Generation Of Arbitrary Topologies For The Evaluation Stages In Critical Node Test Mechanism

Nitiket N Mhala

GJCST Classification
B.4.3,C.2.1

***Abstract*-The applications of MANET are increasing in modern generation. But MANET are more vulnerable to many attacks because of their adhoc nature. The security issue is the main concern in the use of MANET application.Therefor, the selection of efficient methodologies and techniques to protect MANET is an important aspect. Detecting malicious nodes in an open adhoc network in which participating nodes have no previous security associations presents a number of challenges not faced by the traditional wired networks. Traffic monitoring in wired network is usually preferred at switches, routers and gateways, but adhoc network does not have these types of network elements where the Intrusion Detection System (IDS) can collect and analyze audit data for the entire network. Any kind of network diagnosis or intrusion detection depends on the degree of mobility of nodes. This paper presents a Critical Node Test Mechanism which is a lightweight solution that can be used to determine the proper conditions to activate more demanding IDS. Here, we generate arbitrary logical network topologies in order to perform real time operations on adhoc network at a relatively low cost in a laboratory environment without having to physically move the nodes in the adhoc network.**

Keywords- adhoc, test bed, critical node, node degree, MANET, IDS.

I. INTRODUCTION

A mobile adhoc network is a relatively new communication paradigm. In modern generation, theapplications of MANET are increasing in use. MANET does not require expensive base stations of wired infrastructure. Therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. MANET is self organized in such way that a collection of mobile nodes without a fixed infrastructure and central management is formed automatically. Wireless presents a number of unique problems for Intrusion Detection System (IDS). Network traffic can be monitored on a wire segment, but adhoc nodes can only monitor network traffic within their observable radio range. A MANET is most likely not under a single administrative domain, making it difficult to perform any kind of centralized management or control.

In an adhoc network, malicious node may enter and leave the intermediate radio transmission range at random interval, may collude with other malicious nodes to disrupt network activity and avoid detection, or behave maliciously only intermittently, further complication their detection. A node that sends out false routing information could be a compromised node, or merely a node that has a temporarily stale routing table due to volatile physical conditions. Packets may be dropped due to network congestion or because a malicious node is not faithfully executing a routing algorithm [1] MANET with loose or no prior security associations are more difficult to diagnose than a MANET comprised of nodes from the same organization with strong security services. Establishing trust in an open adhoc network in which higher-level security services are unavailable can be hampered by the short lived presence of both collaborating and malicious nodes. In addition to having no previously established trust associations, nodes in an adhoc network have little incentive for reciprocity to faithfully execute a routing protocol or provide a minimum level of service. Closed adhoc networks that support critical applications may not be able to tolerate the presence of malicious nodes; fortunately closed networks can more established prior trust associations for collaborative IDS. The effectiveness of collaborative IDS also depends on the amount and trustworthiness of data that can be collected by each node.

Malicious nodes in sparsely populated networks can be more harmful than malicious nodes in a densely populated network since these nodes can effectively not only disrupt communication but also disconnect the network.

II. RELATED WORK

Various IDS techniques have been proposed in the research literature.Zhang and Lee describe a distributed and collaborative anomly detection-based IDS for adhoc network [2,3]. Theodorakpoulos and Baras present a method for establishing trust metrices and Evaluting trust [4].Michiardi and Molva assign a value to the “reputation” of a node and use this information to identify misbehaving nodes and co-operate only with trusted reputations. [5].Certain nodes in MANETS can produce attacks which cause congestion, distribution of incorrect routing information,services preventing proper operation or disable them[6].As routing protocols exchange routing data between nodes, as a result, they would maintain routing status in each node.Based on routing status ,data packets are transmitted by mediated nodes along an established route to the destination [7]. M.K Rafsanjani,A Movaghar presents a scheme in which nodes do not need to exchange multiple messages to prove their identities[8].

III. METHODOLOGY

The dynamic nature of adhoc networks suggests that preventation techniques that monitor the security status of the network and identify anomalous and /or malicious

About-Associate Professor M.E(Electronic) Phd(Wireless Adhoc Network)(persuing) nitiket_m@rediffmail.com

behavior. These techniques are usually less expensive to implement and can be easily developed in existing adhoc networks without requiring modification to nodes configuration or routing protocols being used. Here, our concept is built around the notion of critical node in an adhoc network. We consider a critical node whose failure or malicious behavior disconnects or significantly degrades the performance of the network.

In order to determine a critical node, a graph theoretic approach to detect a vertex-cut and an edge-cut is studied. [9].A vertex-cut is a set of vertices whose removal produces a sub graph with more components than the original graph. A cut-vertex or articulation point is a vertex cut on sitting of single vertex. An edge-cut is a set of edges whose removal produces a sub graph with more components than original graph. A cut-edge or bridge, is an edge –cut consisting of a single edge. Although the cut-vertex or cut edge of graph G can be determined by applying a straight forward algorithm. Finding a cut vertex in the graphical representation of an adhoc network is not a straightforward, since the nodes cannot be assumed to be stationary. A network discovery algorithm can give an approximation of the network topology, but the value of such an approximation in performing any kind of network diagnosis or intrusion detection depends on the degree of mobility of nodes.

A. Role Of Our Adhoc Network Test Bed

The basic idea of our emulation Test Bed[10] is having a number of MANET nodes physically close to each other inside the laboratory, but forces them to 'think' that they can only communicate with a selected few of them. That way, we can emulate a logical topology. In order to work, there is the need of hardware. Our Test bed is an emulator, not a simulator. So, we have the necessary hardware equipment. Each node is a device that has a wireless (802.11 b/g) interface, so that it can communicate with other adhoc nodes and run MANET protocols. In addition, the device should also have a wired interface (Ethernet), which is used for administrative purposes. In brief, the Test Bed uses the wired interface to transfer files needed for its operation to and from the node and manipulate its networking element in such way that will create logical topology we want. That Leaves the wireless interface free of any interface and most importantly, emulates an actual MANET, which is the whole point all along. In fact, Test Bed uses ix86 architecture and Linux can run even in 80386 machines (at least requirement is Pentium II), so we can gather all those old PCs intended thrown away, adding a PCMCIA wireless card on each of them and set up a MANET test bed in a laboratory at a very low cost.

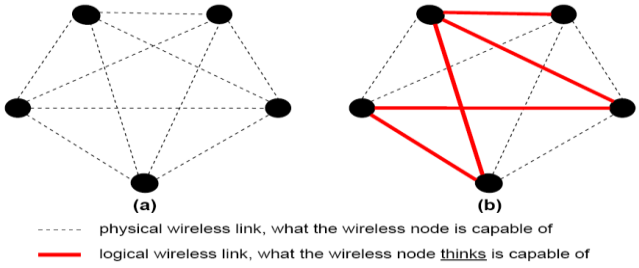

Figure1. (a) Physical links, (b) logical links between MANET nodes

B. Design Concept For Creation Of Logical Topology In Our Test Bed

Determining the global network topology in a mobile adhoc network is somewhat difficult, but determining an approximation of this topology or subset of this topology within a certain time frame may be useful. Our test bed allows user to create arbitrary network topologies and emulate the mobility. By changing the logical topology of the network, users can conduct test on adhoc network without having to physically move the nodes in the adhoc network. By giving the number of nodes in adhoc network Test Bed, each node's IP and MAC address, software module used in a test Bed creates arbitrarily connected graphs and updates each node's IP_TABLES accordingly through socket servers running on each network node in order to reflect the new logical topology. Thus arbitrary graph is represented in an adjacency matrix that is then translated into the corresponding IP_TABLES. Software module uses open source graph visualization tool Graphviz [11] to display the logical topology of the adhoc network as shown below.

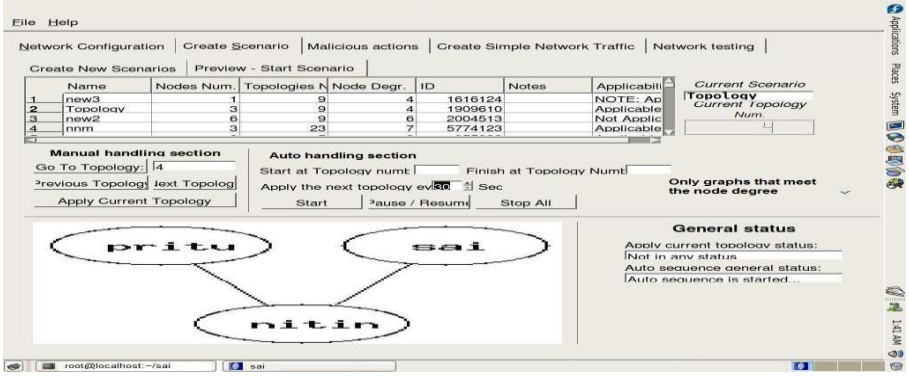

Fig. 2 Logical Topology Creation (Node degree = 4)

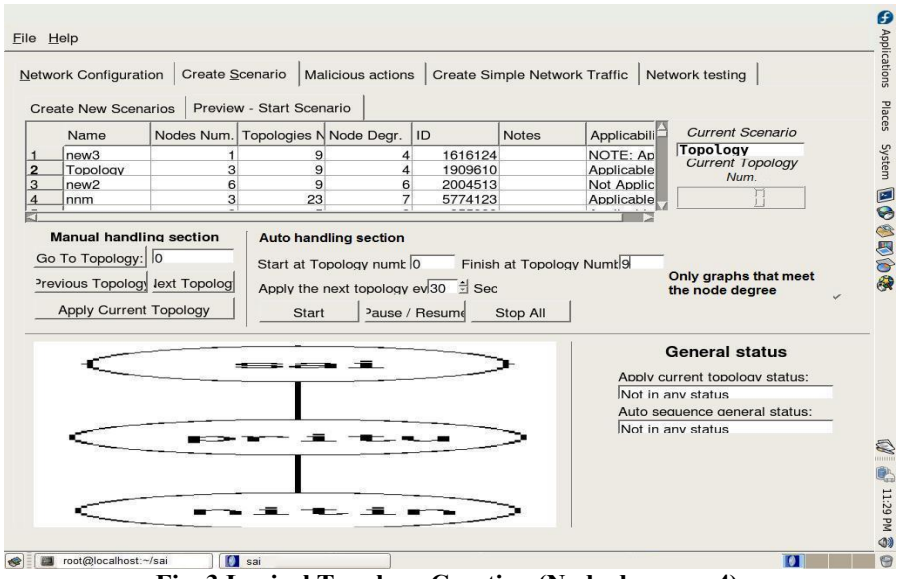

Fig. 3 Logical Topology Creation (Node degree = 4)

Above figures indicates arbitrary creation of logical topology of actual three nodes in every 30 seconds in our laboratory. We can set 150 physical nodes and theoretically, there is no limit to the number of nodes this test bed can handle. Therefore, we design the module which allows users to save and replay different mobility scenarios to control the maximum and minimum degree, produces an output in the form of adjacency matrix for further analysis and produces a framework for building additional adhoc network tools. An approximation of the network topology can provide the useful information about network density, network mobility, critical path and critical nodes.

IV. CRITICAL NODE TEST CONSIDERATION

A. Basic Steps

i. The node performing the test is referred to as testing node and the node under test is referred as node under test.

ii. Use of ip,route and ping utilities The ip utility is a TCP/IP interface configuration and routing utility that configures the network interfaces

iii. The route utility manipulates the Kernel's IP routing Table. It's primary purpose is to set static routes to specific hosts or networks via an interface after it has been configured with ifconfig program.

iv. When used together,ip route provides the necessary tools for manipulating any routing tables such as displaying routes, routing cache ,adding routes, deleting routes, altering routes, getting routing information and clearing routing table.

B. Evaluation Stages In A Critical Node Test Mechanism

It is very necessary to detect whether the testing node shares a critical link with its Neighbors.

i. First Stage

a) To temporarily modify the testing node's routing table to allow only one communication link to be operational at a time, while blocking communication through all others.

b) The enabled communication link will be between the testing node and a node other than the node under test.

c) Each communication link has to test sequentially in this way to determine if an alternative path to the link under test exists.

d) If an alternative path exists, then the link is not critical because its removal will not disconnect the network.

ii. Second Stage

1) This stage is for the host to attempt to discover an alternative path by using ping to the node under testwithout using the suspected cut-edge between the testing node and node under test.

2) To discover an alternative path to the node under test, the testing node executes the following command

#ping –c –s 4 < node_under_test> -A-R

Where –c is the number of pings that the host executes

-s is the number of data bytes to be sent

-A is the audit flag

-R flag returns the route, if exists, to the < node_under_test> node

iii. Third stage

1) When the results of the ping are returned, the network routing table is restored during this finalstep to its initial configuration.
2) . It is very important to note that, after the end of critical node test, all previously established routes are restored .The duration of critical node depends on the network density and topology.
3) Critical node conditions however are likely to occur when a node has a relatively small degree (see fig 3 and fig 4) and therefore fewer tests are required.

V. INFERENCES

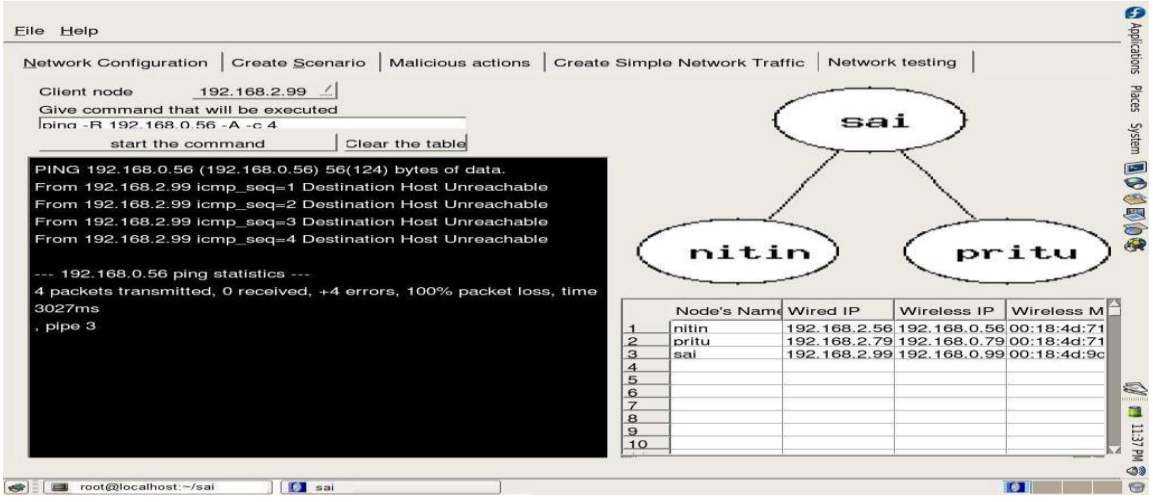

Fig. 4 (node test)

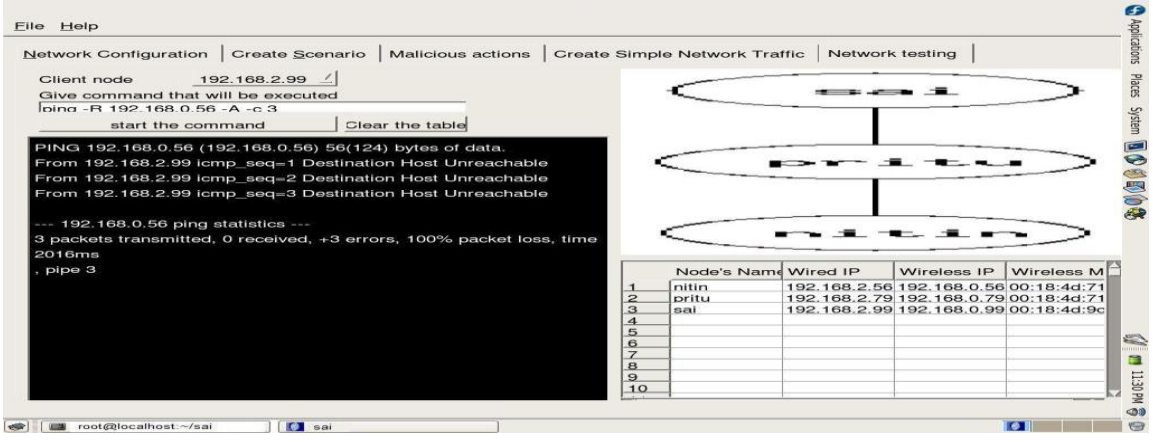

Fig. 5 (node test)

Above two figures show different topology created in our test bed for the same node degree of 4.

Fig 4- indicates the ping results from the Host node Sai (Wired IP 192.168.2.99 & Wireless IP 192.168.0.99) To node nitin (Wired IP 192.168.2.56 & wireless IP 192.168.0.56) showing the node nitin unreachable.

(The statistics is that 4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3027 ms,pipe 3)

Fig 5- indicates the ping results from the Host node Sai (Wired IP 192.168.2.99 & Wireless IP 192.168.0.99) to node nitin (Wired IP 192.168.2.56 & wireless IP 192.168.0.56) showing the node nitin unreachable for the changed topology.

(The statistics is that 3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2016 ms,pipe 3)Thus, we made inference that Host node Sai has a critical (or semi critical) link with node nitin.

VI. . Conclusion and Future Work

In order to improve the lifetime of the network, an effective method in selecting a monitoring node is needed so that a required level of detection Intrusion in MANET would be provided. When a critical link is detected, it can be the focus of more resource intensive or other diagnostic measures. The host node may choose expend additional resources to initiate an IDS module that is more resource intensive such as Traffic monitoring watch dog module or Collaborative IDS.But if there is no critical link then this metric can be used to help decide if the application or risk environment warrant the expenditure of additional requires monitoring diagnosis and and altering other nodes about the problems. Or if there is no critical link then host can use the lighter modules to continue to monitor network traffic. Therefore, we may conclude that Critical Node Test Mechanism is a lightweight solution that can be used to determine the proper conditions to activate more demanding IDS.Involment of Trigger mechanism for the invocation of critical node test in a mobile adhoc network will be the basis of our future work. This paper effort to focus that, generating arbitrary topologies create scenarios can help researchers to test experimental IDS system under the difficult situations. We may conclude since the global topology of the adhoc network is known, which will help researchers to benchmark the actual performance of their adhoc routing algorithms and applications against the theoretical optimal performance.

VII. Acknowledgement

The authors would like to thank everyone, including the anonymous reviewers

VIII. References

1) A.Patwardhan,J.Parkar,A.Johi, A. Karyygiannis and M Iorga. Secure routing and Intrusion Detection in Ad-hoc Networks. Third International conference on Pervasive computing and communications 2005
2) Y. Zhang and W Lee. Intrusion Detection in wireless ad hoc network. In Proceedings of the 6th annual International conference on Mobile Computing and Networking,pp 275-283,2000
3) Y. Zhang, W. Lee and Y.Hang. Intrusion Detection techniques for mobile wireless network. ACM/Kluwer Mobile Networks and applications (MONET), 2002
4) Theodorakopoules, George and Baras, Jhon. Trust evaluation in adhoc networks. Proceedings of the 2004 ACM workshop on Wireless security,pp. 1-10,2004
5) Michiardi, P and Molva, R,"Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Adhoc Networks",Communication and Multimedia Security 2002 Conference.
6) Karygiannis, E.Antonakakis and A. Apostolopoulos, Detecting critical nodes for MANET intrusion detection system. In Proc 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous computing, 2006.
7) N.Komnios, D.Vergados and C. Douligeries. —Detecting unauthorized and compromised nodes in mobile adhoc network." Elseviewer Adhoc network, vol5, n0 3, pp.289-298, 2007
8) M. K Rafsanjani, A Movaghar,"Identifying monitoring nodes with selection of Authorized nodes in mobile Adhoc network",World Applied Sciences Journal,vol4,n03, pp.444-449,2008
9) Graphs:Theory and Algorithms, K. Thuasiraman, M.N.S Swamy.
10) Nitiket N Mhala, N K Choudhari, —An Envision of Low cost Mobile Adhoc network Test bed in a laboratory Environment emulating actual MANET ", IJCNC,Vol.2, No.3,May 2010.
11) http://www.graphviz.org

Global Journals Guidelines Handbook 2010

www.GlobalJournals.org