

Risk - Aware Management of MANET Routing Attacks based on Node Reputation and Attack Frequency

Mr. S. Arunsoundar#1, Mr. S. P. Santhoshkumar #2, Dr. S. Karthik#3

#1UG Student, Department of CSE, SNS College of Technology, Coimbatore, India.

#2Assistant Professor, Department of CSE, SNS College of Technology, Coimbatore, India.

#4 Professor & Dean, Department of CSE, SNS College of Technology, Coimbatore, India.

Abstract—Mobile Ad Hoc Networks are used for establishing wireless communication in environments without any predefined infrastructure or centralized administration. Its network topology is dynamically changing owing to the mobile nature of the nodes. So, it is highly vulnerable to attacks. Among all the attacks, routing attacks cause the most severe damage. A simple binary isolation of the malicious nodes is not a practical solution. The countermeasure may pose a greater risk than the attack itself. Thus, a risk aware mitigation response mechanism is needed. In this paper, we propose a risk aware approach which includes the concept of node reputation while determining the risk factor. The threshold value for determining the risk level is adjusted by keeping into account the node reputation and attack frequency. The appropriate intrusion response is then initiated.

Keywords — Mobile Ad - hoc Network, Routing attacks, Risk Assessment, Node Reputation, Attack Frequency, Intrusion Response

I. INTRODUCTION

MANETs are characterized by their unique features such as dynamic topology and limited constraints. Various routing protocols have been proposed for MANETs. MANET protocols assume a trusted and co-operative environment. However, in reality various attacks are initiated by malicious as well as selfish nodes. Of all the attacks, routing attacks cause the most severe damage to the operation of the network. The routing attacks include flooding, black hole attack, link spoof attack, replay attack and the worst of all

the wormhole attack. Several intrusion detection techniques are proposed to mitigate such attacks. The simplest response is the binary isolation of malicious nodes. But network partitions and uncertainty arises due to binary isolation, which may be critical in a mobile ad hoc network. A risk-aware approach for flexible node isolation based on Dempster - Shafer mathematical theory of evidence is introduced. The D-S theory is extended by using a notion of importance factors and combined evidences. This works best for OLSR protocol. This mechanism tries to combine evidences such as alert confidence from the Intrusion Detection System (IDS) and the possible cases of changed entries in the routing table for risk assessment.

In this paper, we have introduced the concept of node reputation. The risk tolerance threshold value is adjusted based on node reputation and node frequency. The reputation index of the node is arrived based on their past successful delivery of data packets. This reputation level of a node can be used by their neighbor nodes to assess the risk of that particular node isolation.

This mechanism has the following advantages

- 1) Packet delivery ratio increases
- 2) Encourages more co-operation among the nodes thereby indirectly reducing attacks
- 3) Reduces attacks induced by selfish behavior of nodes since nodes always try to increase their reputation level.

II. BACKGROUND

- A. MANET Routing Protocols

- 1) AODV Protocol In Ad-hoc On-Demand Distance Vector Routing (AODV) protocol, each mobile host operates as a specialized router and routes are obtained as and when needed. There is no need for periodic advertisements. This protocol provides loop-free routes and bandwidth usage is much lesser [1].
- 2) OLSR Protocol the Optimized Link State Routing (OLSR) protocol is proactive or table-driven in nature. The topology information is maintained by use of periodic exchange of messages. OLSR protocol is a variation of the pure link - state routing protocol. It uses multipoint relay to reduce the number of exchange messages [2].

B. Routing Attacks

The typical routing attacks include black hole, flooding, replay, colluding and wormhole attack [3]. These attacks fabricate or modify the various fields in routing packets (route request message, route reply message, route error message etc.).

These routing attacks are caused by either malicious nodes or selfish nodes. Malicious nodes initiate active attacks which are intentional and are aimed at disrupting the smooth operation of the MANET. On the other hand, selfish nodes initiate passive attacks and are usually a side effect of a particular node aiming at preserving their limited resources or pure selfishness. Intrusion prevention techniques such as encryption and authentication are used as a first line of defense and are not sufficient for prevention of routing attacks. So some form of mechanism is necessary to detect an intrusion if it happens, to act as a second line of defense.

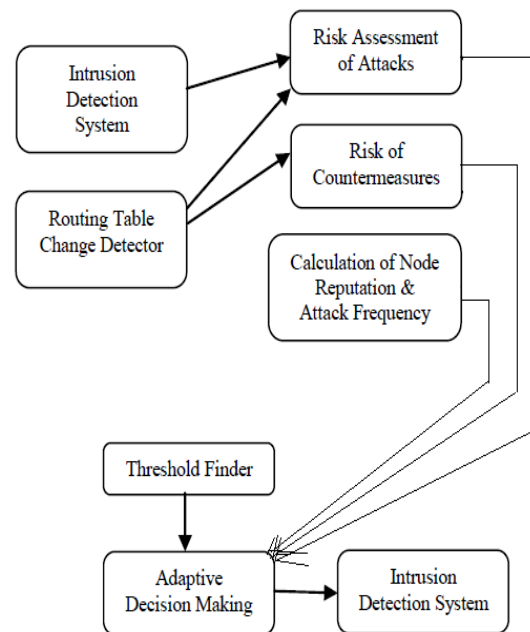


Fig. 1. Risk-aware Response Mechanism with Node Reputation

C. Intrusion Detection System

Intrusion detection can be defined as the process of monitoring activities in a system. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. The number of new attacks is likely to increase quickly and those attacks should be detected before they can do any harm to the systems or data. This can be achieved by a mechanism called Intrusion Detection System (IDS). Various intrusion detection systems such as watchdog and path rater have been proposed [5]. All intrusion detection systems are structured to be distributed and have a co-operative architecture.

III. INTRUSION RESPONSE MECHANISM

The risk-aware response mechanism is based on quantitative risk estimation and risk tolerance. Instead of simple binary isolation of malicious and selfish nodes, our approach follows a risk-aware time-wise isolation. The Dempster-Shafer rule of combination with importance factors (DRC-IF) is replaced with a mechanism which incorporates node reputation (DRC-IF-NR). This mechanism is divided into the following phases.

A. Evidence Collection

The Dempster-Shafer mathematical theory of evidence is both a theory of evidence and probable reasoning. The Dempster's rule of combination is the aggregation of all evidences. Important factor (IF) is a positive real number derived from historical observations and expert experiences and is associated with the importance of evidence. An evidence E is a tuple $\langle p, IF \rangle$ where p is the probability of E. The basic probability assignment function p is defined as

$$p(\emptyset) = 0 \tag{1}$$

and

$$\sum p(A) = 1 \tag{2}$$

where $A \subseteq \theta$ and θ is a finite set of states and A is evidence. In D-S theory, propositions are represented as subsets of a given set. Suppose θ is a finite set of states, and let 2^θ denote the set of all subsets of θ . θ is called as the frame of discernment by the D-S theory. Suppose E1 and E2 are two evidences with important factors IF1 and IF2 respectively, and then the combined evidence is given by

$$E_c = \langle p1 \oplus p2, (IF1 + IF2)/2 \rangle \tag{3}$$

$$E_c = E1 \oplus E2 \tag{4}$$

The alert confidence value given by the IDs and the routing table changing information are considered as independent evidences and are combined by the extended D-S theory.

B. Node Reputation and Attack Frequency

Node Reputation index is a useful measure to encourage cooperation among nodes. It is an efficient parameter to counter malicious nodes [6] and selfish nodes [7]. Node Reputation based on the previous history can be used to increase the packet delivery ratio and throughput. Each node maintains a Node Reputation table, which stores the reputation value for each of the node's next hop neighbors. Consider a set of nodes $N = \{1, 2, \dots, N\}$, then R_{ij} is the reputation index value of node j as signed by node i, for all $i, j \in N$; $dist(i, j) = 1$ where $dist(i, j)$ is the distance in hops between nodes i and j.

Attack Frequency is one another important factor in determining the risk level. Higher the attack frequency, the entire operation of the MANET is in jeopardy. So an attack frequency should be maintained to adjust the threshold levels accordingly.

C. Assessment of Risks

In the risk assessment phase, the combined evidence is used to calculate the risk of the attack. Risk of countermeasures is also calculated during this phase. The entire risk of an attack can be figured out based on the risk of attack and risk of countermeasures. The overall risk is calculated as

$$Risk = RiskA - RiskCM - NR \tag{5}$$

A denotes the attack; CM denotes the countermeasure and NR denotes the node reputation value. If the node reputation value is positive, the risk level reduces. If the node reputation value is negative, the risk level increases.

A function $Bel: 2^\theta \rightarrow [0, 1]$ is a belief function over θ for some basic probability assignment $p: 2^\theta \rightarrow [0, 1]$ if it is given by

$$Bel(A) = \sum p(B) \tag{6}$$

for all $B \subseteq A$; $Bel(A)$ is the measure of local beliefs committed to the evidence A. Thus $BelA(Insecure)$ and $BelCM(Insecure)$ represent the risk of attacks and risk of CM respectively [12] [13].

$$Risk = BelA(Insecure) - BelCM(Insecure) - NR \tag{7}$$

D. Adaptive Decision Making

The adaptive decision making is based on risk tolerance. Decision making is determined based on the risk tolerance threshold and consists of the following three levels of isolation.

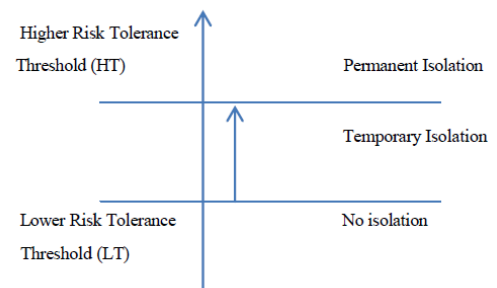


Fig. 2. Time-wise isolation

1. No isolation: The lower risk tolerance threshold (LT) would result in no isolation and all the nodes remain intact.
2. Temporary isolation: If the risk level falls between the lower risk tolerance thresholds (LT) and higher risk tolerance threshold (HT), the appropriate response would be temporary isolation.
3. Permanent isolation: If the risk level is above the higher tolerance threshold (HT), the decision would be permanent isolation.

E. Risk-Aware Response

The routing attacks are dealt with two different responses based on the type of attacks: node isolation and routing table recovery.

1. Node isolation: Based on the adaptive decision making, either temporary isolation or permanent isolation of the malicious nodes takes place. Node isolation is initiated by the neighbors of the malicious node. The neighbors ignore the malicious node by neither forwarding packets through it nor accepting any packets from it.
2. Routing table recovery: Routing table recovery includes local and global recovery. Local routing table recovery is done by the victim nodes that senses the attack and recover its own routing table. On the other hand, global recovery is done by other nodes in the MANET by updating their routing table based on the locally recovered routing information.

IV. RISK-AWARE RESPONSE ALGORITHM

A. DRC-IF-NR-AF Algorithm

This algorithm enhances the DRC-IF mechanism by including the node reputation and attack frequency as an important factor. The risk-aware response mechanism based on node reputation is drafted as follows:

DRC-IF-NR-AF algorithm

```
Assign Lower Risk Threshold (LT)
Assign Higher Risk Threshold (HT)
Assign Reputation table to all nodes N
For each route request from node i
If successful delivery then
increase rij, j ∈ N
```

```
Else
decrease rij, j ∈ N
End if
Update Node Reputation Table
End-for
For each attack alert from IDS
Increase AttackFrequency(AF)
Adjust LT and HT based on AF
Calculate Risk = RiskA - RiskCM - NR
If Risk <= LT then No action
If Risk > LT and Risk <= HT then
Perform Temporary isolation
Else
Perform Permanent isolation
End-if
End-for
Update Routing Table
```

In this section, the conditions of the algorithm are specified. The simulation has number of underlying parameters which defines the behavior of the system. Packet Delivery Ratio and Average Query Delay are considered as the metric to evaluate the effectiveness of each approach. The experiments were done using NS2 by developing a detailed model of the physical, data and network layer which simulate the behavior of a wireless network and allow the mobility of the nodes. The protocol used is AODV. The simulation process is divided into three levels based on the attack phase. Only routing attacks are considered. The three mechanisms considered are

1. Binary Response
2. DRC-IF mechanism
3. DRC-IF-NR-AF mechanism

The simulation parameters are given in Table I.

TABLE I
SIMULATION PARAMETERS

| PARAMETER | VALUE |
|-------------------------|----------------------------|
| Simulator | Ns2 - 2.3x |
| Number of nodes | 50 |
| Simulation Time | 15 min |
| Packet Interval | 0.01 sec |
| Simulation Landscape | 1000 x 1000 |
| Background Data Traffic | CBR |
| Packet Size | 1000 bytes |
| Queue Length | 50 |
| Initial Energy | 100 Joules |
| Transmission Range | 100 Kbytes |
| Node Transmission range | 250 m |
| Antenna Type | Omni directional |
| Mobility Models | Random-waypoint (0-30 m/s) |
| Routing Protocol | AODV |
| MAC Protocol | IEEE 802.11 |

B. Packet Delivery Ratio

It is the ration between the number of packets originated by the application layer and the number of the packets received by the destination. From Fig. 2 we can see that the packet delivery ratio increases as the number of nodes increase. This is because of more choice of routes. Among the three response mechanisms, our DRC-IF-NR-AF mechanism scores better with higher packet delivery ratio.

C. Average Query Delay

The average response time for successful requests, i.e., from sending a request until the response is received. Fig. 3 shows the query delay is substantially reduced in our proposed approach.

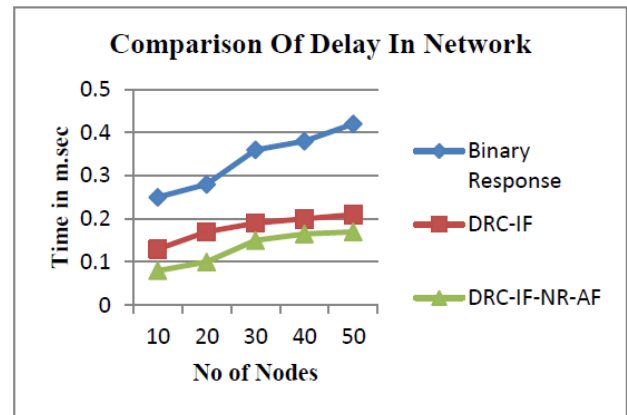


Fig. 4. Average Query Delay

V. CONCLUSIONS

We have proposed a risk-aware mechanism for minimizing MANET routing attacks. The extended Dempster-Shafer theory of evidence with a notion of importance factors is used to measure the risk of both the attacks and countermeasures. The risk tolerance threshold value is adjusted based on node reputation and attack frequency. This reputation level of a node can be used by their neighbor nodes to assess the risk of isolating the particular node. Thus, node reputation acts as an important factor in determining the risk level of the malicious nodes as well as the selfish nodes. The performance of this approach is investigated and the results clearly favor the

REFERENCES

- [1] Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector Routing", Mobile Ad-Hoc Network Working Group, vol.3561, 2003.
- [2] T. Clausen and P. Jacquet, "Opimized Link State Routing Protocol", Network Working Groupo, 2003.
- [3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipur, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp.85-91, Oct 2007.
- [4] S. Marti, t. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", Proc. ACM MobiCom, pp. 255-265, 2000.
- [5] Tiranuch Anantvalee and Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc

Networks.", Wireless/Mobile Network security, pp 17—196, 2006.

[6] P. Dewan, P. Dasgupta and A. Bhattacharya, "On using Reputations in ad hoc networks to counter malicious nodes", Proceedings of the 10th Intl. Conference on Parallel and Distributed Systems, July 2004, pp. 665-672.

[7] "A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks", M. Tamer Refaei, Vivek Srivastava, Luiz DaSilva, Mohamed Eltoweissy, Networking and Services (MobiQuitous '05) 2005.

[8] "Analysis and Feasibility of Reactive Routing Protocols with Malicious Nodes in MANETs", Shilpi Jain, Alankar Shastri, Brijesh Kumar Chaurasia, 2013 International Conference on Communication Systems and Network Technologies.

[9] Wang. C, X. Yang and Y.Gao, 2005. "A routing protocol based on trust for MANETs". Lect.

Notes Computer Science, 3795: 959-964, DOI: 10.1007/111590354_115.

[10] "Mobile Ad Hoc Network Security for Reactive Routing Protocol with Node Reputation Scheme", A. Suresh and Dr. K. Duraiswamy, Journal of Computer Science 7(2): 242-249, 2011.

[11] NS2 Reference from <http://networksimulation.wordpress.com/>

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

[13] Mu, X. Li, H. Huang and S. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory", Proc. 13th European Symp. Research in Computer Security (ESORICS '08), pp.35-48, 2008.

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

IJSHRE