International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-3 Issue-3, February 2014

Mean Probabilistic Approach for Risk Estimation in MANET

Dakshayani. G, Amol P Pande

Abstract: ***Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. MANET has the dynamic infrastructure hence it is highly vulnerable to attacks. Several attacks are possible in MANET networks and among them routing attack could cause the worst damage. There are several solutions available for mitigating the routing attacks based on the intrusion response techniques but most of them isolate the malicious node only based on the binary decisions taken for severity in attacks. This will cause additional damage to the network. Risk mitigating techniques is one of the important factor in MANET environment. This paper is about exchange of data between the various nodes in a MANET in a secure manner. we have designed an approach for fusing the evidences so that risk can be assessed effectively and decision of whether an attacker node has to isolated or not. Since always isolation of attacker could result in more serious damages. Therefore our approach isolates only the fake links established by the attacker, unless the attacker is causing more devastating damages.***

Keywords: - MANET, Routing attacks, routing protocols, Evidence, Risk.

I. INTRODUCTION

Recently laptop computers have replaced desktops with all respect as they continue to show improvements in convenience, mobility, capacity and availability of disk storage. Now small computers can be equipped with storage capacity of Gigabytes, high resolution color display, pointing devices and wireless communication adapters. Since, these small computer can be operated with the power of battery, the user are free to move as per their convenience without bothering about constraints with respect to wired devices.

In wireless ad-hoc network, the devices communicate with each other using a wireless physical medium without relying on pre-existing wired infrastructure. That is the reason why ad-hoc network is also known as infrastructure less network. These networks are also known as mobile ad-hoc networks (MANETs), can form stand-alone groups of wireless terminals, but some of these may be connected to some fixed network. A very fundamental characteristic of ad-hoc networks is that they are able to configure themselves on-the-fly without intervention of a centralized administration. The terminals in the ad-hoc network cannot only act as end-system but also as an intermediate system such as routers. It is possible for two nodes which are not in the communication range of each other, but still can send and receive data from each other with the help of intermediate nodes which can act as routers.

Manuscript published on 28 February 2014.
***** Correspondence Author (s)
Mrs. Dakshayani.G, Assistant Professor, Fr.C.R.I.T, Vashi, India.
Mr.Amol P Pande, HOD Comp Dept, Assistant Professor, Datta Meghe College of engineering, India.

This functionality gives another name to ad-hoc network as "multi-hop wireless network".Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in environments without a predefined infrastructure. MANET has been normally deployed in adverse and hostile environments where central authority is not present. MANET is characterized of dynamic nature for its network topology which would be frequently changed due to the unpredictable mobility of mobile nodes. Further, each mobile node in MANET acts as a router while transmitting data over the network. Hence, any compromised nodes under the control of malicious node could cause significant damage to the functionality and security of its network .Several work addressed the intrusion response actions in MANET one of the approach called binary approach isolates uncooperative nodes based on the node reputation derived from their behaviours[1]. Such improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure .A simple response against malicious nodes often neglects possible negative side effects involved with the response actions. To address the above mentioned critical issues, more flexible and adaptive response measures should be proposed. Therefore this paper we are concerned about the Security in Mobile Ad-Hoc Network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. We make use of routing tables of the table driven protocol and feedback given by the IDS(intrusion detection system) in finding out the risk caused by the attacker for making suitable decision to mitigate the amount of damage caused by the attacker to the MANET. We collect various evidences such as subjective and objective evidences; subjective evidences are basically expert views or historical facts taken into consideration while objective evidence is built up by comparing the routing tables of the nodes that are participating in the network. We further need to combine all these evidences to reach to a conclusion and finally to make a decision of whether the attacker node needs to be isolated or some other measure can be taken to mitigate the risk involved. In order to evaluate our mechanism, we perform a series of simulated experiments with a proactive MANET routing protocol, Optimized Link State Routing Protocol (OLSR) . In addition, we attempt to demonstrate the effectiveness of our solution.

II. BACKGROUND

In this section, we overview the OLSR routing protocols and routing attacks on OLSR [2].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

A. OLSR Protocol

Proactive MANET protocols (PMPs) constantly update network topology information and ensure that it is available to all nodes. PMPs reduce network latency (or system time delay) but increase data overhead by constantly updating routing information. It ensures routes to all destinations are up-to-date and ready for use when required. Examples: OLSR, DSDV etc.

In proactive, OLSR protocol is a variation of the pure Link-state Routing (LSR) protocol and is designed specifically for MANET. OLSR protocol achieves optimization over LSR through the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. Unlike LSR, where every node declares its links and forward messages for their neighbours, only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

Routing Message in OLSR — generally, in the OLSR protocol, two types of routing messages are used, namely, a HELLO message and a topology control (TC) message. A HELLO message is the message that is used for neighbour sensing and MPR selection. In OLSR, each node generates a HELLO message periodically. A node's HELLO message contains its own address and the list of its one-hop neighbours. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbour nodes and are not forwarded further to other nodes. A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically. A TC message contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network.

MPR Selection — For MPR selection, each node selects a set of its MPR nodes that can forward its routing messages. In OLSR, a node selects its MPR set that can reach all its two-hop neighbours. In case there are multiple choices, the minimum set is selected as an MPR set.

B. Routing Attack on OLSR

Attacks on mobile ad hoc networks can be classified into following two categories:

Passive Attacks: A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. One way of preventing such problems is to use powerful encryption mechanisms.

Active Attacks:-An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network[1]. It can be classified into two categories external attacks and internal attacks.

External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls.

Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.

C. Types of active routing attacks

Flooding attack:-The aim of the flooding attack is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.

Black hole attack:-In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

For example, in Fig. I, source node S wants to send data packets to destination node D and initiates the route discovery process. We assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately sends the response to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 2. As a result, all packets through the malicious node is consumed or lost.

Link with holding attack:

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly serious in the OLSR protocol.

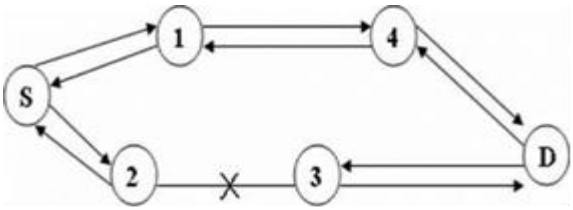

Figure I:-Black hole attack

Wormhole attack:

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

For example in Figure II, X and Y are two malicious nodes that encapsulate data packets and falsified the route lengths.

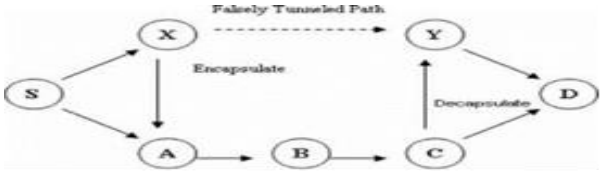

Figure II:- Wormhole attack

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Suppose node S wishes to form a route to D and initiates route discovery. When X receives a route request from S, X encapsulates the route request and tunnels it to Y through an existing data route, in this case {X --> A --> B --> C --> Y}. When Y receives the encapsulated route request for D then it will show that it had only traveled {S --> X --> Y --> D}. Neither X nor Y update the packet header. After route discovery, the destination finds two routes from S of unequal length: one is of 4 and another is of 3. If Y tunnels the route reply back to X, S would falsely consider the path to D via X is better than the path to D via A. Thus, tunnelling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

Replay attack:

In a MANET, topology frequently changes due to node mobility. This means that current net- work topology might not exist in the future. In a replay attack, a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

VI. IDENTIFICATION AND ALLEVIATION OF RISK

In this section, we discuss strategy for identification and alleviation of MANET routing attack Risk. this is carried out in five stages.

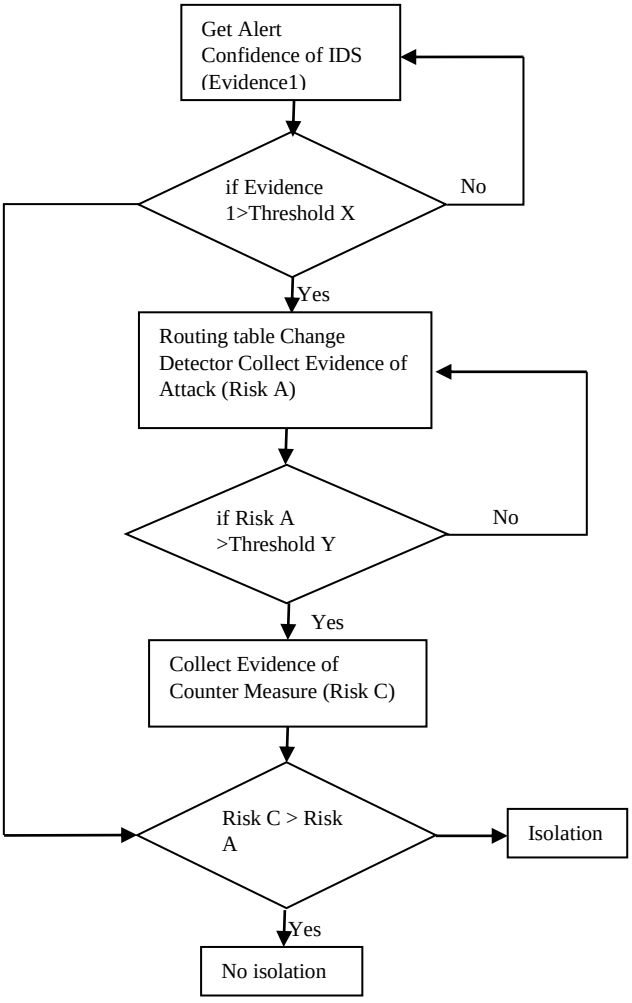

Figure III :Flow of the Approach

AlertConfidence: Here IDS gives attack alert with a confidence message of what percent of damage the attacker may cause to the network. which is treated as the evidence1.

Evidence Collection: In this stage Routing table change detector detects the change in the routing table entries to derive evidences 2 to 6 bas given below.

- Evidence 2: Missing entry. This evidence indicates the proportion of missing entries in routing table.
- Evidence 3: Changing entry I. This evidence represents the proportion of changing entries in the case of next hop being the malicious node. In this case, the malicious node builds a direct link to this node. So, it is highly possible for this node to be the attacker's target.
- Evidence 4: Changing entry II. This evidence shows the proportion of changed entries in the case of different next hop (not the malicious node) and the same distance
- Evidence 5: Changing entry III. This evidence points out the proportion of changing entries in the case of different next hop (not the malicious node) and the different distance.
- Evidence 6: Changing entry IV. This evidence points out the proportion of changing entries in the case of different distance while next hop is same

Risk Analysis: Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the Mean Probabilistic approach. 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: based on the risk analysis phase decision of whether attacker node need to isolated or not will be taken figure IV[1].

Intrusion Response: In this stage after the decision is made routing tables are re-established to suit the existing topology. We use two different responses to deal with different attack methods: routing table recovery and node isolation

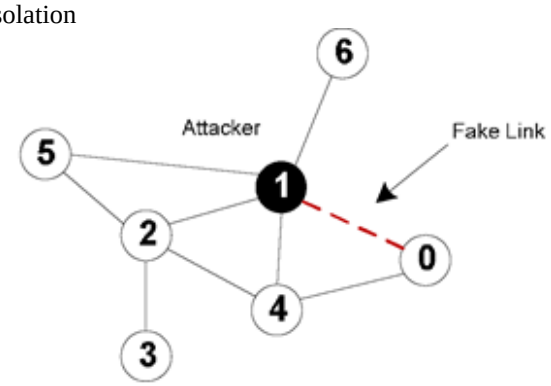

Figure IV: Example scenario

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

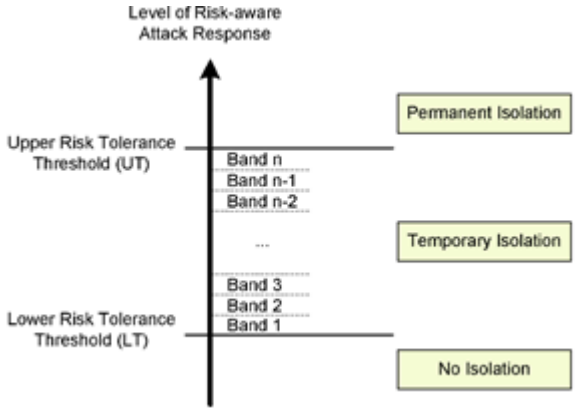

Figure V : Adaptive decision making

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 messages 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 OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

Node isolation may be 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 any packets from it. On the other hand, a binary node isolation response may result in negative impacts to the routing operations, even bringing more routing damages than the attack itself.

V.IMPLEMENTATION

The experiment is carried out using ns2 as a simulation tool with UM-OLSR. NS2 is a discrete event network simulator which provides a detailed model of physical and link layer behavior of a wireless network and allows arbitrary movement of nodes within the network. UM-OLSR is an implementation of optimized link state routing protocol for NS-2, which compiles and supports all core functionalities of OLSR plus the link layer feedback option. In our experiments, we constructed MANET scenarios in a topology of 1000 m ẋ 1000 m area. The total simulation time was set to 1,200 seconds, and the bandwidth was set to 2 Mbps. Constant Bit Rate (CBR) traffic was used to send 512 byte-UDP packets between nodes. The queuing capacity of every node was set to 15.

Consider the example scenario as shown in figure 3 where packets from node 5 to 0 are supposed to go through nodes 2 and 4. Suppose a malicious node 1 advertise it has a direct link (fake link) to node 0 and it would cause every node to update its own routing table accordingly. As a result, the packets from Nodes 5 to 0 traverse Node 1 rather than Nodes 2 and 4. Hence, Node 1 can drop and manipulate the traffic between Nodes 5 and 0. We assume, as Node 1's one-hop neighbors, both Node 0, Node 4, and Node 6 get the intrusion alerts with 80 percent confidence from their respective IDS modules. Figure 11a, 11b, 11c shows the routing tables of the nodes 0, node 4, node 6, before attack, after attack and after isolation respectively.

Algorithm 1: Calculating Risk of Attacker

1. For each node in the MANET other than attacker, Build Evidences from 2 to 5 for attacker by comparing before attach RT with after attack RT.
2. m(insecure)=(total no. of entries in RT matching evidence criteria)/(total no. of row in the before attack RT)
3. m(secure)= (1-m(insecure))
4. Bel(attack)=[m1(insecure)+m2(insecure)+m3(insecure)+m4(insecure)+m5(insecure)]/5

Algorithm 2: Calculating Risk of Countermeasure

1. For each node in the MANET other than attacker, Build Evidences from 4,5and 6 for countermeasure by comparing before attach RT with after isolation RT.
2. m(insecure)=(total no. of entries in RT matching evidence criteria)/(total no. of row in the before attack RT)
3. m(secure)= (1-m(insecure))
4. Bel(Countermeasure)=[m4(insecure) +m5(insecure) + m6(insecure)]/3

Algorithm 3: Decision Making

1. If (Bel(countermeasure)>Bel(attack)) for each node participating in the MANET NO-ISOLATION
2. Else check if(Bel(attack)>0.22)

Then perform TEMPRORAY ISOLATION.

3. And If(Bel(attack)>0.5)

Then Perform PERMANENT ISOLATION

VI. RESULTS

The table gives us comparison results of existing approaches with our approach.

Table 1:-Risk assessment and Decision Making

		Nodes		
Approaches	**Index**	**0**	**4**	**6**
BINARY	Decision	ISOLATION	ISOLATION	ISOLATION
DRC	Risk A	0.00011	0.0000057	0.0000057
	Risk C	0.00164	0.00164	0.0144
	Tot Risk	-0.00153	-0.00163	-0.0143943
	Decision	ISOLATION	ISOLATION	NO ISOLATION
DRCIF	Risk A	0.467	0.00355	0.00355
	Risk C	0.0136	0.0136	0.1
	Tot Risk	0.4534	-0.01005	-0.096
	Decision	ISOLATION	NO ISOLATION	NO ISOLATION
MPA (Mean of Probabilities approach)	Risk A	0.326	0.16	0.16
	Risk C	0.11	0.11	0.33
	Decision	RiskA>RiskC And Risk A>0.22	RiskA>RiskC And Risk A<0.22	RiskA<RiskC
		ISOLATION	NO ISOLATION	NO ISOLATION

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

We have seen that overall performance in terms of time and space complexity is improved since we do not have recursive function calls in our approach. Since belief function corresponds to output of routing table change detector.

VII. CONCLUSION

This paper proposed an approach for identification and alleviation of risk in MANET .Especially, this approach considered the potential damages of attacks and counter-measures. In order to measure the risk of both attacks and countermeasures, we Mean probabilistic approach for combination of evidence .Based on several metrics, we also investigated the performance and practicality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our identification and alleviation of MANET routing attack risks.

VIII. FUTURE SCOPE

We further seek a systematic way to cope up with MANET routing attacks. We will be working on collaborative routing attack where multiple nodes in co-ordination work to degrade the performance of the Network such as wormhole attack, where there are multiple attackers

REFERENCES

[1] Zhao, Ziming, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu. "Risk-Aware Mitigation for MANET Routing Attacks." Dependable and Secure Computing, IEEE Transactions on 9, no. 2 (2012): 250-260.
[2] Wadbude, Durgesh, and Vineet Richariya. "An Efficient Secure AODV Routing Protocol in MANET." *International Journal of Engineering and Innovative Technology (IJEIT) Volume* 1 (2012).
[3] Sabahi, F., and A. Movaghar. "Intrusion detection: A survey." In Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on, pp. 23-26. IEEE, 2008.
[4] Sentz, Kari, and Scott Ferson. Combination of evidence in Dempster-Shafer theory. Vol. 4015. Albuquerque, New Mexico: Sandia National Laboratories, 2002.
[5] Sun, Lili, Rajendra P. Srivastava, and Theodore J. Mock. "An information systems security risk assessment model under the Dempster-Shafer theory of belief functions." Journal of Management Information Systems 22, no. 4 (2006): 109-142.
[6] Shafer, Glenn. A mathematical theory of evidence. Vol. 1. Princeton: Princeton university press, 1976.
[7] Shilpa, S. G., Mrs NR Sunitha, and B. B. Amberker. "A Trust Model for Secure and QoS Routing in MANETS." *Intl. J. of Innovative Technology and Creative Engineering (IJITCE)* 1 (2011).

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)