An Adaptive Risk Aware Response Mechanism for Routing Attack in MANET

[*]Manopriya.V,[*]S.EstherShalinRooth,[*]C.S.Celin,[**] Prof.Venkata subramanian.D

[*]Postgraduate,Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai
[**]Professor,Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai

Abstract- Mobile Ad-hoc Network is a volatile infrastructure network. It is dynamic in nature i.e. it consists of movable nodes. Due to its changing topology it tends to get attacked by unauthorized access. Among various attacks routing attack is the one which causes severe damage to the network infrastructure. There exist a number of techniques and methodologies to overcome this problem but almost all these techniques concentrates on isolating the node at the instant it is being attacked which further ruins the network. In this paper, a filtering technique is proposed to reduce the permanent isolation of nodes.

Index Terms- MANET, Routing attack, Intrusion response, OLSR protocol.

I. Introduction

Secure computing explains how the computer related resources are protected from unauthorized access. The main aim of secure computing is to provide data integrity, confidentiality, reliability and authentication. Using Cryptography, Secure networks, Antivirus software and Firewalls are some of the existing techniques for protecting the resources from being attacked or misused. Authentication is actually an assurance that the communicating entity is the one claimed.Information & Network penetrations do occur from outsiders &insiders in spite of having various security measures .There are two ways to attack computers. Gain physical access to machines and conduct physical attack; Attack by use of malicious software. The advantage of Security in network is that it helps to protect personal data of the computers communicating in the network.

The disadvantages include firewalls may be difficult to configure and sometimes incorrectly configured firewalls may block users from performing certain actions on the Internet. At times it makes the system slower than before.

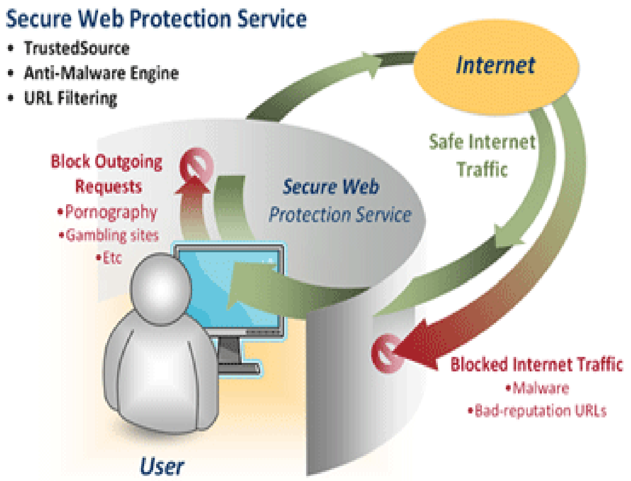

Figure 1.Secure Computing Architecture

II. MANET

A Mobile Ad-hoc network is a wireless ad-hoc network which is used to exchange information. Each node is willing to forward data to other nodes. In MANET a node may function as both host and a router. The control and management Operations are distributed among the terminals since there is no fixed network. It has multi-hop routing facility. i.e. packets can be delivered via one or more nodes. As the network change rapidly, the Mobile nodes dynamically establish routing among themselves and they form their own network. Due to the sharing of end-to-end path by several sessions it has fluctuating link capacity. The MANET nodes are mobile devices with less CPU processing capability.

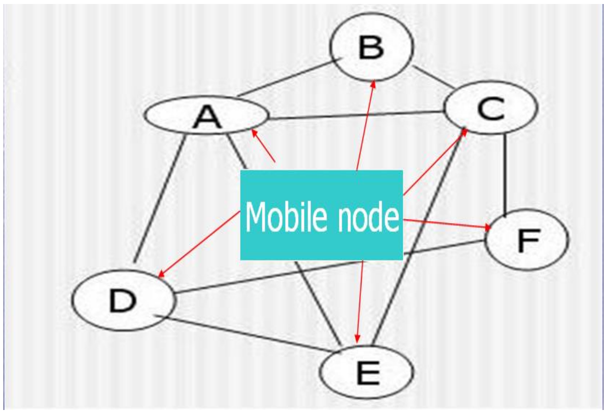

Figure 2. MANET Architecture

Some of the cons in using Mobile Ad-hoc Network are Routing, Security and Reliability, Quality of Service, Internetworking and Power Consumption. Among these the major issue is establishing security within the network.

APPROACHES FOR PROTECTING MOBILE AD-HOC NETWORKS:

A. Reactive approach: Seeks to detect security threats and react accordingly.

B. Proactive approach: Attempts to prevent an attacker from launching attacks through various cryptographic techniques with the help of a protocol misbehaving nodes can be identified and make them unable to interfere with routing. Some of the schemes are neighbor-monitoring, trust-building, and cluster-based voting schemes which are used to detect and report the malicious activity in ad hoc networks.

III. ROUTING ATTACK

Routing attack affects the routing in the network. This can be done by impersonation, modification, fabrication and replay. The following table represents the types of routing attack and the necessary measures to overcome it.

The following two incidents are one of the biggest security breach occurred because of incorrect routing messages being propagated across the Internet.

a. YouTube blockage by Pakistan Telecom

In February 2008, Pakistan Telecom filtered access to YouTube, by sending new routing information via Border Gateway Protocol to PCCW, an ISP in Hong Kong that propagated the false routing information across the Internet.

b. ICANN’s server attack

The Internet Corporation for Assigned Names and Numbers (ICANN) screwed up in November 2007 when it renumbered the DNS root server "L" that it operates. By May 2008, ICANN had all the fake L root servers turned off.

S. NO	NAME OF THE ATTACK	DESCRIPTION	COUNTER MEASURES
1	Flooding attack	Exhaust network resources,	Calculate rate of neighbors RREQs, block if they exceed threshold
2	Black hole attack	Attacking node returns fake routing information, causing the source node to choice a route through it, the attacker can then misuse or drop messages as it sees fit.	Introduce route confirmation requests CREQ and route confirmations reply CREP
3	Link Withhold attack	Attacker does not advertise a link to a specific node or group of nodes	Nodes listen for the TC message from the MPR node they selected, if they do not hear one that MPR node is rated suspicious and additional MPR nodes are selected.
4	Link Spoofing attack	A attacking link advertises links to non-neighbors, by faking links to the two-hop neighbors and can become one of its MPR nodes, and then manipulate traffic.	Equip nodes with GPS and calculate whether two nodes could really have a link.
5	Colluding Mis-relay attack	Two colluding attackers modify or drop packets	An acknowledgment system could detect this but will increase overhead.

Table 1.Routing Attacks and Counter measures

IV. PROPOSED WORK

To avoid the network partition due to isolation of malicious node, Extended Dempster Shafer mathematical theory and its associated properties are used. Following are the steps involved in the risk aware response mechanism.

a. Evidence collection: In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

b. Risk assessment: Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

c. Decision making: The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.

d. Intrusion response: With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

e. Routing table recovery:

Routing table recovery serves as the first response method after successful detection of attacks. The proactive routing protocols like OLSR is used since it periodically goes with routing control messages. It does not bring any additional overhead .Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

V. CONCLUSION

This paper proposes the challenges of routing attack in MANET and the necessary measures needed to overcome the attack. Dempster Shafer theory and its properties are being employed for evidence collection. Further to minimize the isolation of nodes, filtering technique is applied. In future to avoid permanent isolation of nodes, Breadth First Search and Depth First Search techniques can be used by which alternative routes are determined. Based on several metrics, the performance and practicality of this approach is investigated and the experiment results clearly demonstrate the effectiveness and scalability of risk-aware approach

REFERENCES

[1] L.Sun, R.Srivastava and T.Mock,”An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions”.

[2] M.Rafaei, L.DaSilva, M.Eltoweissy and T.Nadeem,”Adaptation of Reputation Management Systems To Dynamic Network Conditions in Ad-hoc Networks”.

[3] P.Karger, G.Wagner and A.Renimger P.Cheng, P.Rohatgi, C.Keser,”Fuzzy Multi-level Security: An Experiment on Quantified Risk-Adaptive Access Control”.

[4] S.Wang, C.Tseng, K.Levitt and M.Bishop,”Cost Sensitive Intrusion Response for Mobile Ad-hoc Networks”.

[5] Y.Sun,W.Yu,Z.Han and K.Liu,”Information Theoretic Framework of Trust Modeling and Evaluation for Ad-Hoc Networks”.

[6] ZimingZhao, HongxinHu,Gail-JoonAhn and RuoyuWu,”Risk-Aware Mitigation for MANET Routing Attacks”.

[7] C. Tseng, S. Wang, C. Ko, and K. Levitt, “DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for Manet,” Proc. Ninth Int’l Symp. Recent Advances in Intrusion Detection (RAID ’06), pp. 249-271, 2006.

[8] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt, “A Specification-Based Intrusion Detection Model for OLSR,” Proc. Ninth Int’l Symp. Recent Advances in Intrusion Detection (RAID ’06),pp. 330-350, 2006.

[9] N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, “Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET,” IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.

[10] J. Felix, C. Joseph, B.-S. Lee, A. Das, and B. Seet, “Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA,” IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, pp. 233-245, Mar./Apr. 2011.

[11] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. ACM MobiCom, pp. 255-265, 2000.

[12] S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour, “Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method,” Int’l J. Network Security, vol. 105, no. 627, pp. 65-68, 2006.

AUTHORS

First Author – Manopriya.V, Postgraduate, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, Email: Celin.cs7@gmail.com

Second Author – S.Esther Shalin Rooth, Postgraduate, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, Email: esthershalin@gmail.com

Third Author – C.S.Celin, Postgraduate, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, Email: vmanopriya@gmail.com

Fourth Author – Prof.Venkata Subramanian.D, Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, Email: venkatasubramanian@saveetha.com