International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 8, August - 2013

Minimizing the risk of routing attacks in MANET by using DRCIF

Ashwini Jeerge
M.Tech Computer Science Engg.
Guru Nanak Dev Engineering College, Bidar, India

Prof. Dayanand Jamkhandikar
Computer Science Engg. (CS)
Guru Nanak Dev Engineering College, Bidar, India

Prof. Rajshekhar Gaithond
Information Science Engg. (IS)
Guru Nanak Dev Engineering College, Bidar, India

Abstract— Mobile Ad Hoc Network (MANET) is distinguished from other networks mainly by its self configuring and optimizing nature. Being the flexible network, MANET is exposed to various kinds of attacks especially the routing attacks, and it has received considerable attention since it could cause the most devastating to MANET. Attack prevention methods such as intrusion detection system, intrusion prevention, authentication and encryption can be used in defence for reducing certain attack possibilities. In case of intrusion response techniques to mitigate such critical attacks, existing solution typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. However, binary responses may lead to unexpected network partition, causing additional damage to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. In this paper, we propose a risk-aware response mechanism to systematically cope with the identified routing attacks. This approach is based on an extended Dempster-Shafer mathematical theory of evidence by introducing a notion of importance factors. The plotted graphs of packet overhead, byte overhead and packet delivery ratio demonstrates the effectiveness of this approach.

***Index Terms*— Ad hoc networks, Dempster-Shafer theory, Dempster rule of combination with important factors (DRCIF).**

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET) is distributed and self configuring wireless network. MANET does not have a predefined network infrastructure. Application of MANET is benefited in areas such as military services, disaster relief and mine site operations. Each node communicates with the other acting as routers. The co-operation and trust between the nodes are depended for the proper functioning of this network. Since the network topology in MANET changes unpredictably and rapidly it is highly vulnerable to various kinds of attacks. Attack prevention methods such as intrusion detection system, intrusion prevention, authentication and encryption can be used in defense for reducing certain attack possibilities. MANET is considered one of the most promising fields in research and development of wireless networks. There exist many intrusion response mechanisms for routing attacks. The existing techniques usually attempt to isolate the malicious nodes from the topology there by causing the partition of network topology. Methods such as binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. Several intrusion detection techniques have been introduced for detecting the malicious nodes and preventing the neighbor nodes compromised by the malicious nodes. Even though many mechanisms and routing protocols are introduced each of them has one or more vulnerabilities. Research on MANET and implementation has become a huge amount of task to be done. When a malicious node is being identified the node has to be either repaired or another route has to be established. In most of the existing techniques the nodes when found slightly malicious is completely isolated from the network which will make splitting of the network and thereby causing communication problems between the nodes. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damage to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Subjective knowledge could be retrieved from previous experience and objective evidence, and objective evidence could be retrieved from previous experience and logical reasoning. Subjective knowledge could be obtained from observation while logical reasoning requires a formal foundation.

II. EXTENDED DEMPSTER-SHAFER THEORY OF EVIDENCE

The Dempster-Shafer mathematical theory of evidence it is both a theory of evidence and a theory of probable reasoning.

While Dempster's rule of combination is the procedure to aggregate and summarize the evidences. However, previous research efforts identify several limitations of the Dempster's rule of combination (DRC).

1. Associative- For DRC, the order of the information in the aggregated evidences does not impact the result, a non associative combination rule is necessary in many cases.

2. Nonweighted- DRC implies that we trust all evidences equally. Here we should consider various factors for each evidence.

III. DEMPSTER'S RULE OF COMBINATON WITH IMPORTANT FACTORS

In this section, we propose a Dempser's rule of combination with important factors. The algorithm for extended Demster-Shafer theory is given below.

Algorithm MUL-EDS-CMB

INPUT: Evidence pool Ep
OUTPUT: One evidence

1. |Ep|= sizeof(Ep);
2. While |Ep|>1 do
3. Pick two evidences with the list IF in Ep, named E1 and E2;
4. Combine these two evidences, E= <m1+m2 ,(IF1+IF2)/2>;
5. Remove E1 and E2 from Ep;
6. Add E to Ep;
7. End
8. Return the evidence in Ep.

IV. DESIGN MODULES

Routing table: includes local routing table recovery and global recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table. Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based through protocols like (AODV/OLSR).

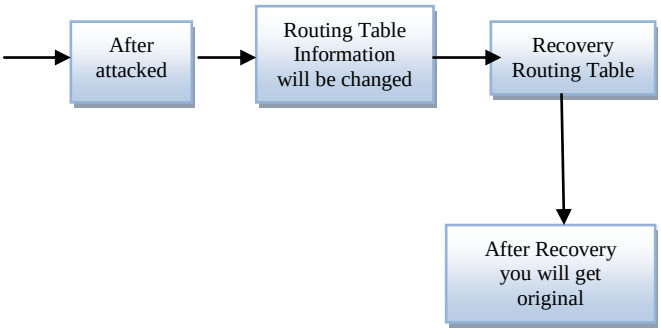

Figure 1: This figure shows the Routing table.

Evidence Collection: In this Module, we can collect the evidence of attacker node. There are two types to collect the evidence.

1. IDS-Gives an Attack Alert.
2. RTCD- How many changes on the routing table.

In this module, 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.

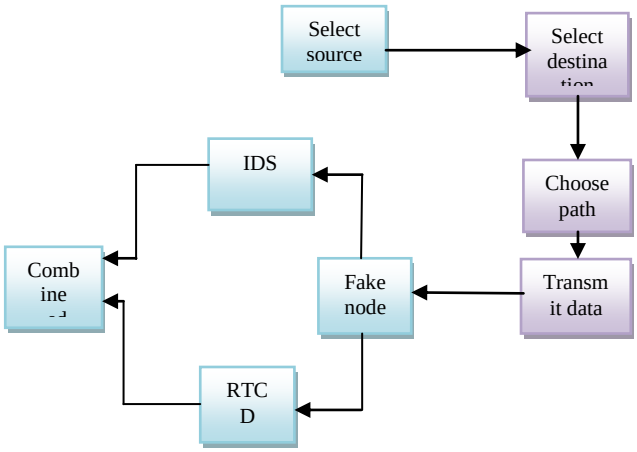

Figure 2: This figure shows the Evidence collection.

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.

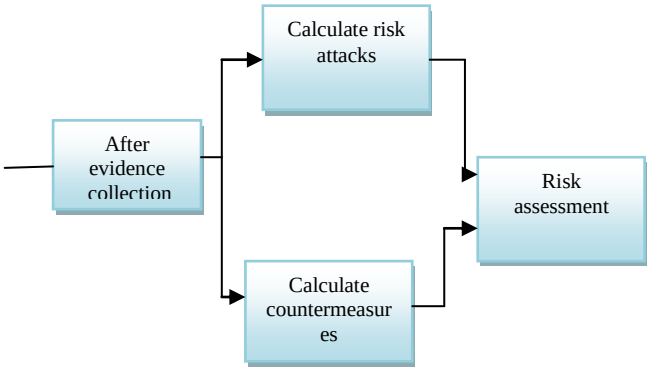

Figure 3: This figure shows the Risk assessment.

Node isolation: It is the most intuitive way to prevent further attacks from being launched by malicious nodes in MANET. To perform a node isolation response, the neighbours of the malicious node ignore the malicious node by neither forwarding packets through it nor accepting packets from it. On the other hand, a binary node isolation response may result

in negative impact to the routing operations, even bringing more routing damages than the attack itself.

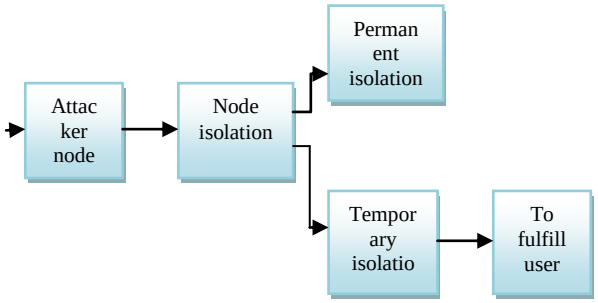

Figure 4: This figure shows the Node isolation.

V. FEATURE DESIGN

We propose adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The addictiveness of our mechanism allows us to systematically cope with MANET routing attacks. We evaluate our response mechanism against representative attack scenarios and experiments. Our result clearly demonstrates the effectiveness and scalability of our risk-aware approach.

VI. WIRELESS SIMULATION

The network simulation-2 implementation contains the following parts.

- Generating wireless environment.
- Creating UDP and FTP agent.
- Various modules are added to simulate node mobility and wireless networking such as mobile nodes, ad-hoc routing such as MAC 802.1, AODV.

Table 1 Show the simulation parameters where the simulation was implemented by using NS2 (network simulator 2.35) [14].

Table 1: Simulation parameter

Simulator	NS-2.35
Routing protocol	AODV,OLSR
Number of nodes	Max 80
Simulation area	2000X2000
Simulation time	500sec
Traffic type	CBR
Mobility speed(m/s)	5,10,15,20
Data packet size	250 bytes
Mobility model	Random way point model
Node transmission range	150m

The below figure 5 shows the simulation at NAM. This simulation modeled in a network area 900X900 m with 80 mobile nodes, routing protocols that we used here are AODV and OLSR. Mobility model used is random way point model, each node randomly selects the moving direction and when it reaches to the boundary of simulation area, it bounces back and continues to move. The mobile speed of each node was from 1 to 25 m/s. Constant Bit Rate (CBR) is used as traffic type. The transmission range was 150m. Data packet size used was 250 bytes.

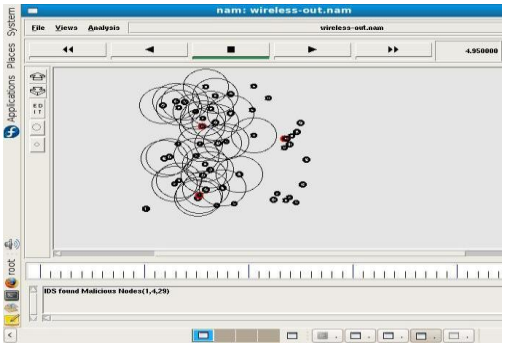

Figure 5: Simulation at NAM

VII. SIMULATION RESULTS.

Figs. 6-8, describe the performance of the system that is packet overhead, byte overhead, Packet delivery ratio with the different number of nodes. **Fig. 6** shows that the packet overhead increases as the number of nodes increases.

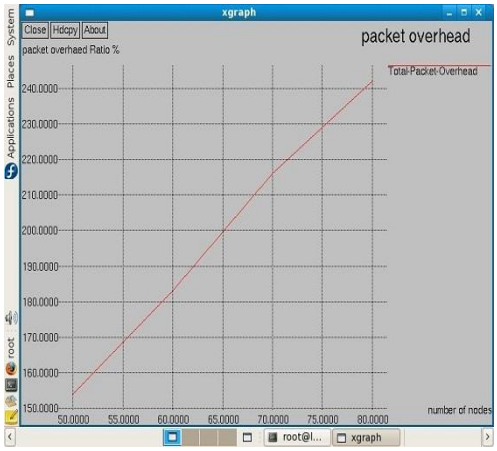

Figure 6: Packet overhead Ratio against number of nodes.

Analysis: In this DRCIF risk-aware response, the number of nodes which isolate the malicious node is less than the other methods. From the figure 6 and 7, we can notice that as the number of nodes increases, the packet overhead and the byte overhead using this DRCIF risk-aware response are slightly higher than those of the other mechanisms.

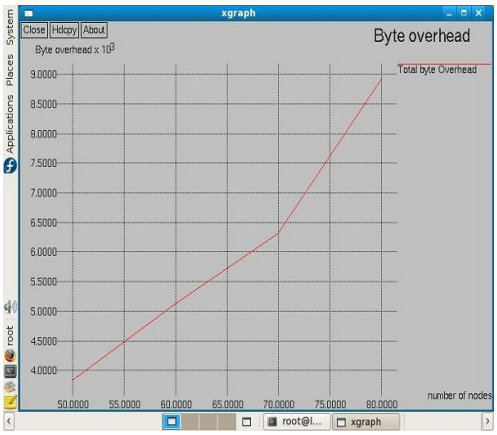

Figure 7: Byte overhead against number of nodes.

Figure 8 describes the packet delivery ratio, as the number of nodes increases packet delivery ratio also increases because there are more route choices for packet transmission.

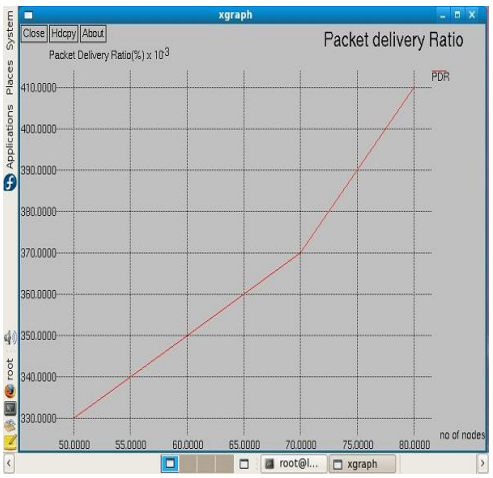

Figure 8: Packet Delivery Ratio Against number of nodes.

VIII. CONCLISION.

In this work, an adaptive risk-aware mechanism with extended trusted centre has been proposed which reduces the MANET routing attacks. Risk-aware approach is based on D-S theory with important factors, and hence it provides maximum trust worthiness and more security in MANET routing. Based on several metrics we also investigated the performance and practicality. The experiment result clearly demonstrated the effectiveness and scalability of our risk aware approach. Based on the promising results obtained through these experiments, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

IX. REFERENCES.

[1]. Y. sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of Trust Modelling and Evaluation for Ad Hoc Networks," IEEE J. Selected areas in comm.., vol. 24, no. 2, pp. 305-317, Feb. 2006.

[2]. M. Refaei, L. Dasilva, M. Eltoweissy, and T. Nadeem, "Adaptation of Reputation Management systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computer, vol.59, no. 5, pp. 707-719. May 2010.

[3]. P. Cheng, p. Rohatgi, c. Keser, p. Karger, G. Wangner, and A. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," proc. 28th IEEE Symp. Security and Privacy, 2007.

[4]. S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost-Sensitive Inrution Responses for Mobile Ad Hoc Networks," Proc. 10th Int'l Symp. Recent Advances in Intrusion Detection (RAID 07), PP. 127-145, 2007.

[5]. G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976.

[6]. Sun, R. Srivastava, and T. Mock, "An Information System Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Function," J. Management Information System, vol. 22, no. 4, pp.109-142, 2006.

[7]. C. Mu, X. Li, H. Huang, and S. Tian, "online Risk Assessmnt of Intrution Scenarios Using D-S Evidence Theory," proc. 13th European symp. Research in Computer Security (ESORICS'08), PP, 35-48, 2008.

[8]. K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," technical report, sandia Nat,l Laboratories,2002.

[9]. C. Perkins, E.Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance vector routing," Mobile Ad-Hoc Network Working Group, vol.3561,2003.

[10]. H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Insrumentation and Measurement Technology Conf., vol. 1,pp. 7-12, 2002.

[11]. T. Clusen and P. Jacquet, "Optimized Link State Routing Protocol," Networking Working Group, 2003.

[12]. H. Deng, W. Li, and D. A grawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, oct. 2002.

[13]. Y. Hu and A. Perrig, "A Survey of secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol.2, no. 3, pp.28-39, May/June 2004.

[14]http://www.isi.edu/nsnam/ns/index.html.