American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-02, pp-14-20
www.ajer.us

Research Paper Open Access

Prevention of Routing Attacks In Manet

N.Rajesh[1], M.Selvi[2],
PG Scholar[1], Associate Professor/ECE[2]
Saveetha Engineering College, Chennai, Tamilnadu, India,

***Abstract**:* Mobile Ad hoc Networks (MANET) are easily prone to attacks due to its network infrastructure. In previous routing attacks the malicious node is isolated using naive fuzzy response decisions. In this paper a new technology of broadcasting the awareness information about attacker node to all the existing nodes in the network is discussed. The awareness approach is based on an extended Dempster-Shafer mathematical theory (D-S Theory). Dempster-Shafer mathematical theory is used to collect the evidence notion of importance factors. The adaptiveness of the mechanism allows to systematically cope with the identified MANET routing attacks. The intrusion response action in MANET was addressed by isolating uncooperative nodes based on the node reputation derived from their behaviors. Here the effectiveness of the approach with the consideration of the packet delivery ratio and routing cost were demonstrated using java swing concepts.

***Keywords**: Mobile Ad hoc Networks, dempster-shafer theory, intrusion response actions, awareness information, intrusion dection system.*

I. INTRODUCTION

Mobile ad hoc networks (MANET) are a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate where as other nodes need the aid of intermediate nodes to route their packets. These networks are fully distributed and can work at any place without the help of any infrastructure. Another unique characteristic of the communication terminals in MANET is the dynamic nature of its network topology which makes frequent changes due to mobility of nodes. Furthermore every node in MANET plays two important role that are routing and data transmission over the network. The performance of ad hoc network depend on co-operation and trusted among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other node without centralized authorizes. The intrusion response action in MANET by isolating uncooperative nodes based on the behavior of node reputation. The simple response of the attacker nodes often neglects possible negative side effects involved with the response action [1], [2]. Improper countermeasure 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. The notation of the risk assessment support adaptive response to routing attacks. Risk assessment is a challenging problem due to its involvement of subjective knowledge, objective evidence and logical reasoning [3].

Routing attacks against MANET can be classified into passive or active attacks. Attacks can be further categorized as either outsider or insider attacks. With respect to the target, attacks could be also divided into data packet or routing packet attacks. In routing packet attacks, attacker could not only prevent existing path from being used, but also spoof non-existing paths to lure data packets to them. Several studies have been carried out on modeling MANET routing attacks [4]. Different routing attacks are black hole, fabrication, and modification of various field in routing packets (route request message, route reply message, route error message, etc.). All these attacks could lead to serious network dysfunctions.

II. SYSTEM ARCHITECTURE

A. Dempster's rule of combination algorithm

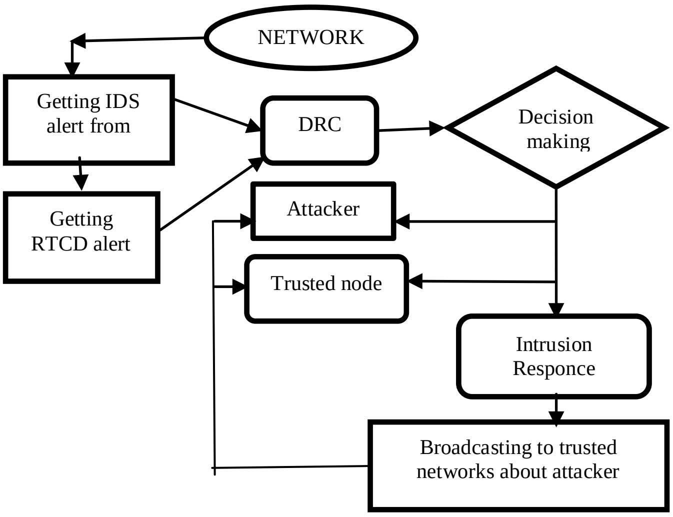


Fig. 1 System Architecture

A network is created with number of nodes and every node send some packets by using dynamic path routing. At that time attacker will get interrupted in the network and it will cause an attack. The attack can be identified from the routing table update report. Due to this attack an alert is given and routing table changes detector report is formed. To know about trusted and untrusted node DRC is applied and message is broadcasted to other nodes. System architecture fig. 1 represent trusted and untrusted node based on DRC and RTCD.

B. Network Creation

The network consists of wireless ad-hoc network. A wireless ad-hoc network is developed using various mobile nodes and then a shortest path is found between the source and destination using Optimized Link State Routing (OLSR) protocol. Every node is initialized using unique ID, port address, port no and its location information.

C. Network Dysfunction

The attacker optimizes like a node and joins the network and it cause additional damage to the network. The attacker node generated the new path for sending message from one place to another as shown in fig. 2. Network dysfunction shows that the sender send packets to malicious node, that data may be hacked or decrypted by malicious node. Thus the network encounters damage with the help of Intrusion Detection System (IDS) the network monitor know about the attacker by getting alert message.

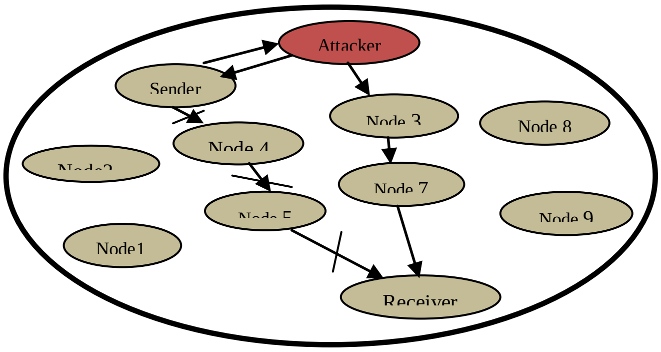


Fig. 2 Network Dysfunction

III. DEMPSTER- SHAFER THEORY

D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems [5]. D-S theory has several characteristic. The first characteristic in D-S theory that enables represents of both subjective and objective evidence with basic probability assignment and belief function. The second characteristic supports Dempster's Rule of Combination (DRC) to combine several evidence together with probable reasoning [6], [7]. An awareness approach is based on an extended Dempster-Shafer (DS) mathematical theory of evidence introducing a notion of importance factor [8].

The behavior of attacker against MANET can be classified into passive or active attacks. Attacks can be further categorized as either outside or inside attacks. With respect to the target, attacks could be also divided into data packet or routing packet attacks. In routing packet attacks, attacker could not only prevent existing paths from being used, but also spoof non-existing paths to lure data packets from attacks [9]. Typical routing attacks include black-hole, fabrication, and modification of various fields in routing packets (route request message, route reply message, route error message, etc.)

Response to routing attacks

Two different response to deal with different attack methods that is routing table recovery and node isolation. Routing table recovery includes local routing table recovery and global routing 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 message by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET. Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In proactive routing protocols like Optimized Link State Routing (OLSR), routing table recovery does not bring any additional overhead since it periodically goes with routing control messages.

Node isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in MANET. To perform node isolation response, the neighbors of the malicious node ignore the malicious node by neither forwarding packet through it nor accepting any packet from it. On the other hand, binary node isolation response may result in negative impacts to the routing operations, even bringing more routing damages than the attack itself. In the above risk-aware response mechanism, it adopt two types of node isolation response, a temporary isolation and a permanent isolation.

IV. DEMPSTER-SHAFER THEORY OF EVIDENCE

The mathematical theory of dempster shafer is both a theory of evidence and a theory of probable reasoning and Dempster's rule combination is the procedure to aggregate and summarize a corpus of evidences which identify several limitations of the Dempster's Rule Combination (DRC). 1. Associative DRC, the order of the information in the aggregated evidences does not impact the result [10], 2. Non weighted DRC implies that we trust all evidences equally.

D. Importance Factors:

In D-S theory, propositions are represented as subsets of a given set. Suppose ɵ . is a finite set of states, and let $2^{ɵ}$ denote the set of all subsets of ɵ . D-S theory calls ɵ , a frame of discernment.

Definition 1.

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

Definition 2.

An evidence E is a 2-tuple (m,IF), where m describes the basic probability assignment [10]. Basic probability assignment function m is defined as follows:

$$M(ɵ) = 0 \quad \text{--------------------------------}(1)$$

And

$$\sum_{A \leq ɵ} M(A) = 1 \quad \text{---------------------------------}(2)$$

According to [5], a function Bel:$2^{ɵ}$ →[0,1] is a belief function over ɵ if it is given by (3) for some basic probability assignment m : $2^{ɵ}$ →[0,1]

$$Bel(A) = \sum_{B \leq A} B(m)=1 \quad \text{------------------------}(3)$$

Where A€$2^{ɵ}$, Bel(A) describes a measure of the total beliefs committed to the evidence A. Given several belief functions over the same frame of discernment and based on distinct bodies of evidence, Dempster's rule of combination, which is given by (4), enables us to compute the orthogonal sum, which describes the combined evidence. Suppose Bel_1 and Bel_2 are belief functions over the same frame ɵ , with basic probability assignments m1 and m2. Then, the function m : $2^{ɵ}$ →[0,1] defined by M(ɵ) = 0 and

$$M(C) = \frac{\sum A_i \cap B_j = C m_1(A_i) m_2(B_j)}{1 - \sum A_i \cap B_j = \varphi m_1(A_i) m_2(B_j)} \quad \text{---------(4)}$$

where nonempty C≤ɵ , m(C) is a basic probability assignment which describes the combined evidence. Suppose IF_1 and IF_2 are importance factors of two independent evidences named E_1 and E_2, respectively. The combination of these two evidences implies that our total belief to these two evidences is less than 1. This is straightforward since if our belief to one evidence is 1, it would mean our belief to the other is 0, which models meaningless evidence. And we define the importance factors of the combination result equals to $(IF_1 + IF_2)/2$.

Definition 3.

Extended D-S evidence model with importance factors: Suppose $E_1 = (m_1, IF_1)$ and $E2 = (m_2, IF_2)$ are two independent evidences. Then, the combination of E_1 and E_2 is $E = (m1 \oplus m2 ,(IF_1 + IF_2) = 2)$, where $\oplus$ is Dempster's rule of combination with importance factors.

E. RISK-AWARE RESPONSE MECHANISM:

Risk tolerance and risk estimation are done by adaptive risk-aware response mechanism. The isolation from the attacking node done by temporal manner based on the risk value [11], [12]. The risk assessment with the extended D-S evidence theory introduced both attacks and corresponding countermeasures to make more accurate response decisions. A risk-aware response system is distributed, which means 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 in fig. 3.

Evidence collection.:

In this 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:

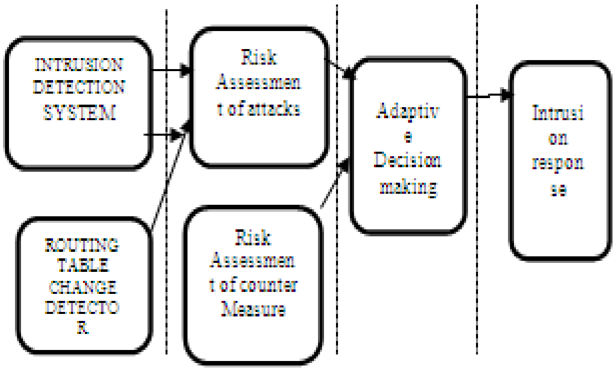
Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the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

Decision making:

The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account.

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.


INTRUSION DETECTION SYSTEM
ROUTING TABLE CHANGE DETECTO R
Risk Assessmen t of attacks
Risk Assessmen t of counter Measure
Adaptiv e Decision making
Intrusi on respon se

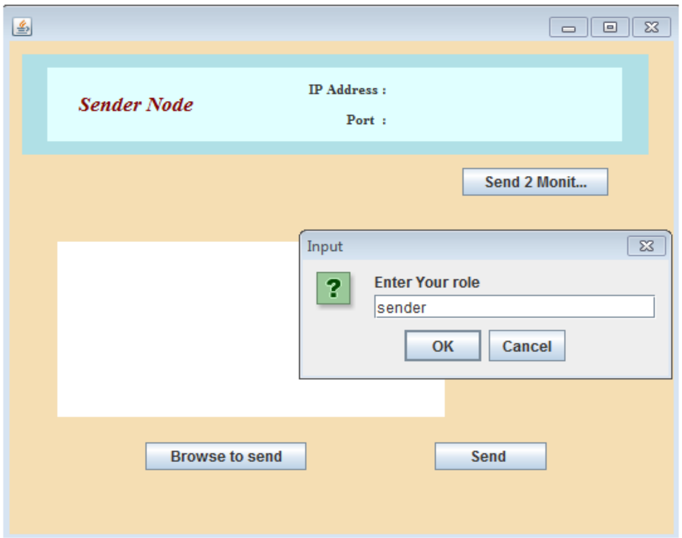
Evidence Risk Decision Intrusion collection Assessment Making response

Fig no: 3 Dempster`s rule Combination Algorithm

V. RESULTS AND DISCUSSION

F. Sender node creation

Here sensor nodes are created using java swing concepts, java Swing is the primary Java Graphical User Interface (GUI) which is the part of Java Foundation Classes (JFC) that provides GUI in Java programs. To implement swing concept netbeans development tool is used. The created sender node is shown in fig. 4 which shows the IP address and PORT number when the user enters the name and clicks ok.



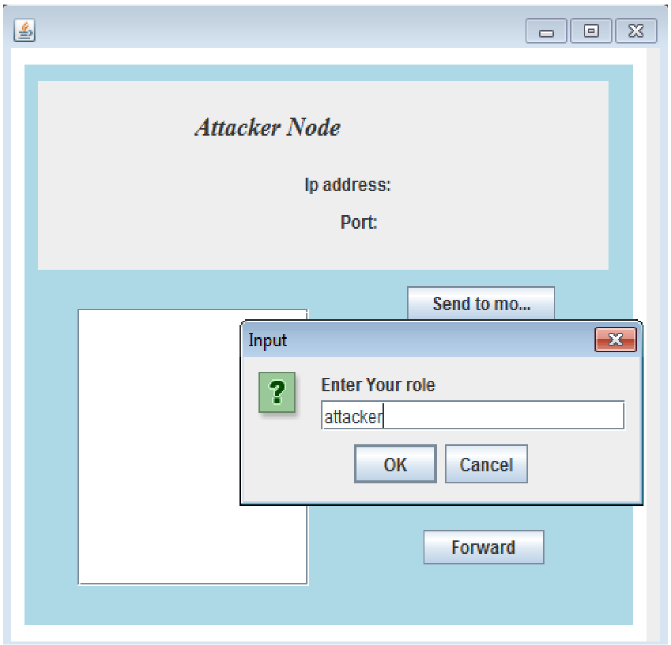
Enter Your role

sender

Fig. 4 Creating a sender node

G. Attacker creation

Similar to the sender node the attacker node is created using label textbox and buttons. Which is shown in fig. 5.



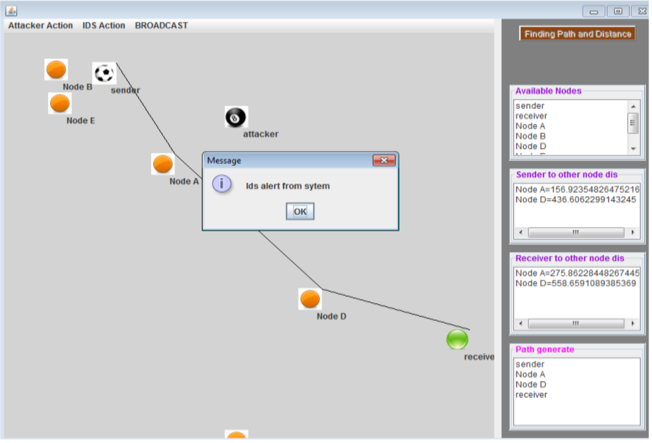
Enter Your role

attacker

Fig. 5 Attacker node creation

H. Network Dysfunction

fig 6 shows the attacker node is entered and it will change neighbor node routing table. When it was known to the neighbor node it will broadcast the alert message to all the nodes.



Ids alert from sytem

Available Nodes

sender
receiver
Node A
Node B
Node D

Sender to other node dis

Node A=156.92354826475216
Node D=436.6062299143245

Receiver to other node dis

Node A=275.86228448267445
Node D=558.6591089385369

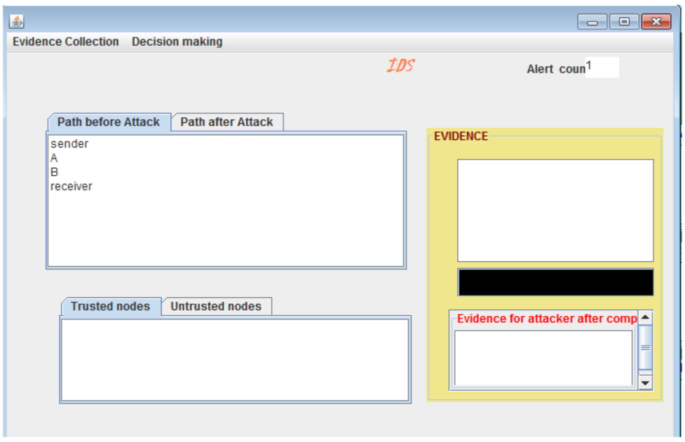
Path generate

sender
Node A
Node D
receiver

Fig. 6 Network Dysfunction

I. Evidence collection

Evidence selection approach consider subjective evidence from experts' knowledge and objective evidence from routing table modification. A unified analysis approach for evaluating the risks of both attacks as shown in fig.7.



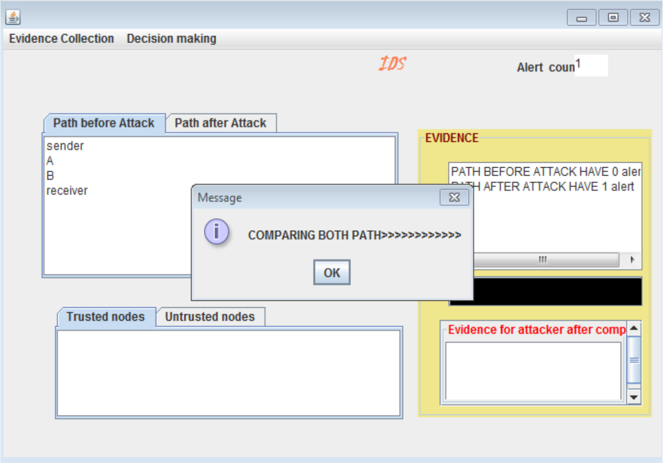
Alert coun 1

sender
A
B
receiver

Fig. 7 Evidence Collection

J. Decision making

Decision making is evolvated based on evidence collection. evidence collection has two field path before attack and path after attack, based on the comparison of two pats decision making is done for trusted and untrusted nodes fig 8 represents decision making.



Alert coun 1

sender
A
B
receiver

COMPARING BOTH PATH>>>>>>>>>>>>

PATH BEFORE ATTACK HAVE 0 aler
PATH AFTER ATTACK HAVE 1 alert

Fig. 8 Decision Making

VI. CONCLUSION

In this paper malicious node in the MANET network is detected and isolated using DUMPSTER-SHAFER mathematical theory. It broadcast alert message about the malicious node to all the nodes in the network so that all the nodes in the network will be aware of malicious node. And, hence it provides maximum security and trust worthiness in MANET routing.

REFERENCES

[1] Y. Sun, W. Yu, Z. Han, and K. Liu, "Information Theoretic Framework of Trust Modeling 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. Computers, vol. 59, no. 5, pp. 707-719, May 2010.

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

[4] 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.

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

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

[7] C. 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), p. 35-48, 2008.

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

[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. *IEEE* Wireless Communications, page 86, 2007.

[10] R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987

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

[12] M. Yamada and M. Kudo, "Combination of Weak Evidences by D-S Theory for Person Recognition," Knowledge-Based Intelligent Information and Engineering Systems, pp. 1065-1071, Springer, 2004.