ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

Identification and Alleviation of MANET Routing Attack Risks

Dakshayani.G, Amol P Pande
[1] Assistant professor, Fr.C.R.I.T, Vashi, India.
[2] HOD Computer Dept, Assistant professor, Datta Meghe College of engineering, Airoli.

Abstract-- A mobile ad-hoc network (MANET) is a self-starting dynamic network comprising of mobile nodes, where each and every participation node voluntarily transmit the packets destined to some remote node using wireless transmission. Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. This project is about exchange of data between the various nodes in a MANET in a secure manner. A protocol has to be designed which can effectively transfer the information. Here we maintain a routing table, based on which routing of packet is carried out. Routing table is also useful for finding out the culprit node, and further suitable action can be taken on culprit node.

Keywords: - **MANET, Routing attacks, MANET routing protocols.**

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in an environment 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 behaviors. 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 focuses on a risk-aware response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on , risk assessment which is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning with help of extended Dempster-Shafer mathematical theory of evidence[1]. 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 MANET routing protocols and routing attacks on OLSR [2].

A. Proactive & Reactive MANET Protocols

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. Reactive MANET protocols determine routing paths only when required. They are associated with lower protocol overheads but longer packet delays. Examples of reactive and proactive protocols include AODV (reactive protocol) and OLSR (proactive protocol). In reactive routing protocols, such as Ad hoc On Demand Distance Vector (AODV) protocol [2], nodes find routes only when they must send data to the destination node whose route is unknown. OLSR, nodes obtain routes by periodic exchange of topology information with other nodes and maintain route information all the time. 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[1] — 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. 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 [2]

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.

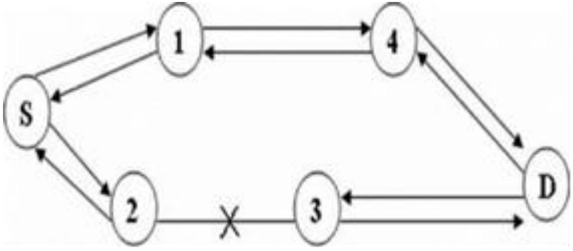

Fig I:-Black hole attack [2]

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.

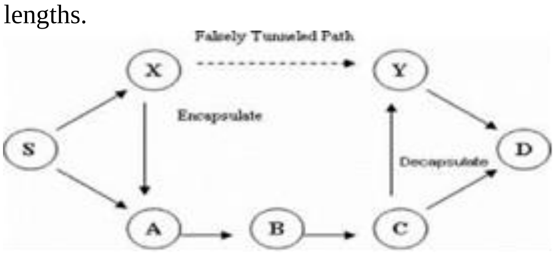

Fig II: - Wormhole attack [2]

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 travelled {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.

III. DEMPSTER-SHAFER THEORY FUNDAMENTALS

The Dumpsters–Shafer theory (DST) is a mathematical theory of evidence.[3] 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. Dempster–Shafer theory is based on two ideas: obtaining degrees of belief for one question from subjective probabilities for a related question, and Dempster's rule for combining such degrees of belief when they are based on independent items of evidence. In essence, the degree of belief in a proposition depends primarily upon the number of answers (to the related questions) containing the proposition, and the subjective probability of each answer. Also contributing are the rules of combination that reflect general assumptions about the data. In this formalism a degree of belief (also referred to as a mass) is represented as a belief function rather than a Bayesian probability distribution. Probability values are assigned to sets of possibilities rather than single events: their appeal rests on the fact they naturally encode evidence in favour of propositions.

A. Belief and plausibility

Shafer's framework allows for belief about propositions to be represented as intervals, bounded by two values, belief (or support) and plausibility:

Belief $\leq$ plausibility.

Belief in a hypothesis is constituted by the sum of the masses of all sets enclosed by it (i.e. the sum of the masses of all subsets of the hypothesis).[clarification needed] It is the amount of belief that directly supports a given hypothesis at least in part, forming a lower bound. Belief (usually denoted Bel) measures the strength of the evidence in favour of a set of propositions. It ranges from 0 (indicating no evidence) to 1 (denoting certainty). Plausibility is 1 minus the sum of the masses of all sets whose intersection with the hypothesis is empty. It is an upper bound on the possibility that the hypothesis could be true, i.e. it "could possibly be the true state of the system" up to that value, because there is only so much evidence that contradicts that hypothesis. Plausibility (denoted by Pl) is defined to be Pl(s) =1-Bel (~s). It also ranges from 0 to 1 and measures the extent to which evidence in favour of ~s leaves room for belief in s. For example, suppose we have a belief of 0.5 and a plausibility of 0.8 for a proposition, say "the cat in the box is dead." This means that we have evidence that allows us to state strongly that the proposition is true with a confidence of 0.5. However, the evidence contrary to that hypothesis (i.e. "the cat is alive") only has a confidence of 0.2. The remaining mass of 0.3 (the gap between the 0.5 supporting evidence on the one hand, and the 0.2 contrary evidence on the other) is "indeterminate," meaning that the cat could either be dead or alive. This interval represents the level of uncertainty based on the evidence in your system.

B. Interpretations on Evidence Measures

Some helpful and interesting interpretations of the evidence measures are given in the literature and cited here.

Basic Assignment: The measure m (A) assigns an evidential weight to the set A, refer Flack [6]. The measure m (A) is the degree of evidence that the element in question belongs exactly to the set A, refer Kiln & Folgers [4]. The measure m(A) is the degree of evidence supporting the claim that a specific element of W belongs to the set A, but not to any special subset of A, refer Kiln & Folgers [11].· The quantity m(A) is the degree of belief that the above specified claim is warranted, refer Kiln & Folgers [4].

Belief: The measure Bel (A) is the degree of evidence that the element in question belongs to the set A as well as to the various special subsets of A, refer Kiln & Folgers [4].· The measure Bel(A) can be interpreted as the total amount of justified support given to A, refer Denorex [4]. · The measure Bel(A) is the degree of evidence supporting the claim that a specific element of W belongs to the set A, but not to any special subset of A, refer Kiln & Folgers [4].

Plausibility: The quantity pl (A) is the degree of evidence that the element in question belongs to the set A or to any of its subsets [or to any set that overlaps with A], refer Kiln & Folgers [4]. · The quantity pl(A) can be interpreted as the maximum amount of specific support that could be given to A, if justified by additional information ,refer Smits [8].

C. Dempster-Shafer Rule of Combination

Dempster [5], [6] followed by Shafer [7] suggested a rule of combination which allows that the basic assignments are combined. There is

$$m(Z)=\frac{\sum_{A\cap B=z\neq\phi} m(A).m(B)}{1-\sum_{A\cap B\neq\phi} m(A).m(B)}$$

with A, B, Z Í W. Verbally: the numerator represents the accumulated evidence for the sets A and B, which supports the hypothesis Z, and the denominator sum quantifies the amount of conflict between the two sets. Depending on the application, the denominator of

$$m(Z)=\frac{\sum_{A\cap B=z\neq\phi} m(A).m(B)}{\sum_{A\cap B=z\neq\phi} m(A).m(B}$$

is easier to apply.

D. Importance Factors and Belief Function [4]

In D-S theory, propositions are represented as subsets of a given set. Suppose Θ is a finite set of states, and let 2 denote the set of all subsets of Θ . D-S theory calls , a frame of discernment. When a proposition corresponds to a subset of a frame of discernment, it implies that a particular frame discerns the proposition. First, we introduce a notion of importance factors.

Definition 1:- Importance factor (IF) is a positive real number associated with the importance of evidence. IF s 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 [5]. Basic probability assignment function m is defined as follows:

$$M\ (\varphi)=0$$

And

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

VI. RISK RESPONSE MECHANISM IN MANET

In this section, we discuss risk response mechanism in Manets. Our risk aware response mechanism is divided into 4 steps.

Evidence collection: here IDS gives attack alert and routing table change detector runs to find out how many changes on routing table entry caused by attack.

Risk estimation: evidence collected from previous stage would be further processed to estimate the risk involved in with attacks and risks involved in counter measures of the attacks.

Decision making: the adaptive decision module provides a flexible response decision, which takes risk estimation and risk tolerance into account to set different thresholds.

Response action: based on the decision making response action will be taken depending to the threshold level like node isolation routing table recovery.

A. Risk estimation

Our evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. We propose a unified analysis approach for evaluating the risks of both attack (Risk A) and countermeasure (Risk C). We take the confidence level of alerts from IDS as the subjective knowledge in Evidence 1. In terms of objective evidence, we analyse different routing table modification cases. There are three basic items in OLSR routing table (destination, next hop, distance). Thus, routing attack can cause existing routing table entries to be missed, or any item of a routing table entry to be changed. We illustrate the possible cases of routing table change and analyse the degrees of damage in Evidences 2 through 5.

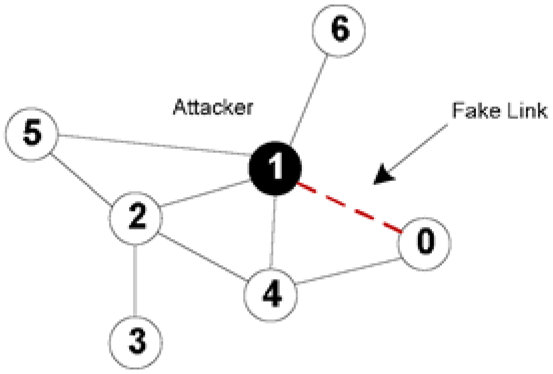

Fig III: Example scenario [1]

Evidence 1: Alert confidence. The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence. Since the false alarm is a serious problem for most IDSs, the confidence factor must be considered for the risk assessment of the attack. The basic probability assignments of Evidence 1 are based on three equations given below:

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

m(Secure)=1-c

m(Secure, Insecure) = 0

Evidence 2: Missing entry. This evidence indicates the proportion of missing entries in routing table. Link with- holding attack or node isolation countermeasure can cause possible deletion of entries from routing table of the node.

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. Malicious node could drop all the packages to or from the target node, or it can behave as a normal node and wait for future attack actions. Note that isolating a malicious node cannot trigger this case.

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. We believe the impacts on the node communication should be very minimal in this case. Both attacks and countermeasures could cause this case.

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. Similar to Evidence 4, both attacks and countermeasures could result in this evidence. The path change may also affect routing cost and transmission delay of the network.

B. Adaptive decision making

Our adaptive decision-making module is based on quantitative risk estimation and risk tolerance, which is shown in Fig. 4. The response level is additionally divided into multiple bands. 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.

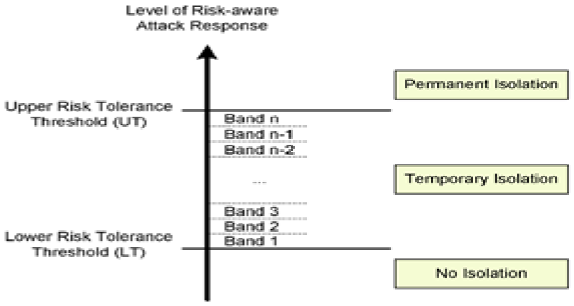

Fig IV: Adaptive decision making [1]

C. Response action to routing attacks

We use two different responses to deal with different attack methods: 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 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. IMPLEMANTATION

The project implementation starts with selection and placement of the nodes in MANET environment as shown in figure III. We are to implement this in five different steps. Once nodes are placed, routing table is formed, routing table entries are source node, destination node, next hop, and distance, and for simplicity we consider unit distance.

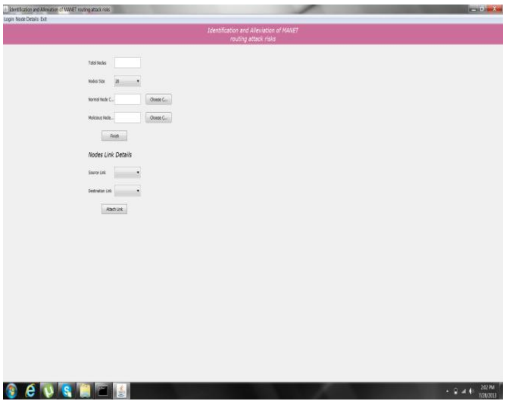

Fig V: Node selections

Each time when packet needs to be sent to destination shortest path from source to destination is calculated and packet takes the shortest path. Since MANET is topology less frequently routing table needs to be updated as host nodes move out of the MANET and some guest node may enter the MANET. Culprit node may intentionally change routing table entries by making distance to his immediate neighbour shortest, since we have taken unit distance for genuine link, therefore culprit distance will be in fraction. When routing table is updated shortest distance will be through culprit node for most of the nodes. Finally we check the intensity of damage by counting the number entries in routing tables i.e., next hop column of the routing table, so that suitable action is taken.

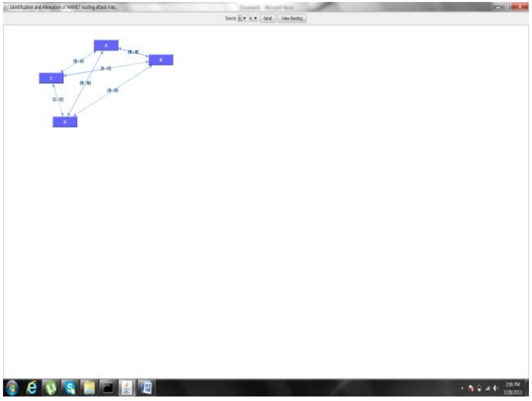
Identification and Alleviation of MANET routing attack risks
Source
Send
View Routing
A
B
C
D

Fig VI: Node placement and routing

VI. CONCLUSION

This paper proposes mechanisms to overcome the some of the risks involved in routing attacks and their counter measures by a careful assessment of the various risks and alleviation of MANET routing attacks. Especially, our approach considered the potential damages of attacks as well as damages caused by counter- measures. In order to measure the risk of both attacks and countermeasures, we use extended Dempster-Shafer theory of evidence with a notion of importance factors. We further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

REFERENCES

[1] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, Ruoyu Wu,” Risk-Aware Mitigation for MANET Routing Attacks”, IEEE Traction on dependable and secure computing ,Vol .9, MARCH/APRIL 2012.

[2] Gulshan kumar, mritunjay Rai “An approach to provide security in MANET using counter mode of encryption on MAC layer.

[3] 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.

[4] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, “Sensor Fusion Using Dempster-Shafer Theory,” Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12- 2002.

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

[6] 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.

[7] 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.

[8] K. Fall and K. Varadhan, “The NS Manual,” 2010.