An Approach for Determining Conditions for Monitoring of Critical Nodes for MANET Intrusion Detection System

Nitiket N Mhala[1] and N K Choudhari [2]
[1]*Associate Professor, Department of Electronics Engg., BDCOE, Sevagram,India*
nitiket_m@rediffmail.com
[2]*Principal, Bhagwati Chadurvedi COE, Nagpur,India*
drnitinchoudhari@gmail.com

Abstract

In modern generation, the applications of MANET are increasing in use. 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. This paper presents an approach for determining conditions under which critical nodes should be monitored. Here, we focus on the trigger mechanism for the invocation of critical node test for MANET Intrusion Detection system.

Keywords*: MANET, IDS, edge-cut, mobile adhoc network*

1. Introduction

MANET 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[10][11][12].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.

2. 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 Evaluating 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]

3. Identification of Critical Nodes

Our approach in this paper is based around the notion of a critical node in an adhoc network. A Critical node is a node whose failure or malicious behavior disconnects or significantly degrades the performance of the network.

Once identified, a critical node can be the focus of more resource intensive monitoring or other diagnostic measures. If a node is not considered critical, this metric can be used to help decide if the application or risk environment warrant the expenditure of additional resources requires monitoring diagnosis and altering other nodes about problem.

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.

Finding a cut-vertex in the graphical representation of an adhoc network is not straightforward, since the nodes cannot be assumed to be stationary. Similarly, determining the global network topology in a mobile adhoc network given the time delays of the diagnostics packets and mobility of the nodes make this difficult, but determining the approximation of this topology or subset of this topology, within a certain time frame may be useful.

An approximation of the network topology can provide useful information about network density, network mobility, critical paths and critical nodes.

3.1. Steps for Critical Node Test

3.1.1 Basic Steps:

- The node performing the test is referred to as testing node and the node under test is referred as node under test.
- Use of ip ,route and ping utilities. The ip utility is a TCP/IP interface configuration and routing utility that configures the network interfaces.
- 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.
- 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.

3.1.2 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.

A. First Stage

- 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.
- The enabled communication link will be between the testing node and a node other than the node under test.
- Each communication link has to test sequentially in this way to determine if an alternative path to the link under test exists.
- If an alternative path exists, then the link is not critical because its removal will not disconnect the network.

B. Second Stage

- This stage is for the host to attempt to discover an alternative path by using ping to the node under test without using the suspected cut-edge between the testing node and node under test.
- 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

C. Third stage

- When the results of the ping are returned, the network routing table is restored during this final step to its initial configuration.
- 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.

- Critical node conditions however are likely to occur when a node has a relatively small degree and therefore fewer tests are required.

3.2. Consideration of Trigger Mechanism

Critical node test determines the nodes whose failure or malicious behavior disconnects or degrades the performance of the network. In order to further reduce the number of test performed, a lightweight trigger mechanism is considered which monitors network traffic and initiates a critical node test when it suspects such a condition might exist. Trigger mechanism is used to allow false Positives that the critical node test will later screen out. The only false negatives that can occur are when there is no traffic to analyze on a cut-edge, but this condition is most likely short-lived and of no consequence. The trigger mechanism monitors the number of connections served by the node as well as the number of packets traversing the test node.

The trigger mechanism runs on a testing node and records Ethernet and IP address of each incoming and outgoing packet that is routed through the testing node. The testing node does not store any packets it sends or receives; instead it tabulates statistics on the Ethernet and IP packet headers. The testing node tabulates information such as ID of each neighboring node, its IP address, MAC address and time that the packet was forwarded. Also, testing node counts the no. of peer-to –peer pair connections that traverse the testing node. Here, the term connection refers to a pair of nodes that have a peer-to-peer TCP, UDP or ICMP connections. These peer-to-peer connections are associated with Ethernet source address, if the packet is incoming or with the neighbour's MAC Ethernet destination address, if the packet is outgoing.

The trigger mechanism can distinguish between these two cases because if the testing node‘s MAC address is in the Ethernet destination field, that means the destination is the testing node therefore it is an incoming packet. If the testing node's MAC address is located in the Ethernet source field this means that the host is either generating this packet or host is forwarding the packet. The trigger mechanism creates two tables; incoming packets and outgoing packets. From this table, the trigger mechanism tries to determine if several nodes rely on communication link incident to the testing node or if the incident communication link is responsible for significant amount of traffic. If either of this condition occurs, the trigger mechanism can invoke the critical test. The trigger mechanism is configurable and requires no changes to the routing table.

4. Conclusion

This paper effort to explain critical node test mechanism briefly. Here, we focus on critical node and detection of critical link by using basic routing utilities. It is inferred that when a critical link is detected, the host node may choose expend additional resources to initiate an IDS module that is more resource intensive, such as traffic monitoring watchdog module or collaborative IDS. But if there is no critical link then the host can use the lighter weight modules to continue to monitor network traffic. This paper emphasis on consideration of trigger mechanism which can invoke the critical test. Thus we may conclude that trigger mechanism is a lightweight solution that can be used to determine the proper conditions to activate a more demanding IDS .This paper submits the approach for detecting critical links and which may be used to provide guidance for how the location of nodes in an adhoc network might be better physically arranged in order to provide more fault tolerance and better Quality of service.

5. 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 6 th 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] A. 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] Puttini, R; Percher, JM; Me, L, Camp, O; de Sousa, R. A Modular Architecture for a Distributed IDS for Mobile AdHoc Networks. Lecture Notes on Computer Science vol.2669, Springer-Verlag, pp. 91-113, 2003.

[11] Ngai, Edith C. H., and Lyu, M. R.. Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks. 24th International Conference on Distributed Computing Systems Workshops, vol. 04, pp. 582-587, 2004.

[12] Parker, J., Undercoffer, J. L., Pinkston, J., and Joshi, A.On Intrusion Detection in Mobile Ad Hoc Networks. In 23rd IEEE International Performance Computing and Communications Conference – Workshop on Information Assurance. IEEE, April 2004.

Authors

Mr. Nitiket N. Mhala is PhD student and also working as Associate Professor & Head in the Department of Electronics Engineering, Sevagram, India. He received his ME Degree from RM Institute of Research and Technology, Badnera, Amravati University and BE Degree from Govt. College of Engineering, Amravati, Amravati University. He published a Book Entitled PC Architecture and Maintenance. He published research papers at National and International level. He is a member of Institute of Electronics and Telecommunication Engineer (IETE). His area of interest spans Data communication, Computer network and Wireless Ad hoc networks.

Dr. N. K. Choudhari is a Professor and completed his Ph.D degree in Electronics Engineering from J.M.I., New Delhi and received his M.Tech in Electronics Engineering from Visveswa-raya regional Engineering College, Nagpur. He received his BE in Power Electronics from B.D.C.O.E., Sevagram. Presently he is Principal at Smt.Bhagwati Chaturvedi COE, Nagpur, India. He is guiding few research scholars for pursuing Ph.D degree in RTM Nagpur University, Nagpur, India. He has worked as member of different advisory committees and was a member of Board of Studies Electronics Engg. of RTM Nagpur University, Nagpur, India.