Secure Network Discovery for Risk-Aware Framework in Manet

Miss. Poornima N, Mrs. Sridevi K. N
CNE, Dept. of CSE CMRIT –Bangalore, India
Assoc. Professor, Dept of CSECMRIT -Bangalore, India

Abstract*: Mobile Ad-Hoc Networks (MANETS) are dynamic in nature. Because of its dynamic nature of its network infrastructure, MANETS are highly vulnerable to attacks. Among these attacks routing attack has considerable attention, since it could cause most destructive damage to MANET. In existing system, binary isolation and DRC techniques are used to isolate the malicious nodes. However, binary isolation leads to unexpected network portioning and DRC is associative and non-weighted. In this paper we proposed adaptive risk-aware response mechanism with an extended trusted center, where a risk-aware approach which is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. Adaptive decision making technique has been used to prevent routing attacks. We also analyses and evaluate routing cost with respect to different technique.*

Keywords- *MANETS, risk-aware, trusted centre, DS theory, adaptive decision.*

Submitted date 17 June 2013 **Accepted Date: 22 June 2013**

I. Introduction

A MANET (Mobile Adhoc Network) is collection of independent mobile devices which can communicate by wireless links without any predefined fixed infrastructure or centralized access point. The mobile nodes /devices can communicate directly which are in the radio range via radio waves, where as other nodes have to use of intermediate nodes using routing path to route their packets to destination. Another unique characteristic of MANET is dynamic nature of network infrastructure. MANETS are highly vulnerable to various kinds of security attacks. In those attacks, we are consider worm hole attack[1] as major issue, since it form a serious threat in wireless network, especially against adhoc network of routing protocols. Worm attack causes an attacker to record to packets in one location and transmit them to another location and again retransmit them there into the network, since it launched in hidden mode. MANETS can be divided to two categories: proactive routing protocols and reactive routing protocols. In this paper we are considering proactive routing protocol such as OLSR [2], which needs more bandwidth and energy resources, and it doesn't support multicast and security. In order to mitigate this attack and to provide security many solutions [3] are introduced which are typically attempt to isolate malicious nodes using binary or naïve fuzzy response decisions. And also address [4], [5] the intrusion response actions by isolating the uncooperative nodes which is based on node reputation derived from their behavior in MANET. The solutions which have been introduced causes unexpected network partition and uncertainty in countering routing attacks in MANET. We can adopt a notion of risk to support adaptive responses to routing attacks. However the notion of risk involves the concept of subjective knowledge which could be retrieved from previous experience, objective evidence obtained from observation and logical reasoning requires formal foundation. D-S theory depends on the above concept and it has a characteristic which support Dempster's Rule of Combination technique [6] which is based on D-S theory is used to combine several evidences together with probable reasoning. However DRC has limitations, such as they are associative and non-weighted i.e. they treat all evidences equally without differentiating each evidence and considering priorities among them.

In this paper, we propose a adaptive risk-aware response mechanism with an extended trusted centre, where a risk aware approach is based on an extended D-S mathematical theory of evidence introducing a notion of importance factors. An adaptive decision making technique has been used to prevent/mitigate routing attacks. We also analyses evaluate routing cost with respect to different technique.

II. Existing System

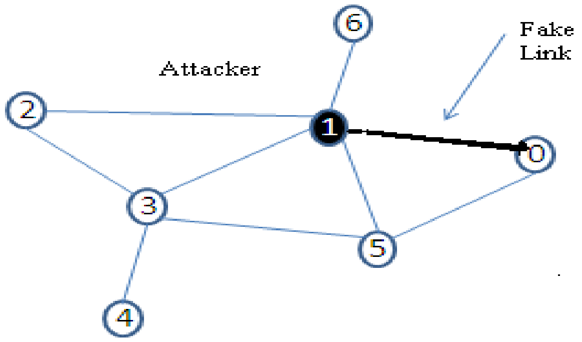


Fig.2.1 Example scenario.

Fig 2.1 shows an example scenario where nodes 2 to 0 are supposed to go through Nodes 3 and 5. Suppose a malicious node 1 advertises a fake link to node 0 and it would also cause all other nodes to update its routing table accordingly. As a result the data from Nodes 2 to 0 traverse Node 1 rather than nodes 2 and 4 and Node 1 can manipulate and drop the traffic between Nodes 2 to 0.

In Existing system, binary solution or naïve fuzzy response decision technique has been used to isolate to malicious nodes. However these techniques has limitations, where binary responses may result in the unexpected network partition, causing damages to the network infrastructure and naïve fuzzy response could lead to uncertainty in countering routing attacks. To overcome this problem notion of risk can be adopted to support adaptive responses to routing attacks. However the notion of risk involves the concept of subjective knowledge which could be retrieved from previous experience, objective evidence obtained from observation and logical reasoning requires formal foundation. D-S theory depends on the above concept and it has two characteristic i.e. it enables to represent both subjective and objective evidences with basic probability assignment and belief function and it also supports Dempster's Rule of Combination technique [6] which is based on D-S theory is used to combine several evidences together with probable reasoning. However DRC has limitations, such as they are associative and non-weighted i.e. they treat all evidences equally without differentiating each evidences and considering priorities among them.

III. Proposed System

3.1 Adaptive Risk-aware response mechanism with an extended trusted center

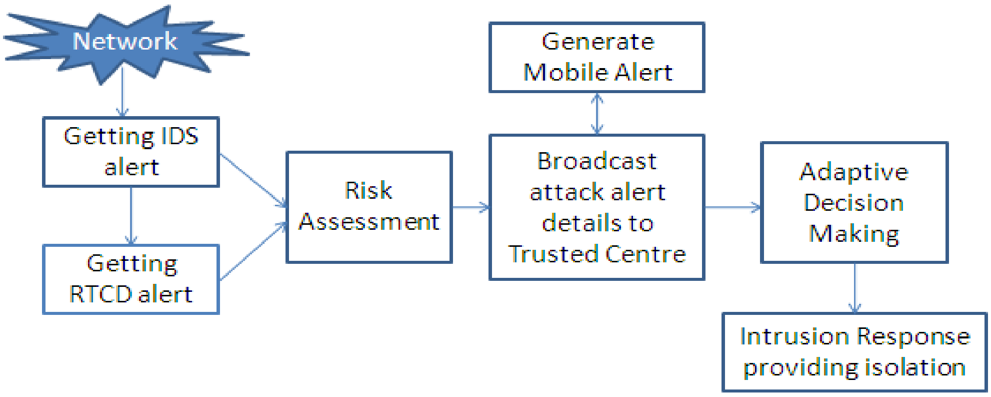


Fig. 3.1 System Architecture

A network is created with 'n' number of nodes and one node will act as sender and another node will act as a destination. Every node will sends some packets by using dynamic path routing. At that time network can interrupt by some attacker and it will cause an attack. The routing table updated report gives the details about attacker. A greedy technique is applied on a network to form different routing paths.

System architecture defines the structure, behavior and more views of a system. A service provider/sender in the network sends the data requested by end user/destination. When a network is interrupted by some attacker, it will cause an attack. An attack can be identified by evidence collection and risk assessment. Evidence collection gives an IDS (Intrusion Detection System) alert and Routing Table Change

Detector(RTCD) alert. Both these two alerts have been considered as two independent evidences for risk calculation and combined with extended D-S theory [6]. This combining multiple evidences to single evidence technique is called as DRC (Dempster's Rule of Combination) with some importance factors. DRCIF gives the attack alert. The trusted center/node which monitors the network, it should check the default routing table. If any changes occur in the routing table by getting an attack alert, trusted center has to provide attacker details and it should generate mobile alert. ADM (Adaptive Decision Making) technique is used to provide a flexible response decision-making mechanism which provide routing table recovery and node isolation. Two isolation techniques are provided for routing attacks. Temporary isolation is provided by selecting alternative path and forwards the data to destination after avoiding the fake link and send packets to destination. The permanent isolation technique is applied to change the routing table permanently.

3.2 Evidences Collection

Selection of evidences considers subjective evidences from expert's knowledge and objective evidence from routing table modifications and analysis the approach for evaluating risk of both attacks and countermeasures.

We can consider subjective evidence from confidence level of alerts from IDS in Evidence 1. Objective evidence can be obtain from different routing table modification, such as existing routing table entries to be missed, or any item in routing table entry to be changed. Objective evidence is analyses in evidences 2 and 3.

Evidence 1: Alert confidence gives the confidence of attack detection by the IDS and it provides the possibility of the attack occurrence. The basic probability assignment of evidence 1 is based on below equations:

m (Insecure)=c, c is confidence given by IDS (1)

m (Secure)=1 (2)

m (Secure,Insecure)=0 (3)

Evidence 2: Missing entry evidence indicates the proportion of missing entries in the routing table.

Evidence 3: Changing entry evidence shows the proportion of changing entries in the case of next hop being the malicious node.

IV. Risk Assesment

In risk assessment phase, alert confidence from IDS and RTDC would be considered as different evidences and these two evidences combined using DCRIF algorithm. It provides entire risk of attack. Security state of MANET can be classified into two categories. {Secure, Insecure} which means security state of MANET could be either secure or insecure. Risk of MANET could be represent by belief function Bel{Insecure}.

V. Dempster's Rule of Combination with some importance factor algorithm

Input: Evidence pool E_p

Output: One evidence which gives attack alert

Varibles: Evidence pool 'E_p', basic probability assignment 'm', basic probability assignment function 'IF' (Importance Factor).

```
1. $|E_p|$ = sizeof($E_p$);
2. While $|E_p|>1$ do
3. Pick two evidences with the least IF in Ep named $E_1$ and $E_2$;
4. Combine these two evidences,
   $E= ( m_1 \oplus m_2, (IF_1 + IF_2)/2)$;
5. Remove $E_1$ and $E_2$ from $E_p$;
6. Add E to $E_p$;
7. End
8. Return the evidence in $E_p$
```

VI. Trusted Center

Trusted Center provides attacker details to service provider whenever attack alert is generated and also generates mobile alert on mobile devices. Suppose if user is out of station whenever attacker attacks original data files an alert message has been provided to registered person through mobile devices.

VII. Adaptive Decision Making (Adm)

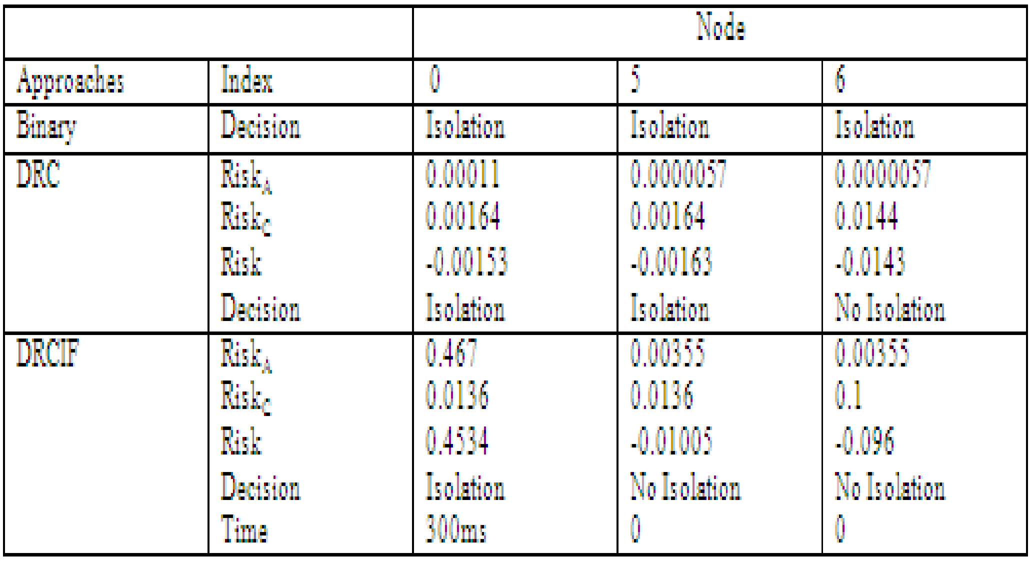
ADM (Adaptive Decision Making) technique is used to provide a flexible response decision-making mechanism when it gets attack alert. The implementation of ADM has been shown when an intruder causes an attack after the connection establishment.

```
If ServerSocket server1=new ServerSocket(10000);
Socket Con;
While(true)
{
Con= server1.accept();
Print a message to establish a connection.
}
If connection is established
Retrieve the details of source node, dest. And attacker.
Query=”select *from Routing Table where SNode=”+s+”andDest=”+d+”andAttacker=”+attack+” “;
ResultSet rs= stmt.executeQuery(query);
If(rs.next()== true)
{
Indicate the attacker by fake link.
Generate a message Attacker found in network!!
Do  you want to apply temp. Isolation to
destination.
}
```

VIII. Results And Evaluation

The results of proposed technique mainly focused on routing cost, which provides the ratio between the total bytes of packets received by the Constant Bit rate sink at the final destination.

In order to evaluate our mechanism we divided process into three stages, such as Before attack, After attack and After response. We are going to carried this process to all three technique and comparing all routing cost with respect three techniques. Before Attack- Random packets are generated and transmitted among the nodes without activating any of the node as attacker. After Attack- Specific nodes are set as attacker and those attackers which can conduct malicious activities for their profit After Response- For each node response decisions were carried out based on three different techniques.



		Node		
Approaches	Index	0	5	6
Binary	Decision	Isolation	Isolation	Isolation
DRC	$Risk_A$	0.00011	0.0000057	0.0000057
	$Risk_C$	0.00164	0.00164	0.0144
	Risk	-0.00153	-0.00163	-0.0143
	Decision	Isolation	Isolation	No Isolation
DRCIF	$Risk_A$	0.467	0.00355	0.00355
	$Risk_C$	0.0136	0.0136	0.1
	Risk	0.4534	-0.01005	-0.096
	Decision	Isolation	No Isolation	No Isolation
	Time	300ms	0	0

Table 8.1: Risk Assessment and Adaptive Decision making.

The risk assessment and Decision making for various mechanism can be shown in below table considering three nodes 0, 5 , 6 as shown in fig. 2.1.

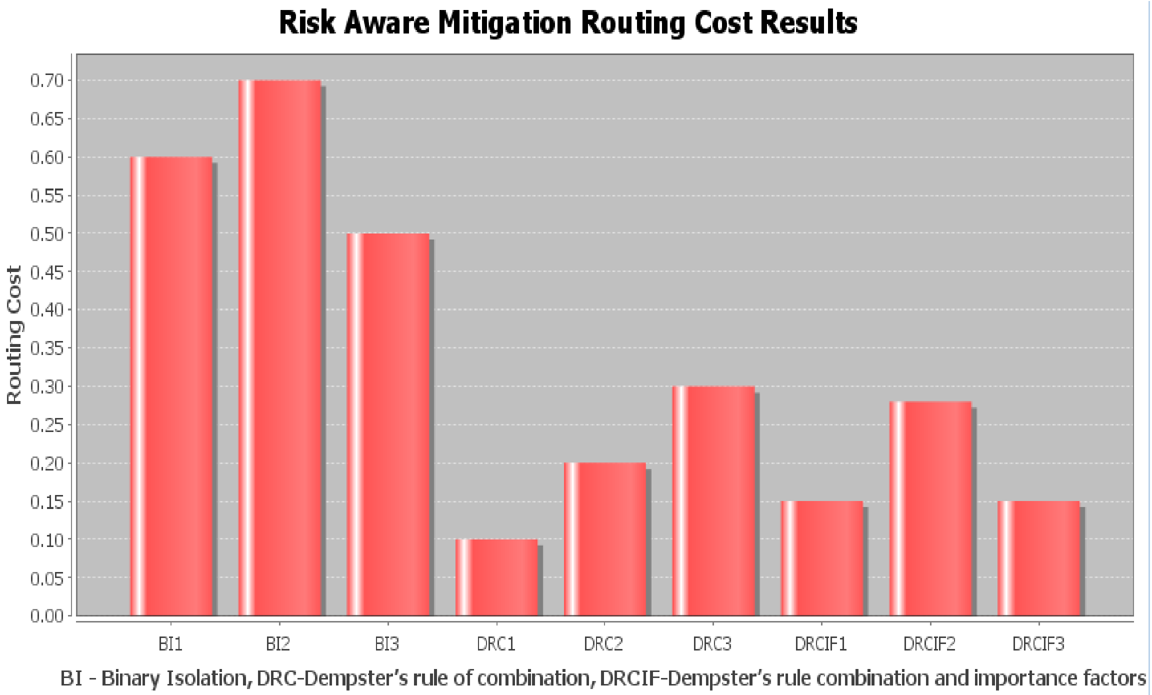


Fig 8.2: Routing Cost

Fig 3.1 represents routing cost with respect to three different mechanisms. Routing cost increases as routing attacks increases. In the above graph routing cost increases in first two mechanism binary isolation and in DRC. Compared to Binary isolation, DRC mechanism routing cost decreases using third mechanism DRCIF and DRCIF handles the routing attack effectively.

IX. Conclusion

We have proposed a adaptive risk-aware mechanism with extended trusted center which reduces the MANET routing attacks. Risk – aware approach is based on D-S theory with importance factors. Trusted center provide Mobile alert for attacked file for mobile devices if user is out of station. Finally provides temporary and permanent isolation by ADM. And, hence it provides maximum trust worthiness and more security in MANET routing

Acknowledgment

The work has been supported by the grants from the US Department of Energy (DEO) (DESC0004308) and the US National Science Foundation (NSF-IIS-0900970 and NSF-CNS-0831360).

REFERENCES

[1] Nabendu Chaki , Reshmi Maulik, “A study on WORMWHOLE Attacks in MANET,” IJCISIM, Volume 3 (2011) pp. 271-279.

[2] M. Mohana Priya, K. Urmila Vidhya, “A Novel Technique for mitigating routing Attacks in OLSR MANET,” IEEE ICIC-2010.

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

[4] W. Yu, Y. Sun, K. Liu , and Z. Han, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks,” IEEE J. Selected Areas in Communication, vol. 24, no. 2, pp. 305-317, Feb. 2006.

[5] L. DaSilva, M. Refaei, M. Eltoweissy, and T. Nadeem, “Adaptation of Reputation Management Systems to Dynamic Network Conditions in Adhoc Networks,” IEEE Transactions Computers, vol. 59, no. 5, pp. 707-
719, May 2010.

[6] Gail-Joon Ahn, Ziming Zhao, “Risk-Aware Mitigation for MANET Routing Attacks,” IEEE Transactions on Dependable and Secure Computing, Vol 9, No. 2, March/April 2012.

[7] Sudhir Agrawal, Sanjeev Sharma, Sanjeev Jain, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks,” Jornal of computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617.

[8] T.J. Giuli, Sergio Marti, Mary Baker, Kevin Lai, “Defending Routing Misbehavior in Mobile Ad Hoc Networks,” Dept. of CSE, Stanford University, Stanford, CA 94305 U.S.A.