International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 11, November 2014 **ISSN 2319 - 4847**

Detection and Segregation of Misbehavior Node(S) for MANETS OLSR Protocol

NUNE SREENIVAS[1], P.G.V.SURESH KUMAR[2]

[1]School of Electrical & Computer Engineering, AAiT, AAU, Addis Ababa, Ethiopia

[2,] Centre for IT&SC, AAiT, Addis Ababa University, Addis Ababa, Ethiopia

ABSTRACT

Intrusions can be imposed from different directions on network environments. Particularly on Mobile ad hoc Networks (MANETs), it is more frequent as the nature of this network is exposed it to be attacked. This happens due to the lack of defined infrastructures i.e uses wireless media and it has no defined perimeters and the communication medium used is not trusted; the mobility of the nodes can create additional problems on management of the topology of the network. These properties of MANET increased its susceptibility to intrusions. To address these problems there are several approaches proposed by different researchers. In this approach additional message for verification of the path, detection and isolation is used to test the validity of the route. Strong security mechanism should be developed to understand the nature of the normal nodes and malicious nodes so as to develop the detection mechanism. Understanding how malicious nodes behave in the network helps to design the intrusion detection mechanism that thwarts the attacks generated from these nodes. MANETs uses different routing protocol for communications to maintain the network and Optimized Link State Routing (OLSR) protocol is one of those protocols. In this work, OLSR protocol is used with an Intrusion Detection System (IDS) mechanism which accurately detects misbehavior node(s) using additional message which help to validate the path and if attacker is detected a message which isolate the attacker using alternative path is designed. This mechanism is investigated on End-to-End (E2E) communication between the source and the destination nodes in a typical MANET. It is effective in detection and isolation of misbehavior nodes using an alternative path to the destination. Based on this framework, simulation has been conducted and the simulation results showed that the proposed mechanism detects and isolates the attackers in a communication path while keeping a reasonably low overhead in terms of network traffic.

Keywords:- Intrusion, IDS, MANETs, OLSR

1.INTRODUCTION

Since the world's first wireless local area network (WLAN), ALOHANET, emerged in 1971 at the University of Hawaii, the growth of the wireless network is significant. Wireless networking is now the medium of choice for many applications. In addition, modern manufacturing techniques allow increasingly sophisticated functionality to reside in devices that are ever smaller, and so increasingly mobile. Mobile ad hoc Networks (MANETs) combine wireless communication with a high degree of node mobility. Contrasted to the wired network, the wireless network is more flexible and convenient, especially for those who like to use some mobile devices, such as laptop, Personal Digital Assistant (PDA), etc. Ethernet port is not necessary when network connection is needed as everything can be accessible using a wireless medium. The news and Email can be read even in a coffee shop or airport. People get access to the network almost whenever and wherever they want .However, such wireless connections actually are not really available anywhere. The connection is constrained by the pre-existed base stations (or access points). In order to get connected, people have to at least stay within the communication radius of one base station. Recent advances in portable computing and wireless technologies are opening up exciting possibilities for the future of wireless mobile networking. MANET is an autonomous system of mobile hosts connected by wireless links. MANETs aim to provide wireless communication in a limited geo-graphical area as Wireless Local Area Networks (WLAN). Most MANETs cover a much smaller area as it depends on the frequency range of the wireless antenna than WLANs but that is not what distinguishes MANETs from WLANs because it is affected by the dynamic movement of mobile nodes. Mobile networks can be classified into infrastructure networks and mobile ad hoc networks according to their dependence on fixed infrastructures. The most prominent characteristic of MANETs is that they do not rely on any fixed infrastructure to establish communication: instead, wireless nodes co-operate among themselves to establish communication. In an infrastructure mobile network, mobile nodes have wired access points (or base stations) within their transmission range. The access points compose the backbone for an infrastructure network. In contrast, mobile ad hoc networks are autonomously self-organized networks without infrastructure support and are therefore known as infrastructure-less wireless networks. In a mobile ad hoc network, nodes move arbitrarily, therefore, the network may experience rapid and unpredictable topology changes. Additionally, because nodes in a mobile ad hoc network normally have limited transmission ranges, some nodes cannot communicate directly with each other. Hence, routing paths in mobile ad hoc

networks potentially contain multiple hops, and every node in mobile ad hoc networks has the responsibility to act as a router. In Fig 1.1 it has been shown that these nodes creates path with nodes in their transmission range. Due to lack of infrastructure and well defined perimeter, MANETs are susceptible to a variety of attack types which are sent from different directions. To develop a strong security scheme; it is necessary to understand how malicious nodes can attack MANETs. In this study, it has been focused on propose an Intrusion Detection System (IDS) mechanism to accurately detect misbehavior node(s) in Optimized Link State Routing (OLSR) protocol based on End-to-End (E2E) communication between the source and the destination. Unlike in fixed networks the mobile Ad Hoc networks needs more security mechanisms. Attackers may intrude into the network through the subverted nodes. The network topology is highly dynamic as nodes frequently join or leave, and roam in the network. In spite of its dynamic nature, mobile users request security services as they move from one place to another. Hence, a powerful security solution is required to achieve protection and high network performance. The security solution should protect each node in the network and the security of the entire network relies on the collective protection of all the nodes. The security solution should protect the network from both inside and outside intruders into the system. The security scheme adopted by each device has to work within its own resource limitations in terms of energy supply, communication capacity, and memory and computation capability. Each security solution should encompass prevention, detection, and reaction. However, an attacker succeeds in infiltrating the security system and causes them to misbehave. Node misbehavior can result in degradation of network performance.

2.METHODOLOGY AND DATA ANALYSIS

2.1 Methodologies

This work established its objective to attain that objective it employed appropriate methodologies which will be followed to accomplish the work. These tasks start by reviewing literatures and related works on the existing protocols for MANET. By reviewing the literatures of the existing protocols for MANET, it is possible to get studies on OLSR and analyze the existing security mechanism. Analyzing the protocol for security, develop an intrusion detection mechanism for misbehaving nodes and test this mechanism on simulation software using different scenarios are tasks in this study. Finally, conclusion and recommendation has been drawn by setting direction for future work.

2.2 Application of Ad-hoc Network

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. Ad-hoc networks are suited for use in situation where an infrastructure is unavailable or to deploy one is not cost effective. One of many possible uses of mobile ad-hoc networks is in some business environments, where the need for collaborative computing might be more important outside the office environment than inside environment, such as in a business meeting outside the office to brief clients on a given assignment. A mobile ad-hoc network can also be used to provide crisis management service applications, such as in disaster recovery, where the entire communication infrastructure is destroyed and restoring communication quickly is crucial or for communication in a battle field, where the network infrastructures are either destroyed or never existed. Another application of MANET is in Bluetooth application, which is designed to support a personal area network by eliminating the need of wires between various devices, such as printers and personal digital assistants. A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on pre-existing infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Limited range wireless communication and high node mobility forces the nodes that they must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met. The dynamic nature of the protocols that enable MANET operation means they are readily suited to deployment in extreme or volatile circumstances. MANETs have consequently become a very popular research topic and have been proposed for use in many areas such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. MANETs by their very nature are more vulnerable to attack than wired networks. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices (which have generally different resource and computational capacities, and run usually on battery power) introduces new security risks. As part of rational risk management an appropriate action must be taken to identify these risks. In some cases we may be able to design out particular risks cost-effectively. In other cases we may have to accept that vulnerabilities exist and seek to take appropriate action when we believe someone is attacking us. As a result, intrusion detection is an indispensable part of security for MANETs. The nature of mobility

for mobile networks needs additional mechanisms for providing security. These vulnerabilities do not exist in a fixed wired network. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. We need to develop new architecture and mechanisms to protect the wireless networks and mobile computing applications.

2.3 Intrusion Detection Systems (IDS)

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource; whereas IDS are a system for the detection of such intrusions. Intrusion detection for MANETs is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. Therefore, conventional IDSs are not easily applied to them. Many intrusion detection systems (IDS) have been proposed in the literature for wired networks but MANETs' specific features make direct application of these approaches to MANETs impossible. Therefore we need to examine special IDS issues of MANETs and propose IDSs for MANET-specific systems to find out how well the proposed systems address these issues. New approaches need to be developed or else existing approaches need to be adapted for MANETs. There are three main components of IDS: data collection, detection, and response. The data collection component is responsible for collection and pre-processing of data tasks: transferring data to a common format, data storage and sending data to the detection module [14]. IDS can use different data sources as input to the system like system logs, network packets, etc. In the detection component data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the response component.

Intrusion detection techniques were classified in to three [13]. The first technique is anomaly-based intrusion detection which profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behaviors. Various techniques have been applied for anomaly detection, e.g. statistical approaches and artificial intelligence techniques like data mining and neural networks. Defining normal behavior is a major challenge. Normal behavior can change over time and intrusion detection systems must be kept up to date. False positives – the normal activities which are detected as anomalies by IDS – can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks. This is very important in an environment where new attacks and new vulnerabilities of systems are announced constantly. Misuse-based intrusion detection compares known attack signatures with current system activities. It is generally preferred by commercial IDSs since it is efficient and has a low false positive rate. The drawback of this approach is that it cannot detect new attacks. The system is only as strong as its signature database and this needs frequent updating for new attacks. Both anomaly-based and misuse based approaches have their strengths and weaknesses. Therefore, both techniques are generally employed for effective intrusion detection. Another technique proposed by these researchers is specification-based intrusion detection. In this approach, a set of constraints on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. It is introduced as a promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with a lower false positive rate. It can detect new attacks that do not follow the system specifications. IDSs on MANETs use a variety of intrusion detection methods. It has been agreed on the most commonly proposed intrusion detection method to date is specification-based detection [13]. This can detect attacks against routing protocols with a low rate of false positives. However, it cannot detect some kind of attacks, such as DoS attacks. As stated by the authors, there are also some anomaly-based detection systems implemented in MANETs. Unfortunately, mobility of MANETs increases the rate of false positives in these systems. There have been few signature-based IDSs developed for MANETs and little research on signatures of attacks against MANETs. Updating attack signatures is an important problem for this approach. Some systems use promiscuous monitoring of wireless communications in the neighborhood of nodes. Many researchers agreed on, a distributed and cooperative IDS architecture, which is generally used to provide a more informed detection approach since nodes in MANETs have only local data. In this architecture, every node has its local IDS agent and communicates with other nodes' agents to exchange information, to reach decisions and respond. It has been agreed on other IDS architectures in MANETs as stand-alone and hierarchical IDSs. In stand-alone IDS architectures, every node in the network has an IDS agent and detects attacks on its own without collaborating with other nodes. It should be possible to classify an IDS in all of the level 1 categories. For example, an IDS has to have a way to detect attacks, a detection method, and so far there are only two different kinds of detection methods; behavior-based and knowledge-based. As long as no new technology appears, there should be no problem to decide whether a detection method is behavior-based, knowledge-based or both. Note that an IDS has to have at least one of the level 2 categories for every level 1 category. Below, the difference between the different categories is explained

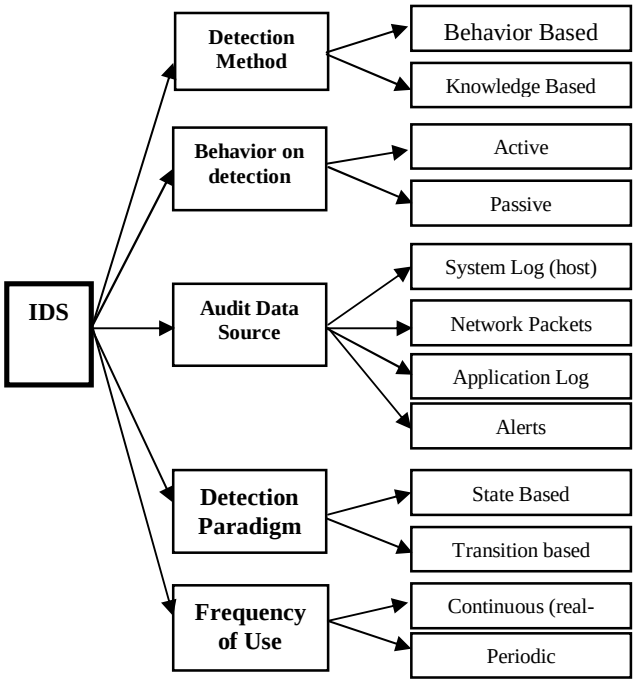

Figure 1 : Taxonomy of Intrusion Detection Systems (IDS)

2.3.1. Audit Data Source

There are different ways for IDS to collect its data. The input to the IDS could be either log files, packets from the network, system and API calls or events from other IDS.

2.3.1.1. Network Packets

If the IDS is network-based (NIDS), the packets are collected from the network. This is usually done by putting one network card of the machine that the NIDS reside on in promiscuous mode and thereby letting the NIDS see all the passing traffic.

2.3.1.2. Application Log Files

When a host-based IDS (HIDS) is in use, the input is most often received from an OS or application log file. These systems are usually applied to important servers, but can also be placed at firewalls to watch the firewall log and alert security officers when something out of the ordinary happens at the firewall.

2.3.1.3. System Log (host) Files

Another type of input that a HIDS could have is system and API calls. A HIDS could reside between the kernel and any other application, looking at all the system calls trying to find (and possibly stop) suspect system calls. In this way, the HIDS could detect malicious behavior of programs as well as users.

3.DESIGN AND IMPLEMENTATION OF MISBEHAVIOR NODE DETECTION MECHANISM ON OLSR PROTOCOL

The Proposed Detection Mechanism on OLSR Protocol This work focuses only on traffic relay/generation refusal where the malicious node acts as a black-hole and drops packets. Two types of attackers are introduced in this study where the first type is the malicious node which drops all the received packets and the second attacker type is the malicious node which is smarter than the first type and drops only data packets and exchanges control packets normally. To detect and isolate these attackers we need to extend the security of OLSR protocol in order to minimize their effects by working on two different aspects. The first security aspect validates the communication path by sending periodic messages and the second aspect is concerned with finding malicious node in the invalid path so that any other measure to make the communication line can be taken.

3.1Path Validation Message (PVM)

This is a message which can be generated by a mobile node which is distinguished as a source. This message is periodically sent to the destination at a specified interval. In OLSR there are different messages sent among nodes. Nodes, selected as MPRs, have a special responsibility when declaring link state information in the network. Indeed, the only requirement for OLSR to provide shortest path routes to all destinations is that MPR nodes declare link-state information for their MPR selectors. Additional available link-state information may be utilized, e.g., for redundancy.

Nodes which have been selected as MPRs by some neighbor node(s) announce this information periodically in their control messages. Thereby a node announces to the network, that it has reach ability to the nodes which have selected it as an MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the

network. Furthermore, the protocol uses the MPRs to facilitate efficient flooding of control messages in the network [RFC 3626]. Therefore, PVM can also be treated as additional message sent by these nodes.

3.2Attacker Finder Message (AFM)

Attacker Finder Message is a message which can be generated by the sender when there is a failure of a path validation message (PVM b) which occurs when there is no replay back message from the receiver or there is assumed a black hole attacker in the path. When the validity of the path between the sender and the receiver is not assured, the sender retransmits the PVM for a specified number of times and as the counter reaches its maximum, the sender now sends the attacker finder message to identify the attacker. Each intermediate node which received this message on the path is required to reply back to the source node with a message (AFMb) that contains information about the hop count and the next-node-to-destination (NNTD) and sends AFM to the destination through NNTD. Figure 4.2 shows how the attacker drops the message sent to the destination.

4.SIMULATION

4.1Simulation Environment

Simulation helps in analyzing the performance and behavior of complex networks before implementing it on real application in today's network environment. There are several network simulators available, which simulates the network as close as possible to real time implementation and its output is also close to the actual implementation. In this work, the researcher used the discrete-event simulator NS2 (version 2.35) [17] and the performance analysis were conducted using AWK script [18]. For the Implementation in the Simulation the researcher used UM-OLSR patching on ns-2 network simulator. UM-OLSR is an implementation of the Optimized Link State Routing protocol for the ns-2 Network Simulator. The code is released under the terms of the GNU General Public License (GPL). UM-OLSR complies with IETF RFC 3626 and supports all core functionalities of OLSR plus the link-layer feedback option. The software has been successfully tested on ns-2, and patchedon ns-2v2.35 simulator. It is widely employed by the wireless communications research community, as the high number of references in research papers reveal. In addition, it was ported to ns-3 by Gustavo Carneiro (INESC Porto) and to Omnet++ by Alfonso Ariza (Universidad de Málaga). Thus, you can also run OLSR simulations in modern network simulators [21].

4.2Simulation Results

Simulation on the designed scenario was done with nodes where there is no attacker in the scenario. When the two attacker types are considered, the second type of attackers is already smarter and the numbers of packets dropped are also less that the type-1 attackers. This shows the smarter attackers contribution to the overhead is slightly greater than the normal attackers. This is also clearly shown in this figure 2.

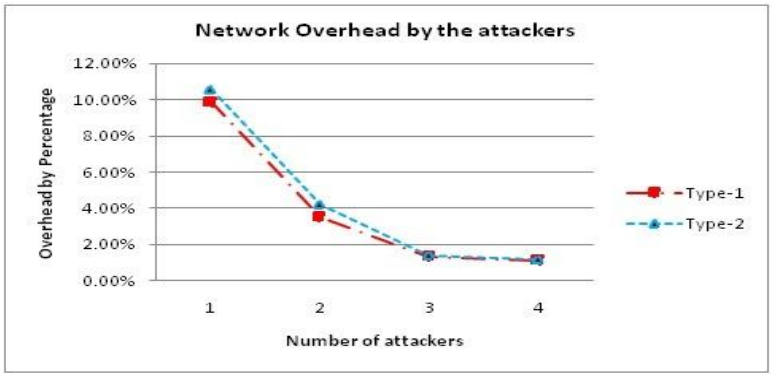

Figure2: Percentage contribution of the two Attackers to Network Overhead

The results discussed above reveal this approach increased the security of OLSR protocol in detection of malicious node and securing the communication route for sustaining the network in very hostile environment

5.CONCLUSION

This work demonstrates a mechanism that detects misbehaving nodes and their isolation mechanism using alternative paths in the network using OLSR protocol. Misbehavior node was identified by the neighboring node which transferred the message sent from the source and the rate of packets dropped by this misbehaving node can be used for determination as misbehavior or not. These nodes were identified by the message that is integrated to the normal protocol message. This message was the message transferred with HELLO and TC messages. For identification, PVM was sent by the source in a time interval of TC message. If the replay back of PVM did not reach the source node for three times, the source therefore initiates the second message, AFM, to find the attacker and this was done correctly in

simulation and the result is promising. The mechanism designed to detect worked well in the scenario developed and for the isolation of the detected node, another method was designed and integrated to the protocol. This mechanism was selecting alternative path to the destination based on the routing protocol of the detecting node. These alternative paths are built from the neighboring nodes to the attacker based on the routing tables of the intermediate nodes. The node identified as an attacker is blacklisted by the node which forwarded the message that validates the path and this blacklisted node will be announced to the other nodes so that they will not use that node as the path. Our mechanism can detect misbehavior node(s) through the path from source to destination as witnessed in the simulation. The overhead of this mechanism is measured and it shows the overhead of the mechanism is at about 11% of the total messages sent if the number if the attacker is less and this overhead decrease as the number of attackers increase. As it adds a significantly small packet used for detection and isolation to the OLSR message, it increases the network overhead. If there is no attacker in the communication line, the overhead of this mechanism is expected slightly higher and this is relatively higher when the attacker is smarter than a normal attacker node. Even though overhead is introduced, it was rewarded by the achievement of this mechanism as it contributed to the security of the network. The developed mechanism was simulated and the result of the simulation is analyzed for different number of attackers and different scenario. Detection of attackers can be done when the attacker were not respond to the PVM and after three trial of PVM by the source it can be blacklisted by the source and the intermediate node previous to the attacker from the source will initiated to use another path by taking 1-hop node in its routing table. The overhead of the added code to the existing protocol was analyzed and its overhead is not significant with the advantage that this mechanism provides for security features enhancement. Even though it seems high (around 11%) for a single attacker, its advantage weighs when the attackers are increasing. This is because the attackers as attackers are added, the number of packet drop increases.

6.FUTURE WORKS

Mobile networking is the richest area for research and the protocols used are in continuous review and modifications by the research community. In this research we contributed little to the security aspect and as it is not an absolute solution, we put a number of future research directions which needs a more extensive investigation. The following points may provide more investigations directions:

- Evaluating the routing protocol and the developed mechanism for minimization of the overhead introduced to the network traffic.
- Instead of reviewing the routing table of the neighboring node, it is better if the collaboration of a group of neighbor nodes is used to make accurate decisions to select the alternative path.
- The mechanism should also consider other characteristics like the node's energy efficiency and distance between the nodes before selecting the alternative path.

REFERENCES

[1] Ahmed M. Abdallaa, Imane A. Saroitb, AmiraKotbb and Ali H. Afsari, "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol", World Conference on Information Technology, 2010, pp. 115 – 121.

[2] Ahmed Mohamed Abdalla, ImaneAlySaroit, AmiraKotb, & Ali Hassan Afsari, "An IDS for Detecting Misbehavior Nodes in Optimized Link State Routing Protocol", International Journal of Advanced Computer Science, Vol. 1, No. 2, Aug. 2011, Pp. 87-91.

[3] Charlie Obimbo, Liliana Maria Arboleda-Cobo, "An Intrusion Detection System for MANET", Communications in Information Science and Management Engineering -- www.jcisme.org, Vol. 2 No. 3 Pp.1-5, 2011-2012.

[4] Ahmed Mohamed Abdalla, Ahmad H. Almazee, "Detection and Isolation of Packet Dropping Attacker in MANETs", International Journal of Advanced Computer Science and Applications, Vol. 4, No.4, 2013

[5] S. Madhavi, Tai Hoon Kim, "An Intrusion Detection System in Mobile Ad-hoc Networks", International Journal of Security and its Applications, Vol. 2 No. 3, July 2008.

[6] T. Clausen and P. Jacquet, "Network Working Group Request for Comment 3626: Category: Experimental – Optimized Link State Routing Protocol (OLSR)" Project Hipercom, INRIA, Oct. 2003

[7] BounpadithKannhavong, Hidehisa Nakayama and Abbas Jamalipour, "SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks",IEEE publication in the ICC 2008, pp.1464 – 1468.

[8] M. Tamer Refaei, YanxiaRong, Luiz A. DaSilva and Hyeong-Ah Choi, "Detecting Node Misbehavior in Ad hoc Networks" Communications, ICC, IEEE International Conference, June 2007, pp. 3425 – 3430.

[9] Hao Yang, HaiyonLuo - "Security in Mobile Ad-hoc Networks: Challenges and Solutions" UCLA – computer Science Department – IEEE Wireless Communications - Feb, 2004

[10] P. Jacquet, P. Muhlethalet, T. Clausen, A. Laouti, A. Qayyum and L. Viennot, "Optimized Link State Routing Protocol for Ad-hoc Networks".

[11] Danny Dhillon, Jerry Zhu and John Rechards - "Implementation & Evaluation of an IDS to Safeguard OLSRIntegrity in MANETs" RSA Security Inc. 2006. pp. 45 – 50.

[12] http://www.olsr.org
[13] SevilSen and John A. Clark – "Intrusion Detection in Mobile Ad-hoc Networks" - Department of Computer Science, University of York, York, UK - 2008.
[14] YannickLacharité, Maoyu Wang, and Louise Lamont, "Findings on a Semantically-Based Intrusion Detection Approach for OLSR MANET Protocol", 3rd OLSR Interop / Workshop V2.0, 2006.
[15] Fre´de´ricCuppens, Nora Cuppens-Boulahia, SeilaNuon and Tony Ramard, "Property Based Intrusion Detection to Secure OLSR", GET/ENST Bretagne, France 2011.
[16] M. Wang, L. Lamon, P. Mason and M. Gorlatova "An Effective Intrusion Detection Approach for OLSR MANET Protocol" IEEE 2005, pp. 55 – 60
[17] Kelvin Fall, "The ns manual (formerly ns Notes & Documentation)", US Berkerley LBL USC/ISI and Xerox PARC, 2010.
[18] Robins A.D.., "GAWK:an effective AWK programming", 3rd ed, April 2010.
[19] S. Mohapatraa, P.Kanungo, "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator" International Conference on Communication Technology and System Design 2011, pp. 69-76.
[20] The Vint Project, "The Network Simulator –ns-2," http://www.isi.edu/nsnam/ns/index.html
[21] F. J. Ro, "UM-OLSR Documentation," University of Murcia, March 2005, http://masimum.dif.um.es/um-olsr/html
[22] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," Proc. 6th Int'l. Conf. Mobile Comp.Net (MobiCom 2000), Aug. 2000, pp. 275–83.
[23] D.Girma "Implementation of Energy-Efficient Routing Protocols for Mobile Ad hoc Networks (MANET)" Addis Ababa University –August – 2004
[24] Sima and A.Kush, "Malicious Node Detection in MANET" – Computer Engineering and Intelligent Systems – ISSN 2222-1719 (paper)/2222-2864(on-line) Vol.2, No.4, 2011.