© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Malicious Nodes Identification and Classification of Nodes and Detection of UDP Flood Attack with ICMP using OLSR Routing Protocol in MANET

Sweta Kriplani, Rupam Kesharwani
Shri Ram Institute of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

Mobile ad hoc networks also known as MANETs have been used extensively for the seamless provisioning of information exchange, where the deployment of infrastructure is difficult, if not impossible. Such cases include remote rural areas with stringent topographical profiles, disaster-recovery terrains, battlefields and popular event sites (i.e. sports stadiums, exhibition venues). This new approach of networking brings a great flexibility and affordability to the world of wireless communications by introducing pervasive computing, document sharing, and smart sensors. However, since this kind of network uses the wireless medium for communication, the wireless ad-hoc network faces several security risks at different layers. A particularly severe security attack that affects the ad hoc network routing protocols at the network layer, is known as the Black hole attack. A malicious node advertises itself as having the freshest or shortest path to destination. Once the malicious node attracts the traffic toward itself, the attacker can misuse or discard the traffic and as a result data through the malicious node is lost. To properly protect these systems with limited resources, the security practitioners need to understand the possible security threats and their impacts on MANETs and have a framework to ensure that the protections implemented to mitigate the vulnerabilities in the systems are the most efficient ones possible. In this Research the effects of malicious nodes on MANETs proactive routing protocol, Optimized Link State Routing (OLSR) were studied using NS-3 and their vulnerabilities compared. A framework for a methodical security analysis and recommendation of efficient protection schemes was also developed as well Support Vector Machine (SVM) for classification of categories of node as malicious and normal nodes and Apply filtering rule on network traffic for identification of UDP FLOOD and ICMP attack using Wireshark.

Keywords: OLSR, SVM, MANET, NS-3, Wireshark, UDP FLOOD, ICMP

I. INTRODUCTION

The term MANET stands for Mobile Ad-hoc Network. This new networking concept defines simple mechanisms which enable mobile devices to form a temporary community without any planned installation, or human intervention. The idea is to form a totally improvised network that does not require any pre-established infrastructure. Each node acts as a host and a router at the same time. This means that each node participating in a MANET commits itself to forward data packets from a neighboring node to another until a final destination is reached. In other words, the survival of a MANET relies on the cooperation between its participating members.

If a source node wants to communicate with another node which is out of its transmission range, the former will send its packets to a neighboring node, which will send them, in its turn, to one of its neighboring nodes, and so on, until the destination node is reached.

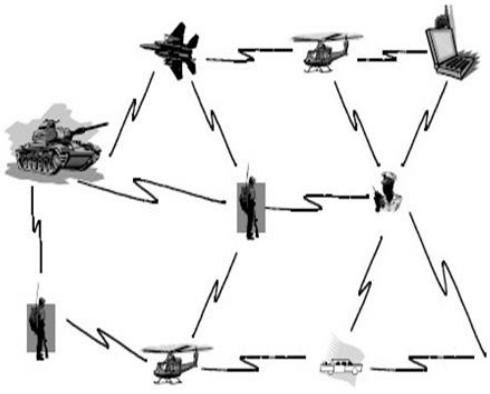


Figure 1: Overview of Mobile Ad hoc Network

This figure is originally from (Ilyas 2003).

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission (Perkins and Royer 1999, pp. 90-100). When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the network topology changes from time to time.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. In order to provide secure communication and transmission, the network administrators must understand different types of attacks and their effects on MANET (H. Nguyen and U. Nguyen 2006). Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack etc are kind of attacks that a MANET can suffer from. Due to the nature of MANETs, some attacks will be successful. Because MANETs are vulnerable, an efficient attack mitigation system that balances financial costs against performance costs is significant (Silva et al. 2005). Attack and protection trees provide an analyst with the tools to properly conduct a security analysis on a system such as a MANET. The framework allows an analyst to model the tradeoffs between system cost and performance while trying to optimize security.

II. METHODS AND MATERIAL

RELATED WORK

2.1 IEEE Standard for Wireless Networks

Institute of Electrical and Electronics Engineers (IEEE) define the standards for related technologies. IEEE defined three main operational standard for wireless LAN i.e. IEEE 802.11a, 802.11b and 802.11g. The entire three standards belong to IEEE 802.11 protocol family. In 1999 802.11a standard was ratified by IEEE. The 802.11 has a nominal data rate of 54Mbps, but the actual data rates varies between 17-28Mbps.

The most established and frequently deployed wireless network standard is 802.11b. Most of the public wireless "hotspots" use this standard. It operates in 2.4 GHz spectrum and the nominal data transfer is 11 Mbps. practically, approximately 4-7 Mbps is the actual data transmission rate of communication between work stations. Nodes are mobile and they have limited resources, achieved by this standard.

2.2 Mobile Ad Hoc Network's Routing Protocols

MANETs work on TCP/IP structure to provide the means therefore the traditional TCP/IP model needs to be refurbished or modified, in order to compensate the MANETs mobility to provide efficient functionality. Routing protocols in MANETs are a challenging and attractive task. Researchers are giving tremendous amount of attention to this key area.

2.3 Classification of MANETs Routing Protocols

Mobile ad hoc network‟s routing protocols are classified into three main categories according to (Hurley and Keller 1999, pp. 75-91). These are proactive routing protocols, reactive routing protocols and hybrid routing protocols. Each category has many protocols.

2.2.1 Reactive Protocols

Reactive protocols are also known as demand driven protocols. The reasons why they are referred to as reactive protocols is that, they do not initiate route discovery by themselves, until they are requested, when a source node requests for a route. These protocols setup routes when demanded (Jani 2002). When a node wants to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will establish a route for the source to destination node. Normally reactive protocols

- Don‟t find route until demanded

- When trying to find the destination "on demand", they use flooding technique to propagate the query.
- Do not consume bandwidth for sending information.
- They consume bandwidth only, when the node start transmitting the data to the destination node.

Examples of different reactive protocols are given below

- Dynamic Source Routing Protocol (DSR)
- Ad Hoc On Demand Distance Vector Routing Protocol (AODV)

Temporally Ordered Routing Algorithm (TORA) Associability Based Routing (ABR) Location aided Routing (LAR)

2.2.2 Proactive Protocols

Proactive routing protocols work the other way round as compared to reactive routing protocols. These protocols constantly maintain updated topology of the network. Every node in the network knows about the other node in advance, in other words the whole network is known to all the nodes making that network. All the routing information is usually kept in tables (Erdal and Chunming 2009, p. 116). Whenever there is a change in the network topology, these tables are updated according to the change. The nodes exchange topology information with each other; they can have route information any time when needed.

PROPOSED WORK

Malicious Node Detection Algorithm

Following steps we follow for classification of malicious node and normal node:

we have store the routing table in XML file and after that we will apply XML as a input to SVM

Step 1. Generates randomly an initial population of size based on routing table of nodes generated by ns3 simulator.

Step 2.Training SVM Classifier. SVM classifier is trained by training set with feature subset selected and variable value of parameters.

Step 3. For each set of the population, train SVM Classifier for computing fitness of each 2 subset of features.

Step 4. Select individuals from population directly based on fitness values and regenerate new individuals from old ones.

Step 5. If the maximum number of iteration is not yet reached, we proceed with the next generation operation. The termination criteria are that the max generation number reached or the fitness function(threshold mechanism) value does not improve during the last generations return to step 2.

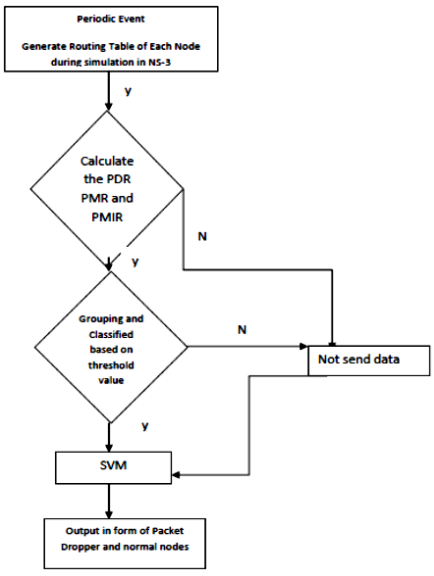
Step 6. Select the best fitness as optimal subset feature in this step we got the result of packet dropper node and normal node.

Step7. Apply the optimal feature to dataset (routing table).

Step 8: and Apply filtering rule on pcap file of each node in network and identify UDP FLOOD attack and ICMP attack using Wireshark.

Step 9: Final result shows malicious traffic and normal traffic of each node in network.

And Flow chart for algorithm as follows:



For better approximation of dropping node we have choose following metrics to conjunction with threshold metrics [€, α, β, μ], they are listed below

1. Packet Delivery Ratio (pd)
2. Packet Modification Ratio (pm)
3. Packet miss routed ratio (pm_r)

4. Residual Energy (re)

Now authors [1] metric will be modified and calculated using above metrics (assuming A, and C is MANET Node)

€ ⟶ f(pd, pm, pm_r, re) and same for other metrics α, β, μ.

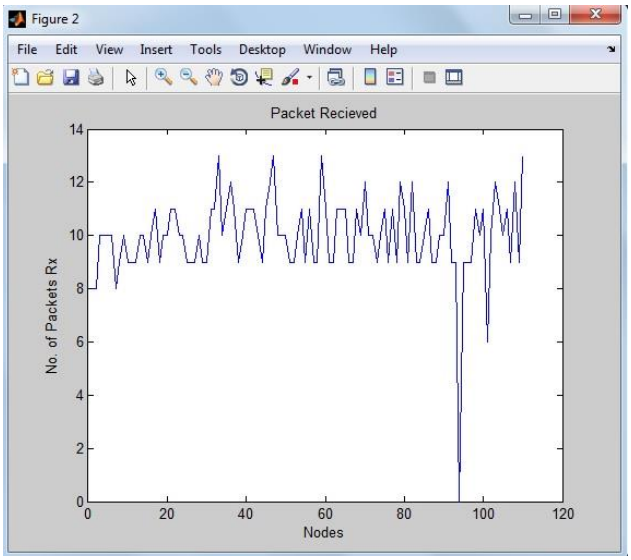
Fundamentally we will find malicious node with normal node and simulation setup on NS3.

III. RESULTS AND DISCUSSION

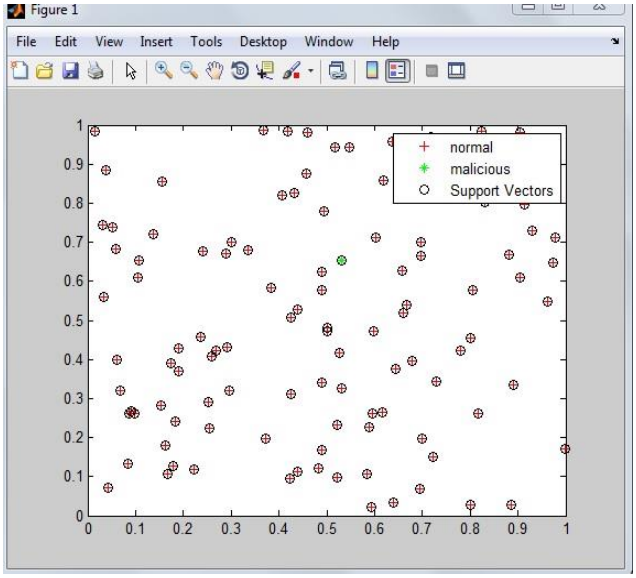
SIMULATION AND RESULTS

We have done simulation in NS-3 and *ns-3* has been developed to provide an open, extensible network simulation platform, for networking research and education. In brief, *ns-3* provides models of how packet data networks work and performs, and provides a simulation engine for users to conduct simulation experiments. Some of the reasons to use *ns-3* include to perform studies that are more difficult or not possible to perform with real systems, to study system behavior in a highly controllled, reproducible environment, and to learn about how networks work. Users will note that the available model set in *ns-3* focuses on modeling how Internet protocols and networks work, but *ns-3* is not limited to Internet systems; several users are using*ns-3* to model non-Internet-based systems.

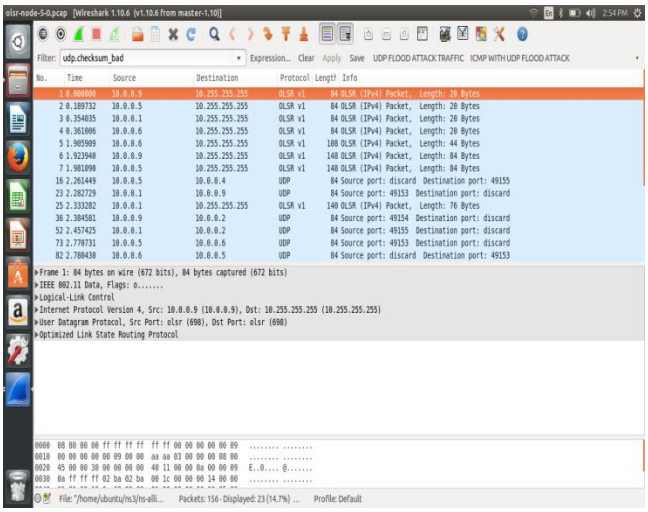
(A) This graph shows the number of packet received between nodes during simulation.



(B) This represent SVM output for classification of malicious and normal nodes.



(C) This represent the UDP FLOOD attack detected by putting the rule udp.chechksum_bad on traffic generated by nodes using NS3 Simulator and output contain destination port discard message which indicate DOS attack on particular connection made by node during simulation.



IV. CONCLUSION

In this paper focus on network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of OLSR. The protocols have more severe effect when there is higher number of nodes and more route requests. The impact of malicious node attack on network End-to-End delay is

severe with OLSR. Reactive protocols do not maintain unused routes and search them when they are needed.This fact increases the delay suffered by packets, because they remain waiting at buffers before being transmitted. OLSR being a proactive routing protocol stores upto date routing table and route are indentified before sending data this enable the source nodes to avoid the black hole route. The throughput of OLSR is effected by twice as compared to existing approach.

This research also develops the framework for using an attack and protection tree methodology to analyze the security of a MANET. To accomplish this, the structure of attack trees is extended and modified to create the concept of protection trees. To demonstrate the general usefulness of this novel methodology, it is used to analyze the impact of malicious node attack in mobile ad hoc networks and credible recommendation of efficient protection schemes. The framework methodology developed out of this research is an ideal candidate for security analysis of critical systems such as MANETs and SVM is used to fabricate the categories of nodes as malicious and normal node and Identify UDP FLOOD and ICMP attack on network traffic generated in NS3 simulator using wireshark.

V. REFERENCES

[1] Abolhasan M., Wysocki T., Dutkiewicz E., 2003, "A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia.

[2] Al-Shurman M., Yoo S.M., and S. Park, 2004, "Black Hole Attack in Mobile Ad-Hoc Networks," ACM Southeast Regional Conf.

[3] Ammann, P. E. and Sandhu R. S., 1991,"Safety Analysis for the Extended Schematic Protection Model," Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, pp. 87-97.

[4] Awerbuch B., Holmer D., Nita-Rotaru C., and Rubens H., 2002, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures," Proceedings of the ACM Workshop on Wireless Security, pp. 21-30.

[5] Beyer D., Vestrich M.D., and Garcia-Luna-Aceves J.J., 1999, ``The Rooftop Community Network: Free, High-Speed Network Access for Communities," The First 100 Feet: Options for Internet and Broadband Access, The MIT Press, pp. 75-91.

[6] Bishop, M., 2003. Computer Security Art and Science. Boston, MA: Addison-Wesley. 7] Bistarelli S., Fioravanti F., and Peretti P., 2006, "Defense Trees for Economic

[7] Evaluation of Security Investments," Proceedings of the First International 183 Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, pp. 416-423.

[8] Biswas K. and Md. Liaqat Ali, 2007, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March.

[9] Brooke, P. J. and Paige R. F., 2003, "Fault Trees For Security System Design and Analysis," Computers & Security, vol. 22, no. 3, pp. 256-264.

[10] Cisco Networking, Accessed, Feb –April 2011, http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.pdf

[11] Creswell J. W., 2002. Research Design: Qualitative, Quantitative and Mixed Methods Approach, 2nd Ed, Sage Publication Inc, California.

[12] da Silva A., Martins M., Rocha B., Loureiro A., Ruiz L., and Wong H., 2005,"Decentralized Intrusion Detection in Wireless Sensor Networks," Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, Montreal, Canada.

[13] Deng H., Li W., Agrawal, D.P., 2002, "Routing security in wireless Ad-Hoc networks," Cincinnati University of Cincinnati, OH, USA; IEEE Communications Magazine, ISSN: 0163-6804, Vol.40, Oct, pp.70- 75.

[14] Erdal Cayirci, Chunming Rong, 2009, Book Security in wireless Ad Hoc and Sensor Network, John Wiley & Sons Ltd, page 116.

[15] Hu Y., Perrig A., and Johnson D., 2002. Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta.