International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

# "A STUDY ON -RISK AWARE MITIGATION FOR MANET ROUTING ATTACKS"

**GANGOTHRI**

*Associate Professor, Srinivas Institute of Technology Valachil, Mangalore, 574143 Karnataka, India .*

---

**Abstract -** *A Mobile Ad hoc Network (MANET) is a dynamic wireless network that can be formed by infrastructure less connections in which each node can act as a router. It is distinguished from other networks mainly by its self configuring and optimizing nature. Mobile Ad hoc Networks have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. Even though there exists several intrusions response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. 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.*

*In this paper, a new technology of broadcasting the awareness information about attacker node to all the existing nodes in the network is used. The awareness approach is based on an extended Dempster-Shafer mathematical theory (D-S Theory). Dempster-Shafer mathematical theory is used to collect the evidences with notion of importance factors. The adaptiveness of the mechanism allows to systematically cope with the identified MANET routing attacks. Here the effectiveness of the approach with the consideration of several performance metrics such as packet delivery ratio, routing cost etc were demonstrated using java swing concepts.*

***Key Words:*** **Mobile ad hoc networks, intrusion response, risk aware, dempster-shafer theory.**

## 1. 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 depends on co-operation and trusted among distributed nodes. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other node without centralized authorizes.

The intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Simple response against malicious nodes often neglects possible negative side effects involved with the response actions [1]. 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 in this paper.

### 1.2 Problem Statement

Based on the behavior of attackers, 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, attackers could not only prevent existing paths from being used, but also spoof non existing paths to lure data packets to them. 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.). All these attacks could lead to serious network dysfunctions.

In terms of attack vectors, a malicious node can disrupt the routing mechanism (as shown in figure 1.2 ) in the following simple ways:

- It changes the contents of a discovered route, modifies a route reply message, and causes the packet to be dropped as an invalid packet.
- Then, it validates the route cache in other nodes by advertising incorrect paths, and refuses to participate in the route discovery process.
- Finally, it modifies the contents of a data packet or the route via which the data packet is supposed to travel or behave normally during the route discovery process but the packets can be dropped.

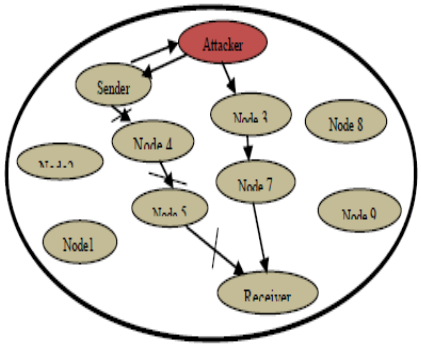



**Fig. 1.2** Network Dysfunction

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 neighbors, only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs. In OLSR, any node can either modify the protocol messages before forwarding them, or create false messages or spoof an identity. Therefore, the attacker can abuse the properties of the selection algorithm to be selected as MPR. The worst case is the possible selection of the attacker as the only MPR of a node. Or, the attackers can give wrong information about the topology of a network (TC message) in order to disturb the routing operation.

In this paper, a risk aware adaptive mechanism is proposed to deal with the problem of routing attacks in MANET and solution to defend against this attack.

### 1.3 Existing System

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. The notion of risk can be adopted to support more adaptive responses to routing attacks in MANET [3].

S.Wang [4] proposed a naive fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation.

In this paper, Dempster-Shafer mathematical theory of evidence (D-S theory) is used to bridge the gap, which offers an alternative to traditional probability theory for representing uncertainty [7]. D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields, where precise measurement is impossible to obtain or expert elicitation is required. D-S theory has several characteristics. First, it enables us to represent both subjective and objective evidences with basic probability assignment and belief function. Second, it supports Dempster's rule of combination (DRC) to combine several evidences together with probable reasoning. However, as identified in [7], Dempster's rule of combination has several limitations, such as treating evidences equally without differentiating evidence and considering priorities among them.

To address these limitations in MANET intrusion response scenario a new Dempster's rule of combination with a notion of importance factors (DRCIF) in D-S evidence model is introduced.

### 1.4 Proposed Solution

An adaptive risk-aware response mechanism based on quantitative risk estimation and risk tolerance is proposed. Instead of applying simple binary isolation of malicious nodes, this approach adopts an isolation mechanism in a temporal manner based on the risk value. An extended D-S evidence model with the notion of importance factors is also proposed here .A risk assessment with the extended D-S evidence theory introduced for both attacks and corresponding countermeasures to make more accurate response decisions.

## 2. LITERATURE SURVEY

Several techniques have been proposed in the literature in order to prevent routing attacks in MANET. In the following section, a brief survey of the work done by researchers is presented here.

- Yan Lindsay. Sun, Wei .Yu, Zhu Han, in their paper [1] presented an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. They developed four Axioms that address the basic understanding of trust and the rules for trust propagation. Based on these axioms, they also proposed two trust models: entropy-based model and probability-based model, which satisfy all the axioms. The

proposed trust evaluation method and trust models are employed in ad hoc networks for secure ad hoc routing and malicious node detection. A distributed scheme was designed to acquire, maintain, and update trust records associated with the behaviors of nodes' forwarding packets and the behaviors of making recommendations about other nodes.

- M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, in their paper [2] proposed how to isolate malicious nodes based on their reputations. Their work fails to take advantage of IDS alerts and simple isolation may cause unexpected network partition.

- P. Cheng,P.Rohatgi ,C.keser in their paper [3] presented a fuzzy logic control model for adaptive risk-based access control. They also illustrated this concept by showing how the rationale of the well-known multi-level security (MLS) access control model could be used to develop a risk-adaptive access control model.

- Shiau-Huey Wang, Chinyang Henry Tseng, and Karl Levitt in their paper [4] addressed how to perform cost-sensitive responses to routing attacks on MANET. Here cost sensitive concept is used and developed a cost model for MANET . Two indices, Topology Dependency Index (TDI) and Attack Damage Index (ADI), are developed to reflect the response cost and attack damage respectively. TDI measures the positional relationship between nodes and the attacker, and ADI represents the routing damage caused by the attacker. Response cost, routing damage brought by the isolation response, can be calculated from TDI. Comparing TDI with ADI helps the response agents (RAs) to perform Adaptive Isolation with maintaining good network throughput.

- D. Raman , M. Siva Shankar Reddy , Y. Srinivas Reddy in their paper [5] has taken one of the most amazing network concepts which makes network simpler. By considering the aspect of both side as of good and its related issues like most important and unavoidable is i.e. “Security”. Hence, enhancing the security in wireless networks has become of vital importance. In this perspective of concept, mainly two security aspects of wireless networks have been discussed. One is service confidentiality and access control that is to ensure only legitimate users can access service data according to their privileges and in other perspective is of service attack. Wireless broadcast is a convenient and effective approach for disseminating data to a number of users. User training in computer and network security is crucial to the survival of modern networks, yet the methods employed to train users often seem ineffective. The secrecy issues in the context of mandatory and discretionary access control in a multilevel networked environment. Hence in this paper two aspects of key management scheme is proposed to address secrecy and efficiency in broadcast services, where keys are used for service confidentiality and access control.

- C. Mu, X. Li, H. Huang, and S. Tian in their paper [6] presented a risk assessment model based on D-S evidence theory. The model can quantitate the risk caused by an intrusion scenario in real time and provide an objective evaluation of the target security state. The results of the online risk assessment show a clear and concise picture of both the intrusion progress and the target security state. The model makes full use of available information from both IDS alerts and protected targets. Reactive routing protocols like Ad-hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing in Ad-Hoc Wireless Networks (DSR) which are used in Mobile and Ad-hoc Networks (MANETs) work by flooding the network with control packets. There is generally a limit on the number of these packets that can be generated or forwarded. But a malicious node can disregard this limit and flood the network with fake control packets. These packets hog the limited bandwidth and processing power of genuine nodes in the network while being forwarded. Due to this, genuine route requests suffer and many routes either do not get a chance to materialize or they end up being longer than otherwise

- Kari Sentz, Scott Ferson in their paper [7] analyzed the DS theory. Dempster-Shafer theory offers an alternative to traditional probabilistic theory for the mathematical representation of uncertainty. The significant innovation of this framework is that it allows for the allocation of a probability mass to sets or intervals. Dempster-Shafer theory does not require an assumption regarding the probability of the individual constituents of the set or interval. This is a potentially valuable tool for the evaluation of risk and reliability in engineering applications when it is not possible to obtain a precise measurement from experiments, or when knowledge is obtained from expert elicitation. An important aspect of this theory is the combination of evidence obtained from multiple sources and the modeling of conflict between them.

- Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto in their work [8] analyzed the blackhole attack which is one of the possible attacks in ad hoc networks. In

a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node.In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. In this paper an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals are proposed. The simulation results show the effectiveness of the scheme compared with conventional scheme.

- C.Perkin,E. belding –Royer and S.Das in their paper [9] proposed a non cryptographic solution to the above problem and proved its efficiency by means of simulation.

- H. Deng, W.Li in their paper [10] studied the routing security issues of MANETs, and analyzed in detail one type of attack called as the "black hole" problem that can easily be employed against the MANETs. They also proposed a solution for the black hole problem for ad hoc on-demand distance vector routing protocol.8

- Some research efforts have been made to seek preventive solutions for protecting the routing protocols in MANET. “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks “proposed by Y. Hu, A. Perrig, and D. Johnson is one of the work [11]. Although these approaches can prevent unauthorized nodes from joining the network, they introduce a significant overhead for key exchange and verification with the limited intrusion elimination. Besides, prevention-based techniques are less helpful to cope with malicious insiders who possess the legitimate credentials to communicate in the network. Numerous IDSs for MANET have been recently introduced. Due to the nature of MANET, most IDS are structured to be distributed and have a cooperative architecture. Similar to signature-based and anomaly based IDS models for the wired network; IDSs for MANET use specification-based or statistics-based approaches.

- C. Tseng , S.Wang ,C. Ko in their paper [12] [13] proposed a Distributed Evidence-driven Message Exchanging intrusion detection Model (DEMEM) for MANET monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. They also proposed a specification-based intrusion-detection model for ad hoc routing protocols in which network nodes are monitored for operations that violate their intended behavior and also applied the model to detect attacks on the OLSR (Optimized Link State Routing) protocol. They also analyzed the protocol specification of OLSR, which describes the valid routing behavior of a network node, and developed constraints on the operation of a network node running OLSR. They also designed a detection mechanism based on finite state automata for checking whether a network node violates the constraints. The detection mechanism can be used by cooperative distributed intrusion detectors to detect attacks on OLSR.

- On the other hand, statistics-based approaches, such as Watchdog by S. Marti, T. Giuli, K. Lai, and M. Baker in their work [14] compare network activities with normal behavior patterns, which result in higher false positives rate than specification-based ones. Because of the existence of false positives in both MANET IDS models, intrusion alerts from these systems always accompany with alert confidence, which indicates the possibility of attack occurrence.

- Teo in his work [15] applied dynamic risk-aware mechanism to determine whether an access to the network should be denied or permitted.

## 3. THEORETICAL BACKGROUND

Theoretical background highlighting some topics related to paper work. The description contains several topics which are worth to discuss and also highlight some of their limitation that encourage going on finding solution as well as highlights some of their advantages for which reason these topics and their features are used in this paper.

### 3.1 Overview

#### 3.1.1 Routing in MANET

In MANET topology is expected to change and all network nodes cooperate to provide routing services. The characteristics of the MANET (i.e., dynamic topology, bandwidth-constrained, variable capacity links, energy-constrained, scalability, etc) require a fundamental change in routing protocol design. The major task of the routing protocol is to discover the topology to ensure that each node can acquire a recent map of the network to construct routes to its destinations. Several efficient routing protocols have been proposed for MANET.

### 3.1.2 OLSR Protocol

The major task of the routing protocol is to discover the topology to ensure that each node can acquire a recent map of the network to construct routes to its destinations. Several efficient routing protocols have been proposed for MANET.

These protocols generally fall into one of two major categories:

- Reactive routing protocols.
- Proactive routing protocols.

In reactive routing protocols, such as Ad hoc On Demand Distance Vector (AODV) protocol, nodes find routes only when they must send data to the destination node whose route is unknown.

In proactive routing protocols, such as Optimized Link-state Routing (OLSR), nodes obtain routes by periodic exchange of topology information with other nodes and maintain route information all the time.

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 neighbors, only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.

### 3.1.3 Routing Attack on OLSR

Based on the behavior of attackers, 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, attackers could not only prevent existing paths from being used, but also spoof non-existing paths to lure data packets to them. Several studies [14], [15], [16], [17] have been carried out on modeling MANET routing attacks. 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.). All these attacks could lead to serious network dysfunctions.

In terms of attack vectors, a malicious node can disrupt the routing mechanism in the following simple ways: first, it changes the contents of a discovered route, modifies a route reply message, and causes the packet to be dropped as an invalid packet; then, it validates the route cache in other nodes by advertising incorrect paths, and refuses to participate in the route discovery process; and finally, it modifies the contents of a data packet or the route via which the data packet is supposed to travel or behave normally during the route discovery process but the packets are dropped.

In OLSR, any node can either modify the protocol messages before forwarding them, or create false messages or spoof an identity. Therefore, the attacker can abuse the properties of the selection algorithm to be selected as MPR. The worst case is the possible selection of the attacker as the only MPR of a node. Or, the attackers can give wrong information about the topology of a network (TC message) in order to disturb the routing operation.

## 3.2 Extended DS Theory of Evidence

The Dempster-Shafer mathematical theory of evidence is a theory of evidence and a theory of probable reasoning. The degree of belief models the evidence, while Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidences. There are several limitations in the Dempster's rule of combination.

**1. Associative:** For DRC, 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. Nonweighted:** DRC implies that all the evidences are treated equally but in reality, they may differ.

Yager [19] proposed rules to combine several evidences presented sequentially for the first limitation. Wu et al. [20] suggested a weighted combination rule to handle the second limitation. However, the weight for different evidences in their proposed rule is ineffective and insufficient to differentiate and prioritize different evidences in terms of security and criticality.

### 3.2.1 Importance Factors and Belief Function

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

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

$$m(\phi) = 0 \quad (1)$$

and $$\sum_{A\in\theta}^{n} m(A) = 1 \quad (2)$$

According to Mathematical theory of reference, a function Bel: $2^{\theta} \rightarrow [0,1]$ is a belief function over ɵ if it is given by (3 ) for some basic probability assignment m: $2^{\theta} \rightarrow [0,1]$

$$Bel(A) = \sum_{B\in A}^{n} m(B) \quad (3)$$

for all A€ $2^{\theta}$ 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 Bel1 and Bel2 are belief functions over the same frame ɵ, with basic probability assignments m1 and m2. Then, the function m: $2^{\theta} \rightarrow [0,1]$ defined by m(ϕ)=0 and

$$m(C) = \frac{\sum Ai\cap Bi = C\ m1(Ai)m2(Bj)}{1-\sum Ai\cap Bi = \phi m1(Ai)m2(Bj)} \quad (4)$$

for all C€ ɵ ,m(C) nonempty is a basic probability assignment which describes the combined evidence.

Suppose $IF_1$ and $IF_2$ are importance factors of two independent evidences named E1 and E2, respectively. The combination of these two evidences implies that, total belief to these two evidences is 1, but in the same time, belief to either of these evidences is less than 1. This is straight forward since if our belief to one evidence is 1, it would mean our belief to the other is 0, which models meaningless evidence. And 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 E1 =(m, $IF_1$) and E2= (m, $IF_2$) are two independent evidences.The combination of E1 and E2 is E=(m1 $\oplus$ m2,$(IF_1 + IF_2)/2$), where $\oplus$ is Dempster's rule of combination with importance factors.

### 3.3 Expected Properties of Dempster's Rule of combination with Importance Factors

The proposed rule of combination with importance factors should be a superset of Dempster's rule of combination. In this section, we describe four properties that a candidate Dempster's rule of combination with importance factors should follow. Properties 1 and 2 ensure that the combined result is valid evidence. Property 3 guarantees that the original Dempster's Rule of Combination is a special case of Dempster's Rule of Combination with importance factors, where the combined evidences have the same priority. Property 4 ensures that importance factors of the evidences are also independent from each other.

**Property 1:** No belief ought to be committed to ϕ, in the result of combination rule

$$m'(\phi)=0 \quad (5)$$

**Property 2:** The total belief ought to be equal to 1 in the result of combination rule

$$\sum_{A\in\theta}^{n} m'(A) = 1 \quad (6)$$

**Property 3:** If the importance factors of each evidence are equal, our Dempster's rule of combination should be equal to Dempster's rule of combination without importance factors

**$m'(A, IF_1, IF2) = m(A)$, if $IF_1 = IF_2$** (7)

for all A€ ɵ where m(A) is the original Dempster's Combination Rule.

**Property 4:** Importance factors of each evidence must not be exchangeable

**$m'(A, IF_1, IF_2) \neq m'(A, IF_2, IF_1)$ if $(IF_1 \neq IF_2)$** (8)

### 3.4 Risk Aware Response Mechanism

In this paper, an adaptive risk-aware response mechanism is based on quantitative risk estimation and risk tolerance is proposed. Instead of applying simple binary isolation of malicious nodes, this approach adopts an isolation mechanism in a temporal manner based on the risk value and it performs risk assessment with the extended D-S evidence theory for both attacks and corresponding countermeasures to make more accurate response decisions.

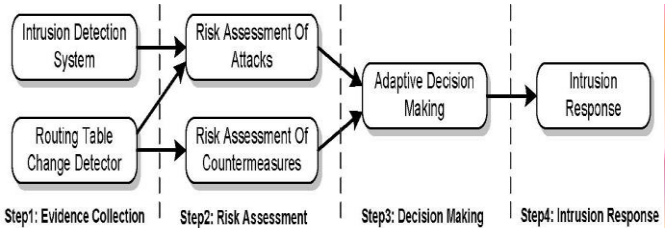



**Fig. 3.4. Risk aware response mechanism**

Because of the infrastructure-less architecture of MANET, this 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. This risk aware response mechanism is divided into the following four steps as shown in Fig. 3.4.

- **Evidence collection:** 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:** 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. 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 isolation, are carried out to mitigate attack damages in a distributed manner.

## 3.5 Response to Routing Attacks

In this approach two different responses to deal with different attack methods are used: 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 neighbors 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.

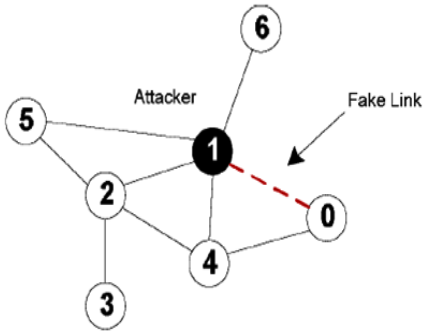



**Fig. 3.5. Example scenario**

For example, in Fig. 3.5., 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 mechanism is required. In this risk-aware response mechanism, two types of time-wise isolation responses are adopted: temporary isolation and permanent isolation

## 3.6 Risk Assessment

Since the attack response actions may cause more damages than attacks, the risks of both attack and response should be estimated. The security states of MANET are classified into two categories: {Secure, Insecure}. In other words, the frame of discernment would be {_, {Secure}, {Insecure}, {Secure, Insecure}}. Note that {Secure, Insecure} means the security state of MANET could be either secure or insecure, which describes the uncertainty of the security state. Bel(Insecure) is used to represent the risk of MANET.

### 3.6.1 Selection of Evidences

This evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. A unified analysis

approach for evaluating the risks of both attack $Risk_A$ and countermeasure $Risk_C$ are proposed. The confidence level of alerts from IDS as the subjective knowledge in Evidence 1 is taken. In terms of objective evidence, different routing table modification cases are analyzed. 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. The possible cases of routing table change are illustrated and analyzed the degrees of damage in Evidences 2 through 5.

- **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:

$$m(Insecure) = c,\ c \text{ is confidence given by } IDS \quad (9)$$

$$m(Secure) = 1 - c \quad (10)$$

$$m(Secure,\ Insecure) = 0. \quad (11)$$

- **Evidence 2:** Missing entry. This evidence indicates the proportion of missing entries in routing table. Link withholding 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. The impacts on the node communication should be very minimal in 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. Basic probability assignments of Evidences 2 to 5 are based on (12-14). Equations (12-14) are piecewise linear functions, where a, b, c, and d are constants and determined by experts. d is the minimum value of the belief that implies the status of MANET is insecure. On the other hand, 1-d is the maximum value of the belief that means the status of MANET is secure. a, b, and c are the thresholds for minimum belief or maximum belief for each respective mass function.

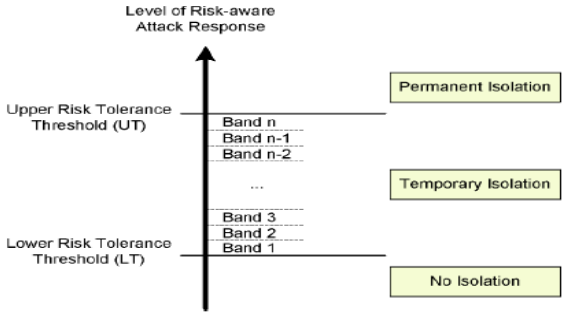
$$m(Insecure) = \begin{cases} d & x \in [0,a] \\ \left(\frac{1-2d}{c-a}\right)(x-a) & x \in (a,c] \\ 1-d & x \in (c,1], \end{cases} \quad (12)$$

$$m(Secure) = \begin{cases} 1-d+\left(\frac{2d-1}{b}\right)x & x \in [0,b] \\ d & x \in (b,1], \end{cases} \quad (13)$$

$$m(Secure, Insecure) = \begin{cases} \frac{1-2d}{b}x & x \in [0,a] \\ d-\frac{2d-1}{b}x- & \\ \left(\frac{1-2d}{c-a}\right)(x-a) & x \in (a,b] \\ 1-b- & \\ \left(\frac{1-2d}{c-a}\right)(x-a) & x \in (b,c] \\ 0 & x \in (c,1]. \end{cases} \quad (14)$$

### 3.7 Adaptive Decision Making

This adaptive decision-making module is based on quantitative risk estimation and risk tolerance, which is shown in Figure. 3.7.1. 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 given by the formula (15) and (16), where n is the number of bands and i is the corresponding isolation band.




$$i = \left\lceil \frac{Risk - LT}{UT - LT} \times n \right\rceil, \; Risk \in (LT, UT), \qquad (15)$$

$$T = 100 \times i \; (milliseconds). \qquad (16)$$

**Fig 3.7. Adaptive Decision Making**

The value of lower risk tolerance threshold will be 0 initially if no additional information is available. It implies when the risk of attack is greater than the risk of isolation response, the isolation is needed. If other information is available, it could be used to adjust thresholds. For example, node reputation is one of important factors in MANET security; this adaptive decision-making module could take this factor into account as well. That is, if the compromised node has a high or low reputation level, the response module can intuitively adjust the risk tolerance thresholds accordingly. In the case that LT is less than 0, even if the risk of attack is not greater than the risk of isolation, the response could also perform an isolation task to the malicious nodes. The risk tolerance thresholds could also be dynamically adjusted by other factors, such as attack frequency. If the attack frequency is high, more severe response action should be taken to counter this attack. This risk-aware response module could achieve this objective by reducing the values of risk tolerance threshold and narrowing the range between two risk tolerance thresholds. It may be hacked, dropped or decrypted by malicious node.

**Accessing the Risk using DS theory:** 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. Based on this information 5 evidences are calculated and are combined using DS theory of evidence with the notion of importance factors which will result in risk value.

**Based on risk value, filter the attacker temporarily, timed-wait, blocked:** Next upper and lower threshold values are set which will represent the maximum and minimum threshold values. Adaptive decision making approach will be used to remove the attacked nodes from the MANET environment by comparing these threshold values with the obtained risk value. 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.

## 4. INTERPRETATION OF RESULTS

### 4.1 Results

The following snapshots define the results or outputs that are obtained after step by step execution of all the modules of the system.

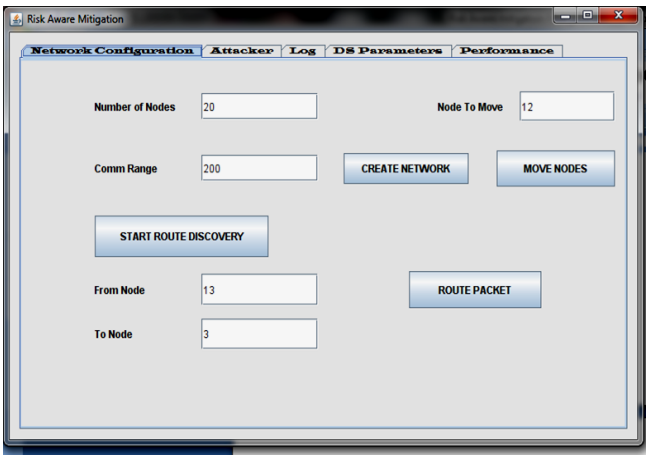



**Chart -1**: creation of MANET

**Interpretation: -** Here mobile nodes are created using java swing concepts. Java Swing is 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. Once application is started, MANET is created with number of nodes and every node sends some packets by using dynamic path routing. It also shows source and destination for routing the packet and node to be moved in MANET environment.

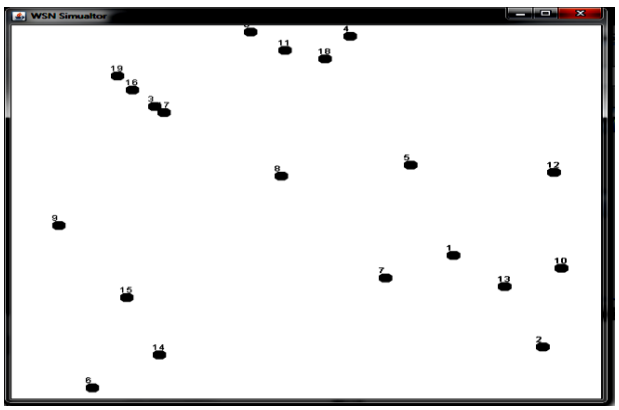



**Chart -2**: placement of Nodes

**Interpretation: -** Every node is initialized using unique ID and its location information. After specifying the required information and pressing create network, network will be displayed in neat gui by randomly placing these nodes in a 600 *600 grid.

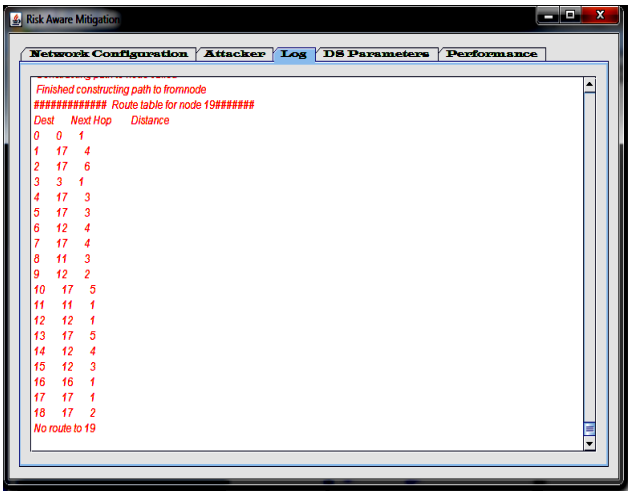



**Chart -3**: Route Discovery

**Interpretation:-** Once the nodes are randomly placed, on pressing Start Route Discovery, distance between the nodes are calculated and based on this and range information MPR nodes are calculated for each node which is used for broadcasting the information about the topology of the network.. Once the MPR information is broadcasted, topology table is constructed for each node and from this information routing table is constructed which is used for packet routing. All these information's will be stored in the log.

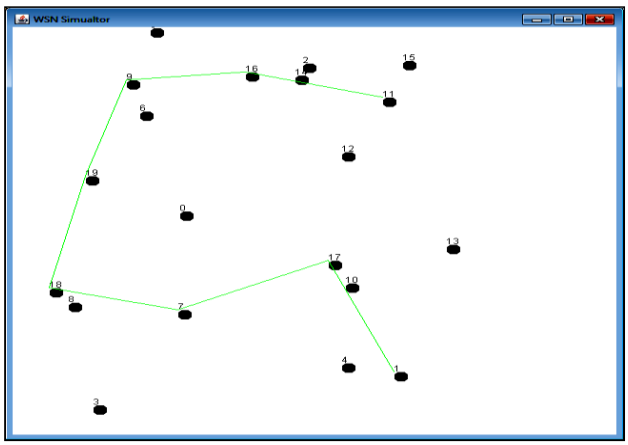



**Chart -4**: Routing of the packet

**Interpretation:-** Every node sends some packets by using dynamic path routing. When Route packet button is pressed after specifying the source and destination for routing the packet, routing of the packet is displayed in a neat gui.

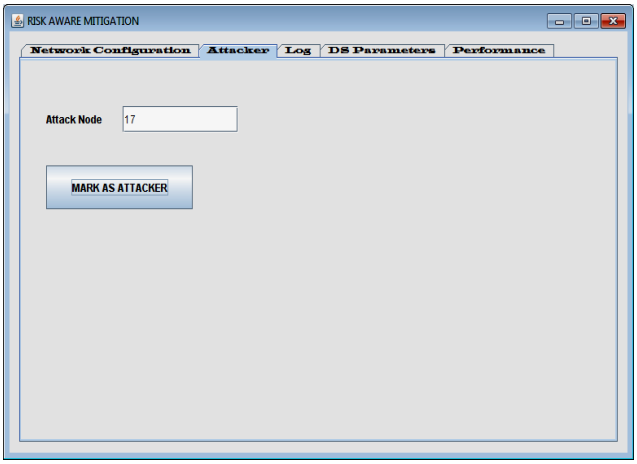



**Chart -5**: Marking the Attacker Node

**Interpretation: -**. Any node in the network can be marked as a attacker node. The attack can be identified from the routing table update report.

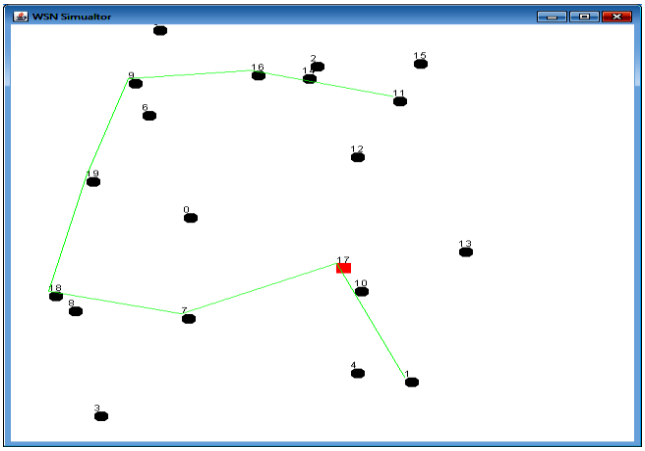



**Chart -6**: Malicious node

**Interpretation: -** Every node sends some packets by using dynamic path routing. The attacker optimizes like a node and joins the network and it cause additional damage to the network.

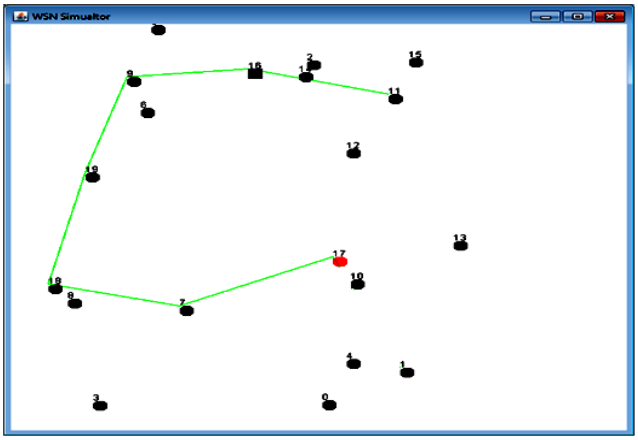



**Chart -7**: Dropping the packet by malicious node

**Interpretation:-**Network dysfunction shows the implementation of black hole attack in which, the sender sends the packets, that data may be hacked or dropped by malicious node. Due to this attack, an alert is given and routing table changes detector report is formed.

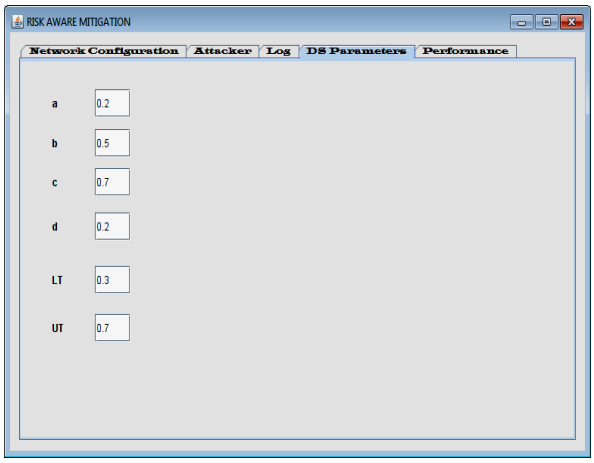



**Chart -8**:Finding the risk value

**Interpretation: -** The figure above shows the DS parameters which are used to find the risk value where d is the minimum value of the belief that implies the status of MANET is insecure. On the other hand, 1-d is the maximum value of the belief that means the status of MANET is secure. a, b, and c are the thresholds for minimum belief or maximum belief for each respective mass function. LT and UT represent lower and upper threshold values respectively.

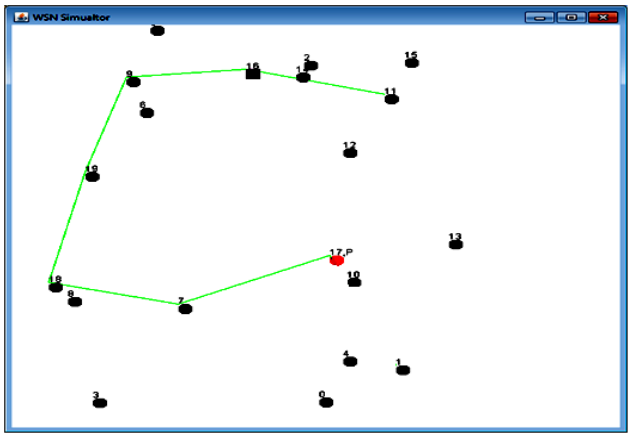



**Chart -8** : Decision making

**Interpretation: -** Decision making is evaluated based on the evidence collection. Evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. Due to attack, an alert is given and routing table changes detector report is formed. Based on this information 5 evidences are calculated and are combined using DS theory of evidence with the notion of importance factor, which will produce risk value as an output. Next upper and lower threshold values are set which will represent the maximum and minimum threshold values. Adaptive decision making approach will be used to remove the attacked nodes from the MANET environment by comparing these threshold values with the obtained risk value. 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. Node isolation is the process of removing the attacked nodes from the MANET area. Routing table recovery will used to re compute the original routing table from the attacker routing table.

### 4.2 Analysis

In order to test the effectiveness and scalability of this solution, the risk-aware approach with DRCIF is evaluated on different random network topologies. These five topologies have different set of nodes respectively. The figures below shows the performance results in these random network topologies of risk-aware approach with DRCIF, risk-aware approach with binary isolation approach.

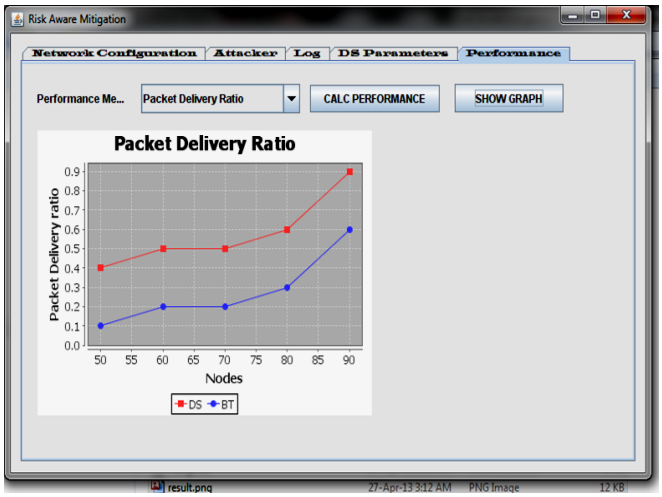



**Chart -9**: Packet delivery ratio

**Interpretation**: - Packet delivery ratio is the ratio between the number of packets originated by sources and the number of packets received by destinations. As the number of nodes increases, the packet delivery ratio also increases because there are more route choices for the packet transmission. Moreover, among these two response mechanisms, the packets delivery ratio of DRCIF risk-aware response is higher than that of binary isolation.


**Chart -10**: Routing Cost

**Interpretation: -** Routing Cost is the ratio between the total bytes of routing packets transmitted and the total bytes of packets received by destinations. The routing cost of DRCIF risk-aware response is lower than the binary isolation approach. The fluctuations of routing cost shown in figure below are caused by the random traffic generation and random placement of nodes which may have more influence on the routing cost.

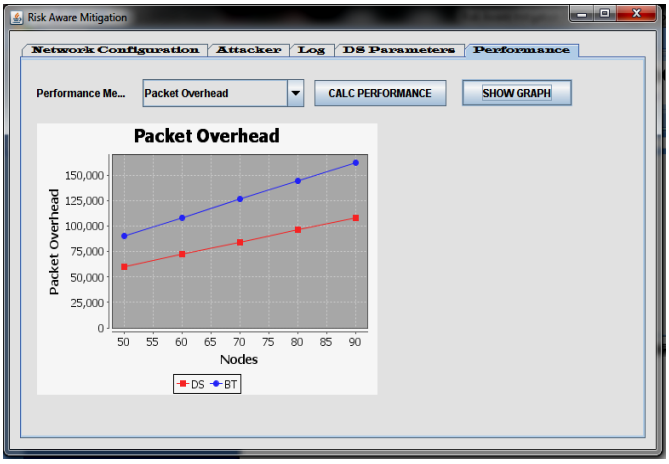



**Chart -11**: Packet overhead

**Interpretation:-** Packet overhead is the number of transmitted routing packets; for example, a HELLO or TC message sent over four hops would be counted as four packets in this metric. In DRCIF risk-aware response, the number of nodes which isolate the malicious node is less than the binary isolation. Therefore as the number of nodes increases, the packet overhead using our DRCIF risk-aware response are slightly higher than binary isolation .

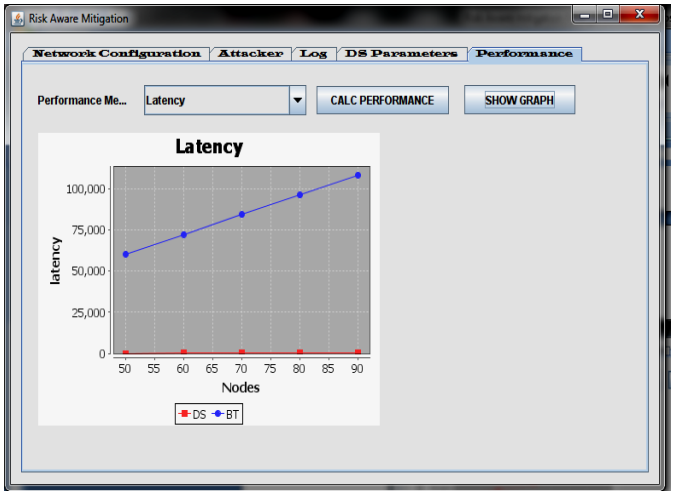



**Chart -12**: Latency

**Interpretation: -** Latency is the time elapsed from "when a data packet is first sent" to "when it is first received at its destination." The figure below shows, the latency using DRCIF risk-aware response is higher than the binary isolation approach, when the number of nodes is smaller than 50. However, when the number of nodes is greater than 50, the latency using DRCIF risk-aware response approach is less than binary isolation approach.

## 5. CONCLUSIONS

MANET is distinguished from other networks mainly by its self configuring and optimizing nature. Being the flexible network, MANET is exposed to various kinds of attacks especially the routing attacks. This paper proposed a risk-aware response solution for mitigating MANET routing attacks. In this paper malicious node in the MANET network is detected and isolated using Dempster-Shafer mathematical theory.

Especially, risk-aware approach considered the potential damages of attacks and countermeasures. In order to measure the risk of both attacks and countermeasures, extended Dempster-Shafer Theory of evidence with a notion of importance factor is used.

Based on several metrics, the performance and practicality of this approach is investigated and the experiment results clearly demonstrated the effectiveness and scalability of risk aware approach. Based on the promising results obtained through these experiments, one would further seek more systematic way to accommodate node reputation and attack frequency in this adaptive decision model.

The paper can be carried forward by making certain addition. Some of the suggestions with regard to this are as follows:

- The number of evidences required to compute the risk factor for each node can be increased to improve the accuracy.
- The various routing attacks performance can be studied by considering different proactive routing protocols.
- This approach can be applied for reactive routing protocols by using route maintenance procedures.

## 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] 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.

[5] D.Raman , M. Siva Shankar Reddy , Y. Srinivas Reddy : "Risk Assessment for Identifying Intrusion Detection using DS-evidence Theory in MANET "Vol.1 (3) 2012.

[6] 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), pp. 35-48, 2008.

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

[8] Shiau-Huey Wang, Chinyang Henry Tseng, Karl N. Levitt, Matt Bishop " Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks " RAID, pp. 127- 145, 2007.

[9] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.

[10] 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.

[11] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, no. 1, pp. 21-38, 2005.

[12] C. Tseng, S. Wang, C. Ko, and K. Levitt, "DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for MANET," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06), pp. 249-271, 2006.

[13] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt, "A Specification-Based Intrusion Detection Model for OLSR," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06),pp. 330-350, 2006.

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

[15] L. Teo, G. Ahn, and Y. Zheng, "Dynamic and Risk-Aware Network Access Management," Proc. Eighth ACM Symp. Access Control Models and Technologies (SACMAT '03), pp. 217-230, 2003.

[16] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.

[17] 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

[18] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

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

[20] 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.