International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 03, Volume 4 (March 2017) Special Issue www.ijirae.com

SECURE ROUTING AND DETECTION OF HYBRID ATTACK IN MANET

S.Karthikrajakumar[1]
Sengunthar College of Engineering, Tiruchengode

N. Sangeetha Priya[1]
HOD, Dept of Electronics and Communication Engineering Sengunthar College of Engineering, Tiruchengode

ABSTRACT *---- A Mobile Ad hoc NET work (MANET) is a collection of autonomous nodes that have the ability to communicate with each other without having fixed infrastructure or centralized access point such as a base station. This kind of networks is very susceptible to adversary's malicious attacks, due to the dynamic changes of the network topology, trusting the nodes to each other, lack of fixed substructure for the analysis of nodes behaviors and constrained resources. One of these attacks is black hole attack. In this attack, malicious nodes inject fault routing information to the network and lead all data packets toward themselves, then destroy them all. In this paper, we propose a solution, which enhances the security of the Ad-hoc On-demand Distance Vector (AODV) routing protocol to encounter the black hole attacks. Our solution avoids the black hole and the multiple black hole attacks. The simulation results using the Network Simulator NS2 shows that our protocol provides better security and better performance in terms of the packet delivery ratio than the AODV routing protocol in the presence of one or multiple black hole attacks with marginal rise in average end-to-end delay and normalized routing overhead*

INTRODUCTION

MANET (MOBILE AD HOC NETWORK)

A Mobile Adhoc Network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and also change its links to other devices frequently. The primary challenge in building a MANET is equipping each device to continuously evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space maintain the information required to properly route traffic. Mobile Adhoc networks may operate by themselves. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer Adhoc network. The growth of laptops and 802.11/Wi-Fi wireless networking has made MANETs a popular research topic since the mid 1990s. Many academic papers, Different protocols are evaluated based on measure such as packet drop rate, overhead introduced by routing protocol, end-to-end packet delays and network throughput.

For Ad Hoc wireless network, route discovery and route maintenance are two main tasks of the routing protocol. If the routing protocol is reactive (on-demand), then broadcasting route request is used to find a network route. To control propagation of broadcasting messages in the network, flooding control mechanisms are used to control the route request packet forwarding. An Adhoc network is a wireless network formed by wireless nodes without any help of infrastructure. In this network, nodes are mobile and can communicate dynamically in an arbitrary manner. MANET is characterized by absence of central administration devices such as base stations. Nodes should be able to enter and leave the network easily. In these MANET, nodes act as routers. Routers play an important role in route discovery and maintenance of routes from source to destination. If link breakages occur, network has to stay operational by building new routes. The main technique used is multi-hopping is to increase the overall network capacity and performance. By using multi-hopping, one node can deliver data to a determined destination [6]. The Figure 1.1 shows the structure of the wireless Ad-hoc networks. A Mobile Ad hoc Network (MANET) represents a system of wireless mobile nodes that can self-organize freely and dynamically into temporary network topology. It can be quick deployed at any time as to eliminate the complexity of infrastructure setup. Other problems are route errors and higher overhead, caused by the mobility of nodes. To avoid designing bugs is necessary to analyze the designed protocols formally before protocols are deployed. Considering the particularities of MANET, the secure traits are different from the traditional security as secrecy and authenticity. Formal analysis methods are used for many years in cryptographic protocols.

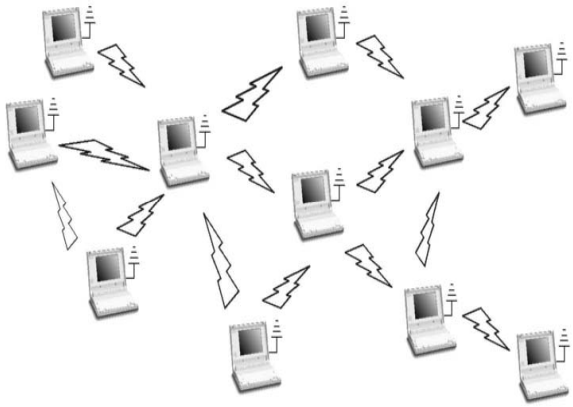


Figure 1.1

In this method, a research project team engaged in excavation work constructs an ad hoc network on a mountain. The results obtained from the investigation may consist of various types of data such as numerical data, photographs, sounds and videos.

NEED FOR AD-HOC NETWORKS

Ad-Hoc networks are needed as mobile hosts to communicate with no fixed infrastructure and administrative help because,

a. *It may not be physically possible for the establishment of the infrastructure*
b. *It may not be practically economical to establish the infrastructure*
c. *It may be because of the expediency of the situation does not permit the installation of the infrastructure.*

USAGE OF THE MANET

i. *Tactical operation – for fast establishment of military communication during the deployment of forces in unknown and hostile terrain.*
ii. *Rescue mission – for communication in areas without adequate wireless coverage.*
iii. *National security - for communication in times of national crisis existing communication infrastructure is non-operational due to a natural disaster.*
iv. *Law enforcement – for fast establishment of communication in exhibitions, conferences and sales presentations.*
v. *Commercial use – for setting up communication in exhibitions, conferences.*
vi. *Education – for operation of wall-free (virtual classrooms).*
vii. *Sensor networks - for communication between intelligent sensors mounted on mobile platforms.*

APPLICATIONS OF MANET

There are a number of possible application areas for MANET. These can range from simple civil and commercial applications to complicated high risk emergency services and battlefield operations. Some significant examples include civil, emergency, military domains and other examples.

BATTLE FIELD OPERATIONS

In future battlefield operations, autonomous agents such as unmanned ground vehicles and airborne vehicles will be projected to the front line for intelligence, surveillance, enemy antiaircraft suppression, damage assessment and other tactical operations. It is envisaged that these agents, acting as mobile nodes, will organize into groups of small unmanned ground, sea and airborne vehicles in order to provide fast wireless communication, perhaps participating in complex missions involving several such groups.

EMERGENCY SERVICES

MANET can be very useful in emergency search and rescue operations. Conventional infrastructure-based communication facilities are destroyed due to natural calamities like earthquakes. Immediate deployment of MANET in these scenarios can assist rapid activity coordination. Police squad vehicles and fire brigades can remain connected to exchange information more quickly if it cooperates to form ad hoc networks.

CIVIL AND COMMERCIAL APPLICATIONS

Two emerging wireless network scenarios that are soon likely to become part of the daily routines are vehicular communication in an urban environment, and personal area networking. In the vehicular communication scenario, short range wireless communication will be used within the car for monitoring and controlling the vehicle's mechanical components. Potential applications include road safety messages, coordinated navigation and peer to peer interactions.

SYSTEM SPECIFICATION

HARDWARE REQUIREMENTS

Processor	:	Intel Pentium IV
Processor Speed	:	1.4 GHz
Memory (RAM)	:	512 MB
Hard disk	:	80 GB
Monitor	:	14"IBM color monitor
Input Device	:	Keyboard (104)

SOFTWARE REQUIREMENTS

Operating System:		Windows XP, Linux
Simulator Tool	:	NS2
Language	:	C++ and TCL

NS2-NETWORK SIMULATOR VERSION 2

NS-2 was built in C++ and provides a simulation interface through OTcl, an object-oriented dialect of Tcl. The user describes a network topology by writing OTcl scripts, and then the main ns-2 program simulates that topology with specified parameters. It runs on Linux, FreeBSD, Solaris, and Mac OS X and on Windows using Cygwin. It is licensed for use under version 2 of the GNU General Public License.

WORKFLOW FOR NS

It includes four steps:

1. *Implement protocol models.*
2. *Setup simulation scenario i.e. Make Tcl file in which you mention what type of scenario you want, e.g. no of nodes, kind of agent working on nodes.*
3. *Run simulation i.e. Run the Tcl file. Analyze simulation results.*

FEATURES OF NETWORK SIMULATOR

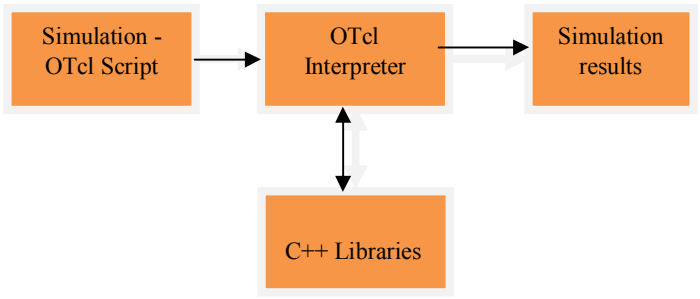
Network simulator (NS) is an object–oriented, discrete event simulator for networking research. NS-2 is written in C++, with an OTcl1 interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. Advantages of this split-language program approach are that it allows for fast generation of large scenarios. To simply use the simulator, it is sufficient to know OTcl. And disadvantage is the modifying and extending the simulator requires programming and debugging in both languages.

NS-2 can simulate the following:

1. *Topology: Wired, wireless*
2. *Scheduling Algorithms: RED, Drop Tail,*
3. *Transport Protocols: TCP, UDP*
4. *Routing: Static and dynamic routing*
5. *Application: FTP, HTTP, Telnet, Traffic generators*

USER'S VIEW OF NS-2

From the user's perspective, NS-2 is an OTcl interpreter that takes an OTcl script as input and produces a trace file as output in fig 4.1 NS-2.



The wireless model essentially consists of the Mobile Node at the core with additional supporting features that allows simulations of multi-hop ad-hoc networks, wireless LANs. The Mobile Node object is a split object. The C++ class Mobile Node is derived from parent class Node. A Mobile Node is the basic Node object with added functionalities of a wireless and mobile node like ability to move within a given topology, ability to receive and transmit signals to and from a wireless channel. A major difference between is that a mobile Node is not connected by means of Links to other nodes or mobile nodes. Mobile Node is the basic ns Node object with added functionalities like movement, ability to transmit and receive on a channel that allows it to be used to create mobile, wireless simulation environments. The class Mobile Node is derived from the base class Node.

The four ad-hoc routing protocols that are currently supported are Destination Sequence Distance Vector (DSDV), Dynamic Source Routing (DSR), Temporally ordered Routing Algorithm (TORA) and ad-hoc On-demand Distance Vector (AODV).

THE GENERAL STRUCTURE FOR DEFINING A MOBILE NODE IN NS2

$ns node-con fig ad-hoc Routing $opt (ad-hoc Routing)

-IIType $opt (II)
-macType $opt (mac)
-ifqType $opt (ifq) -ifqLen $opt (ifqlen)
-antType $opt (ant)
-proplnstance [new $opt (prop) -phyType $opt (netif)
-channel [new $opt (chan)]
-topolnstance $topo -wiredRouting OFF
-agentTrace ON
-routerTrace OFF
-macTrace OFF

The above API configures for a mobile node with all the given values of ad- hoc-routing protocol, network stack, channel, topography, propagation model, with wired routing turned on or off (required for wired-cum-wireless scenarios) and tracing turned on or off at different levels.

TRACE ANALYSIS

Running the TCL script generates a NAM trace file that is going to be used as an input to NAM and a trace file called out.tr that will be used for our simulation analysis. The trace format and example trace DATA from out.tr. Each line in trace file represents an event associated to a packet. Each field in the line is coded. Each trace line starts with an event (+, -, d, r) descriptor followed by the simulation time (in seconds) of that event, and from and to node, which identify the link on which the event occurred. The next information in the line before flags (appeared as no flag is set) is packet type and size (in Bytes). The next field is flow id (fid) of IPv6 that a user can set for each flow at the input OTcl script. In the fid field may not be used in a simulation, users can use this field for analysis purposes. The fid field is also used when specifying stream color for the NAM display. The next two fields are source and destination address in forms of node**.** Port. The next field shows the network layer protocol's packet sequence number. The last field shows the unique id of the packet.

NETWORK ANIMATOR (NAM)

Network animator (NAM) is an animation tool for viewing network simulation traces and real world packet teaches. It supports topology layout, packet level animation and various DATA inspection tools. Before starting to us NAM, trace file need to be created. This trace file is usually generated by NS. It contains topology information, e.g. nodes and links, as well as packet traces during a simulation, the user can produce topology configurations, layout information and packet traces using tracing events in NS. Once the trace file is generated, NAM can be used to animate it. Upon startup, NAM will read the trace file, create topology, pop up a window, do layout if necessary and then pause at time 0. Through its user interface, NAM provides control over many aspects of animation.

OTHER FEATURES OF NS2

1) *A network simulator must enable a user to represent a network topology, specifying the nodes on the network, the links between those nodes and the traffic between the nodes.*
2) *Network simulators are relatively fast and inexpensive.*
3) *Network simulators, as the name suggests are used by researchers, developers and engineers to design various kinds of networks,*
4) *Analyze the effect of various parameters on the network performance.*
5) *Simulation provides modeling flexibility. Various parameters may be changed and various combinations of parameters may be evaluated.*
6) *Simulation provides the ease in modeling the system.*

FEATURES OF LINUX OS

a) **Multi-tasking:** Several programs can run at the same time.
b) **Multiuser:** Several users can logon to the same machine at the same time. There is no need to have separate user licenses.
c) **Multiplatform:** Linux runs on many different CPUs and it support multiprocessor machine.
d) **Multithreading:** Linux has native kernel support for multiple independent threads of control within a single process memory space.
e) **Crash proof:** Linux has memory protection between processes, so that one program can't bring the whole system down.
f) **Demand loads executables:** Linux only reads from those parts of a program that are actually used on the disk.

g) **Shared copy-on-white pages among executables:** This means that multiple processes can use the same memory to run in. One tries to write to that memory, that page (with 4KB piece of memory) is copied. Copy-on-write has two benefits are the increasing speed and decreasing memory.

CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

An efficient and novel strategy that protects critical nodes from DDoS attacks in MANETs. Considering the different roles that certain nodes play in a MANETs, it is assumed that there are some important nodes that should be protected with higher priority. Lower level nodes would be allocated as protection nodes to handle the incoming traffic to the higher level nodes a node is able to deduce suspect nodes and refrain from nominating them as a sole MPR, thus, sidestepping the essential element of the attack. Experiment done Through intensive simulation experiments using NS-2 and proved that every functionality works well As expected, there is rise in routing overheads about 5-10% for node velocities up to 30 m/congestion of the network disappears and load is transmitted uniformly throughout the network. The modified OLSR also gives the reduction in average end to end delay.

FUTURE ENHANCEMENT

In order to estimate the signal parameters accurately for mobile systems, it is necessary to estimate a system's propagation characteristics through a medium. The MANET mobility models considered are Random Waypoint model, Random Direction model, Gauss-Markov model, City Section model, Manhattan model. A characteristic feature of every mobility model is to ensure that a Mobile node will not travel outside the network area. The performance metrics of specific interest are the lifetime per multi-path set and the multi-path set size.

REFERENCES

[1]. Brad Karp and Kung H .T, (2001), 'Greedy Perimeter Stateless Routing for Wireless Networks', Proc. ACM/IEEE Mob Com, pp. 243-254.
[2]. Camp's and Liu. Y, (2003), 'An Adaptive Mesh-Based Protocol for Geocast Routing', J. Parallel and Distributed Computing', vol. 63, no.2, pp. 196-213.
[3]. Chiang. C, Gerla. M, and Zhang. L, (1998), 'Forwarding Group Multicast Protocol (FGMP) for Multihop Mobile Wireless Networks', ACM J. Cluster Computing, special issue on mobile computing, vol. 1, no. 2, pp. 187-196.
[4]. Das S.M, Pucha. H, and Hu .Y .C, (2008), 'Distributed Hashing for Scalable Multicast in Wireless Ad Hoc Network', IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 3, pp. 347-362.
[5]. Devarapalli. V and Sidhu. D, (2001), 'MZR: A Multicast Protocol for Mobile Ad Hoc Networks', Proc. IEEE Int'l Conf. Comm. (ICC '01).
[6]. Ferouz A Forouzan, 'Computer Networks' Fourth Edition.
[7]. Garcia-Luna-Aceves. J. J and Madruga .E (1999), 'The Core-Assisted Mesh Protocol',IEEE selected Areas in Comm., vol. 17, no. 8, pp. 1380-1394.
[8]. Gui.C and Mohapatra .P, (2004), 'Scalable Multicasting for Mobile AdHoc Networks', Proc.IEEE INFOCOM.
[9]. Gerla.M, Lee S .J, and Su .W, (2000), 'On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks', Internet draft, draftietf- manet-odmrp-02.txt.
[10]. Giordano.S and Hamdi .M, (1999) 'Mobility Management: The Virtual Home Region', technical report.
[11]. Ji.L and Corson. M. S, (2001), 'Differential Destination Multicast: A MANET Multicast Routing Protocol for Small Groups', Proc. IEEE INFOCOM.
[12]. Ko Y.B and Vaidya. N, (1999), 'Geocasting in Mobile Ad Hoc Networks: Location Based Multicast Algorithms', Proc. Second IEEE Workshop Mobile Computing Systems and Applications (WMCSA).
[13]. Lee.S, Su .W, Hsu M. Gerla, and R. Bagrodia,(2000), 'A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols', Proc. IEEE INFOCOM.
[14]. Liao. W, Tseng , and Sheu. J, (2000), 'Geogrid: A Geocasting Protocol for Mobile Ad Hoc Networks Based on Grid', J. Internet Technology, vol. 1, no. 2, pp. 23-32.
[15]. Mauve.M, Fubler .H, Widmer .J, and Lang .T, (2003), 'Position-Based Multicast Routing for Mobile Ad-Hoc Networks', Proc. ACM MobiHoc, poster section.
[16]. Wu. S and Candan K.S,(2006), 'GMP: Distributed Geographic Multicast Routing in SWireless Sensor Networks', Proc. 26th IEEE Int'l Conf. Distributed Computing.
[17]. Woo. C and Singh .S,(2001), 'Scalable Routing Protocol for Ad Hoc Networks', Wireless Networks, vol. 7, pp. 513-529.
[18]. Xiang. X, Zhou .Z, and Wang .X,(2007), S'Self-Adaptive On Demand Geographic Routing Protocols for Mobile Ad Hoc Networks', Proc. IEEE INFOCOM.
[19]. Xiang. X and Wang .X,(2006), 'An Efficient Geographic Multicast Protocol for Mobile Ad Hoc Networks', Proc. IEEE Int'l Symp. World of Wireless, Mobile and Multimedia Network (WoWMoM).
[20]. Zayson , Liu .M, and Noble .B, (2009), 'Random Waypoint Considered Harmful', Proc. IEEE INFOCOM, vol. 2, no. 4.

