Risk Aware Mitigation for MANET Routing Attacks Using Dempster-Shafer Theory

Prof. B. W. Balkande
Department of Computer Engineering
BharatiVidyapeeth College of Engineering,
NaviMumbai , India.

Gandhali Inamdar
Department of Computer Engineering
BharatiVidyapeeth College of Engineering,
NaviMumbai , India.
.

Prachi Karne
Department of Computer Engineering
BharatiVidyapeeth College of Engineering,
NaviMumbai , India.

Manali Kaundinya
Department of Computer Engineering
BharatiVidyapeeth College of Engineering,
NaviMumbai , India.
.

***Abstract*— MANET (Mobile Ad hoc Network) is wireless network of the mobile computing devices with no support of any fixed infrastructure also highly vulnerable. Thus, network wireless topology may be unpredictable and may change rapidly. Quick deployment and absence of a central governing authority makes ad hoc network suitable for emergency situations like natural disasters, military conflicts, emergency medical situations etc. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. Each node plays an important role to transmit data over network under adversary control could cause significant damage to functionality and security algorithm. So, it uses binary response and naive fuzzy response. However, 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. So we propose a risk-aware approach is based on an extended Dempster-Shafer mathematical theory for effective measures of routing protocol to check its performance.**

Keywords— ***Mobile ad hoc networks, intrusion response, risk aware, Dempster-Shafer theory.***

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. There is no predefined infrastructure or centralized administration in a MANET unlike other networks like Ethernet. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. MANETS have some unique characteristics like dynamic network topology which arises due to mobility of participating mobile nodes, dual functionality of each participating node where each mobile node also plays a role of router while transmitting data packets in network. Because of this a MANET is highly vulnerable to threats and security attacks with even one node compromised.

The routing in MANETs is dependent on routing protocols. Hence the security provided by them is of crucial importance in determining the security of MANET itself. Many approaches to routing protocol attacks have been proposed earlier such as isolation of compromised nodes and deletion of links. However such measures are extreme in nature and often result in disturbing the entire network traffic in MANET. Especially in MANET, such countermeasures may lead to network partitioning or cause damage to infrastructure. It is for these reasons that a need arises for flexible and agile approaches to routing protocols intrusions.

Risk Assessment is can be cause due to the subjective knowledge, objective knowledge and the logical reasoning. Objective evidence information can be gathered from overall

Observation of system, Subjective knowledge information can be gathered from past study experiment result and logical reasoning knowledge information can be gathered from Standard fundamental study. So In this paper, we are going to use mathematical theory Dempster-Shafer theory of evidence (D-S theory), rather than traditional theory of evidence it gives better solution for uncertainty.[6][7]

D-S theory is used for evaluating reliability and security in information systems where precise measurement is impossible to obtain or expert elicitation is required.

In this paper, we propose a risk-aware response mechanism for finding out routing attacks on MANET network while communication between MANET takes place, also gives solution as isolation method for attacker nodes. Our risk-aware approach is based on the extended D-S evidence model. To implement our risk response solution for MANET network we are using MANET proactive protocol. While proactive protocol used in MANET is Optimized Link State Routing Protocol (OLSR).

II. BACKGROUND KNOWLEDGE

Main task of routing protocol is to find out nature of network which can be effectively used to get the all knowledge of

network, so that each node in communication will be able to find out least possible route to destination node. There are several routing protocols are used for MANET. But there are two major category of it reactive protocol and proactive protocol. Example of Reactive protocol is Ad hoc On Demand Distance Vector (AODV) protocol nodes track routes whenever one node wants to send data to the destination node whose route is unknown. Likewise, in proactive routing protocols, example is OLSR (Optimal Link State Routing Protocol), in this routing protocol each node maintains its routing table information up to date by continuously or periodically sending message to every node in the network. [2]

Basically OLSR protocol is extension of the pure Link-state Routing (LSR) protocol and which is designed specifically for MANET. OLSR protocol achieves optimization over LSR by use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required.

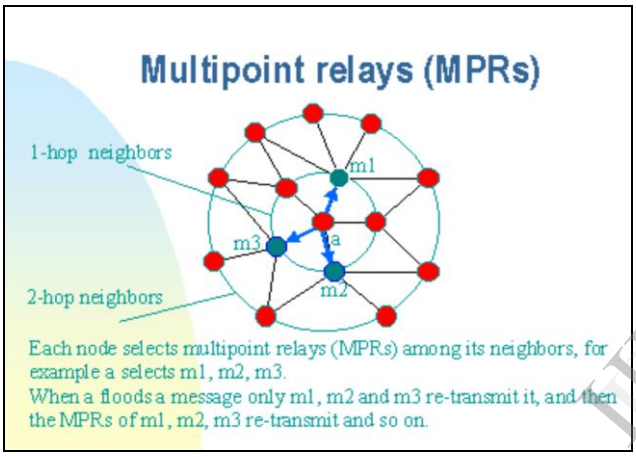


Fig. 1 Multipoint Relays(MPRs)

A. *Routing Attacks On OLSR*

There are two different types of attacks are possible on MANET, active attacks and passive attacks. Active attacks are type of attack which may harm the system or network actually and may cause adverse condition. While passive attacks are types of attack are not actually attacks because in this type communication in network is just observe by attacker by stealing information, these type of attack is hard to detect because there is no change in system configuration or working. Attacks can be further categorized as either outsider or insider attacks. Even on individual layer different types of attacks are possible. On physical layer eavesdropping, on data link layer traffic analysis attacks which of passive type of attack. Typical routing attacks include black hole, fabrication, worm hole attack [5] and modification of various fields in routing packets (route request message, route reply message, route error message, etc.)[3][4]

An attacker node can disrupt the routing mechanism in the system. Depending on nature of attack it causes harmness to system. Initially attacker of any type insider or outsider may discovered itself by showing that it has minimum routing cost path, so indirectly it changes the route of the packet and while in communication once the packet is sent over the route of attacker, then the packet will be received by malicious node. So in that case malicious node can redirect the path of packet so that it will not reach to destination. Or attacker can even drop the packet rather than forwarding to destination. Even in case of attack, malicious node may change the content of the packet, also it may send unwanted request in the communication network so that it may cause network conjetion.[3]

In OLSR, any node can either modify the protocol messages before forwarding them, or create false messages or spoof an identity. Or, the attackers can give wrong information about the topology of a network (TC message) in order to disturb the routing operation.

III. DEMPSTER SHAFER THEORY OF EVIDENCE

The Dempster–Shafer theory (DST) is a mathematical theory of evidence.[1] It allows one to combine evidence from different sources and arrive at a degree of belief (represented by a "belief function") that takes into account all the available evidence.It is both subjective and objective in nature.

Dempster–Shafer theory is based on two ideas:-

1. Obtaining degrees of belief for one evidence from subjective probabilities for a related evidence,
2. Dempster's rule for combining (DRC) such degrees of belief when they are based on independent items of evidence.

The degree of belief models the evidence, while DRC is the procedure to aggregate and summarize a corpus of evidences.However, DRC has two limitations:

1. Associativity: The order of the information in the aggregated evidences does not impact the result .A non-associative combination rule is necessary for many cases.
2. Non-weightedness: Trust all evidences equally. However, in reality, our trust on different evidences may differ.

Hence, the use of DRCIF (DRC with Importance Factor) is made.[6]

A. *Importace Factor*

Importance factor (IF) is a positive real number associated with the importance of evidence. IFs are derived from historical observations or expert experiences.

B. *Evidence*

An evidence E is a 2-tuple {m,IF} where m describes the basic probability assignment. Basic probability assignment function m is defined as follows:

$$m'(\emptyset) = 0$$

and

$$\sum_{A \subseteq \theta} m(A) = 1$$

C. *Belief Function*

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. D-S theory calls Θ, a frame of discernment.
A function Bel : 2^{Θ} [0;1] is a belief function over Θ ,for some basic probability assignment m :2^{Θ} [0;1]

$$Bel(A) = \sum_{B \subseteq A} m(B)$$

for all A belonging to 2^{Θ}, Bel(A) describes a measure of the total beliefs committed to the evidence A.[6]
for all nonempty C belongs to Θ, m(C) is a basic probability assignment which describes the combined evidence.
The importance factors of the combination result equals to $(IF_1 + IF_2)/2$.

D. DRCIF

Suppose Bel_1 and Bel_2 are belief functions over the same frame of discernment Θ, with basic probability assignments m1 and m2. The importance factors of these evidences are IF_1 and IF_2. Then, the function
m' :2^{Θ} [0;1] defined by
$m(\Phi)=0$ and
m`(C,IF1,IF2)

$$= \frac{\sum Ai \cap Bj = c \left[m1(Ai)^{\frac{IF1}{IF2}}, m2(Bj)^{\frac{IF1}{IF2}} \right]}{\sum C \subseteq \theta, C \neq \phi \ \sum Ai \cap Bj = c \left[m1(Ai)^{\frac{IF1}{IF2}}, m2(Bj)^{\frac{IF1}{IF2}} \right]}$$

for all nonempty C belonging to Θ, m' is a basic probability assignment for the combined evidence.

E. Extended D-R Theory

Extended D-S evidence model with importance factors: Suppose $E_1=\{m_1;IF_1\}$ and $E_2=\{m_2;IF_2\}$ are twoindependent evidences. Then, the combination of E_1 and E_2 is
E = { m1⊕; $(IF_1 + IF_2)/2$ }whereis DR⊕F.

Our proposed DRCIF is non-associative for multiple evidences. The complexity of our algorithm is O(n), where n is the number of evidences. It indicates that our extended Dempster-Shafer theory demands no extra computational cost compared to a naıve fuzzy-based method.

IV. RISK-AWARE RESPONCE

Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. We perform risk assessment with the extended D-S evidence theory introduced in Section 3 for both attacks and corresponding countermeasures to make more accurate response decisions.

Each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships. Our risk- aware response mechanism is divided into the following four steps shown in Fig. 2.

Evidencecollection. 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.

*Risk Assessment.*Alertconfidence fromIDSandthe 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.

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.

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

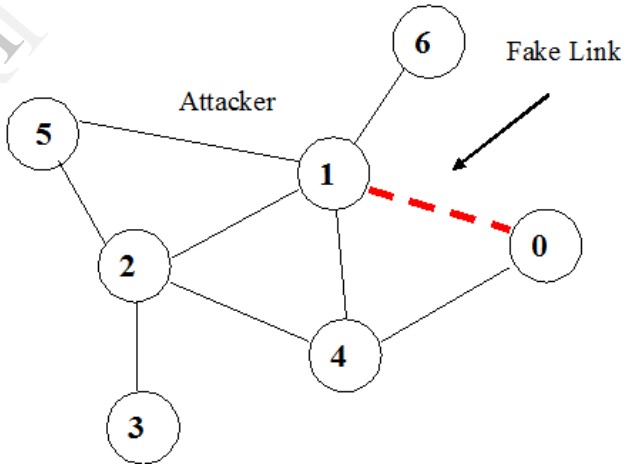


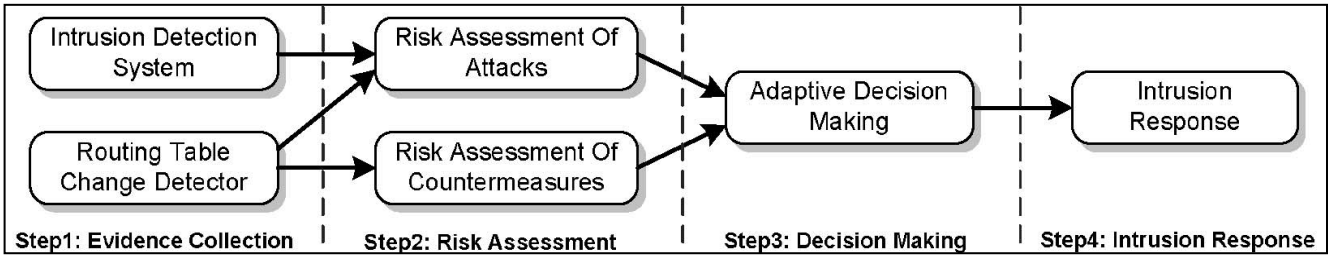
Fig.2MANET Scenario

A. Response to Routing Attacks

As can be seen in Fig. 2, Node 1 behaves like a malicious node. However, if every other node simply isolates Node 1, Node 6 will be disconnected from the network. Therefore, more flexible and fine-grained node isolation mechanisms are required. In our risk-aware response mechanism, we adopt two types of time wise isolation responses:
Temporary isolation and permanent isolation.

B. Risk Assessment

It may so happen that the attack response actions may cause more damages than attacks, hence the risks of both attack and response should be estimated. We classify the security states of MANET into two categories:
{Secure, Insecure}.
Fig 3. Risk Aware response



Bel(Insecure) is used to represent the risk of MANET.

We take the confidence level of alerts from IDS as the subjective knowledge in Evidence 1. In terms of objective Evidence, we analyze different routing table modification cases.

Evidence 1: Alert confidence. The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence.

m(Insecure) = c; c is confidence given by IDS

Evidence 2: Modified Entry. This evidence tells us if the message field has been tampered with in any way.

C. Adaptive Decision Making

Our adaptive decision-making module is based on Quantitative risk estimation and risk tolerance. Each band is associated with an isolation degree, which presents a different time period of the isolation action. The response action and band boundaries are all determined in accordance with risk tolerance and can be changed when risk tolerance threshold changes. The upper risk tolerance threshold (UT) would be associated with permanent isolation response. The lower risk tolerance threshold (LT) would remain each node intact. The band between the upper tolerance threshold and lower tolerance threshold is associated with the temporary isolation response, in which the isolation time (T) changes dynamically based on the different response level where n is the number of bands and i is the corresponding isolation band.

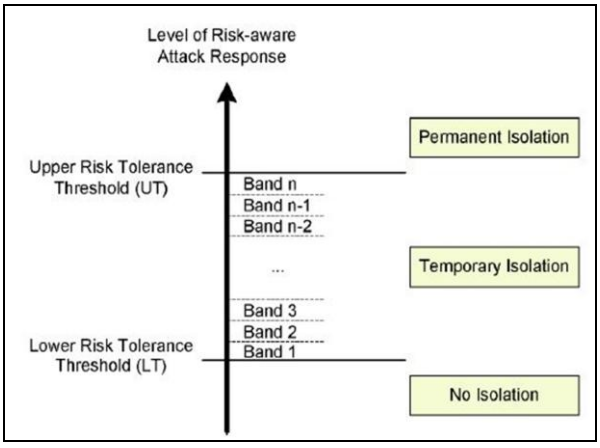


Fig 4. Adaptive Decision Making

Depending on range in which the risk value lies we can choose type of isolation and period of isolation. The time period for isolation can be calculated by given formula[7]

$$i=\left[\frac{Risk-LT}{UT-LT}\times n\right],\ \text{Risk} \in (LT,UT)$$

T = 100 * i (milliseconds)

V. CONCLUSION

We have proposed a risk-aware response solution for mitigating MANET routing attacks .Especially, our approach considered the potential damages of attacks and counter-measures. Based on the promising results obtained through these applications, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

REFERENCES

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

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

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks,vol. 1, nos. 2/3, pp. 293-315, 2003.

[4] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM Mobi Com,pp. 255-265, 2000.

[5] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, vol. 3, pp. 1976-1986, 2004.

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

[7] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu, "Risk-Aware Mitigation for MANET Routing Attacks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012.

[8] Agrawal, Sanjeev Jain, Sanjeev Sharma, January 2011, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of Computing, Volume 3, Issue 1, 41-48.