proposed [1] intrusion detection techniques to detect misbehaving activities in the network. An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system or a network node. Intrusion detection is a security technology that attempts to identify those misbehaving works and who is trying to break into and misuse a system without authorization. And those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, PC or any information system being monitored by an intrusion detection system. An IDS dynamically monitors a system and users' actions in the system to detect intrusions and intruders. Because an information system can suffer from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain an intrusion system that is not susceptible to attacks. An IDS, by analyzing the system and users' operations, suspicious activities, and in search of undesirable may effectively monitor and protect against threats. Intrusion detection technique encodes known attack signatures and system vulnerabilities and stores them in a database. If deployed IDS find the match between current activities and signatures, an alarm is generated. These detection techniques are not effective to detect novel attacks because of the lack of corresponding signatures. Any detection technique creates normal profiles of system states or user behaviors and compares them with current activities. If a significant deviation is observed, the IDS raise an alarm.

4.5 Mission Oriented Intrusion Detection

For mission oriented mobile group systems designed to continue mission execution in hostile environments in the presence of security attacks. It is critical to properly deploy intrusion detection techniques to cope with insider attacks and to enhance the system reliability. J. Cho et al (2007) proposed [20] IDS with analyze the effect of intrusion detection system techniques on the reliability of a mission oriented group communication system consisting of mobile groups set out for mission execution in mobile ad hoc networks. Unlike the common belief that IDS should be executed as possible to cope with insider attacks to prolong the system lifetime, it is discovered that IDS should be executed at an optimal rate to maximize the mean time to failure of the system in the network. Further, the optimal rate at which IDS is executed depends on the operational conditions, system failure definitions, attacker behaviors, and IDS techniques used. It is developed mathematical models based on Stochastic Petri nets to identify the optimal rate for IDS execution to maximize the mean time to failure of the system, when given a set of parameter values characterizing the operational conditions, and attacker behaviors. It concerns the failure time of a mission oriented GCS consisting of mobile groups in MANETs equipped with intrusion detection to deal with inside attackers. The notion of a mobile group is defined based on connectivity. When all nodes are connected, there is only a single group in the system. That is, group members must maintain connectivity to be in the same group. The GCS, and its constituent mobile groups are mission oriented in the sense that a mobile group may be partitioned into several groups due to network partition derived from node mobility, or node failure. However, these partitioned groups will still continue with the same mission assigned throughout their lifetime. Later, when two or more partitioned groups merge into one, the merged group will still continue with the same mission execution. Therefore, mission execution is an application-level goal built on top of connectivity oriented group communications. Each mobile group performs secure group communications by using a symmetric key, called the group key, shared by group members. The group key is employed to encrypt the message sent by a member to others in the group for confidentiality. The group key is rekeyed upon group member join/leave/eviction, and group partition/merge events to preserve secrecy.

5. CONCLUSION AND FUTURE WORK

MANETs are a new technology used increasingly in many applications. Because of the characteristics of the MANET, these networks are more vulnerable to attacks and have most security problems than other networks. In terms of MANET security the Intrusion Detection is the most considerable one. If the IDS are well designed, it can effectively identify malicious activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defense in depth security mechanisms for MANETs. In this paper, it is briefly explained on existing intrusion detection techniques in the context of MANETs. Since Intrusion prevention alone is not sufficient to achieve security in a network, it is presented a way to manage MANET security, by enhancing the existing secure protocols adding the component of Malicious nodes, not only in determining the route for sending packets, but also avoiding attempts of Denial of Service from Malicious Nodes. The accuracy of IDS can suffer from the high false positive or low false negative rates. If the majority of the mobile nodes are compromised then the intrusion detection becomes fail. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself, which may be addressed in future. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. As a consequence intrusion detection for MANETs remains a complex and challenging topic for security researchers.

6. REFERENCES

[1] B. Sun, L. Osborne, Y. Xiao and S. Guizani, “Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks,” IEEE Wireless Communications, pp. 56-63, October 2007.

[2] S. Sen and J. A. Clark, “Intrusion Detection in MANETs,” Department of Computer Science, University of York, York, UK.

[3] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion Detection in Wireless Ad Hoc Networks,” IEEE Wireless Communications, pp. 48-60, February 2004.

[4] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” Wireless/Mobile Network Security, Springer, pp. 170–196, 2006.

[5] J. Zhang and M. Zulkernine, “A Hybrid Network Intrusion Detection Technique Using Random Forests,” Proceedings of the First International Conference on Availability, Reliability and Security (ARES’06), IEEE Computer Society, 2006.

[6] C. Xenakis, C. Panos and I. Stavrakakis, “A comparative Evaluation of Intrusion Detection Architectures for MANETs,” computers & security 30, Elsevier, pp. 63-80, 2011.

[7] A. Nadeem and M.P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, IEEE Communications Surveys & Tutorials, 2013.

[8] A. Nadeem and M.P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”, IEEE Communications Surveys & Tutorials, 2013.

[9] M. Bishop, “Computer Security: Art and Science”, Addison Wesley, Nov. 2002.

[10] S. Buchegger and J. L. Boudec, “Performance Analysis of the CONFI-DANT Protocol”, Proc. of ACM Int. Sym. on MANET and Computing, 2002.

[11] M. Y. Su, “Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems,” Computer Communications, Elsevier, 34, pp.107–117, 2011.

[12] X. Y. Zhang, Y. Sekiya and Y. Wakahara, “Proposal of a Method to Detect Black Hole Attack in MANETs”, Proc. IEEE Inter. Symp. on Autonomous Decentralized System ISADS, 2009.

[13] E. A. Panaousis, L. Nazaryan and C. Politis, “Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications”, Sep. 7-9, 2009, London, UK.

[14] H. L. Nguyen and U. T. Nguyen, “A study of different types of attacks on multicast in MANET”, Elsevier, Ad Hoc Networks, 2008.

[15] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha, “Threshold-based Intrusion Detection in Ad Hoc Networks and Secure AODV,” Ad Hoc Networks 6, Elsevier, pp. 578–599, 2008.

[16] A. Mishra, K. Nadkarni, A. Patcha and V. Techintrusion, “Detection In Wireless Ad Hoc Networks,” IEEE Wireless Communications, pp. 48-60, February 2004.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, pp. 255–265, 2000.

[18] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs,” IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[19] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, “Video transmission enhancement in presence of misbehaving nodes in MANETs,” Int. J. Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct. 2009.

[20] J. Cho, I. Chen and P. Feng, “Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks,” IEEE Transactions on Reliability, Vol. 59, No. 1, pp. 231-241, March 2010.