Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 67 (2014) 21603-21608

ISSN: 2229-712X

# Handling Manet routing attacks using risk aware mitigation mechanism with extended D-S theory

A.Jaganraj[1], A.Yogaraj[2], N.Vignesh[3] and R.V.Anuroop[2]

[1]Arulmigu Meenakshi Amman College of Engineering, Near Kanchipuram, India.

[2]ECE Dept.,Veltech Dr.R.R & Dr.S.R Technical University, Avadi, Chennai, India.

[3]EEE Dept.,Veltech Multitech Engineering College, Avadi, Chennai, India.

**ARTICLE INFO**

**Article history:**

Received: 26 July 2013;

Received in revised form:

24 January 2014;

Accepted: 8 February 2014;

**Keywords**

Mobile ad hoc networks,

Intrusion response,

Risk aware,

Dempster-shafer theory.

**ABSTRACT**

Mobile Ad hoc Networks (MANET) 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 exist several intrusion response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naıve fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naıve fuzzy responses could lead to uncertainty in countering routing attacks in MANET. In this paper, we propose a risk-aware response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of several performance metrics.



## Introduction

MOBILE Adhoc Networks (MANET) is utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. 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. Several work [1], [2] 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]. 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. Wang et al. [4] proposed a naı¨ve 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. In this paper, we seek a way to bridge this gap by using Dempster-Shafer mathematical theory of evidence (D-S theory), which offers an alternative to traditional probability theory for representing uncertainty [5]. D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields [6], [7], 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 [8], [9], [10], [11], Dempster's rule of combination has several limitations, such as treating evidences equally without differentiating each evidence and considering priorities among them. To address these limitations in MANET intrusion response scenario, we introduce a new Dempster's rule of combination with a notion of importance factors (IF) in D-S evidence model. In this paper, we propose a risk-aware response mechanism to systematically cope with routing attacks in MANET, proposing an adaptive time-wise isolation method. Our risk-aware approach is based on the extended D-S evidence model. 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) [12]. In addition, we attempt to demonstrate the effectiveness of our solution.

## 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

Tele:

E-mail addresses: jagan_math88@yahoo.co.in

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. Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation. Wang et al. proposed a naıve 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.

**Disadvantage of existing system:**

However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning.

**Proposed system:**

We formally propose an extended D-S evidence model with importance factors and articulate expected properties for Dempster's rule of combination with importance factors (DRCIF). Our Dempster's rule of combination with importance factors is nonassociative and weighted, which has not been addressed in the literature. We propose an adaptive risk-aware response mechanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of our mechanism allows us to systematically cope with MANET routing attacks. We evaluate our response mechanism against representative attack scenarios and experiments. Our results clearly demonstrate the effectiveness and scalability of our risk-aware approach.

**Backgrounds**

In this section, we overview the OLSR and routing attacks on OLSR.

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

**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 nonexisting paths to lure data packets.

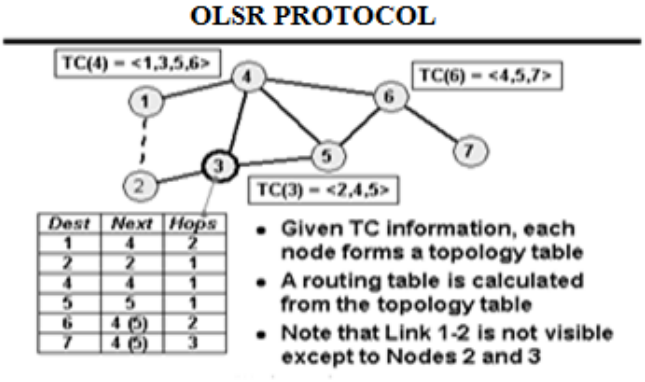


**Fig. 1. OLSR Protocol.**

**Extended dempster-shafer theory of evidence**

The Dempster-Shafer mathematical theory of evidence is both 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.

**Dempster's rule**

1. **Associative**. For DRC, the order of the information in the aggregated evidences does not impact the result. As shown in [10], a nonassociative combination rule is necessary for many cases.

2. **Nonweighted**. DRC implies that we trust all evidences equally [11]. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence.

**Importance Factors and Belief Function**

In D-S theory, propositions are represented as subsets of a given set. 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. Ifs are derived from historical observations or expert experiences.

*Definition 2.*

An evidence E is a 2-tuple hm; IFi, where m describes the basic probability assignment [5].Basic probability assignment function m is defined as follows: $m(\Phi)=0$ and $\Sigma m(A)=1$ (1) and $\Sigma m(A)=1$ (2) According to [5], a function Bel:2θ ->[0,1] ,a belief function over θ if it is given by (3) for some basic probability assignment m:2θ->[0,1] $Bel(A)=\Sigma m(B)$ for all $A \epsilon 2^{\theta}$ ,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 θ, with basic probability assignments m1 and m2.Then, the function m : 2 θ->[0,1]; defined by $m(\theta)=0$ and $m(C)=(\Sigma Ai \cap Bj = Cmi (Ai)\ m2\ (Bj))/(1-\Sigma Ai \cap Bj=\Phi m1(Ai)m2(Bj))$ (4) for all nonempty $C \subseteq \theta$,, m(C) is a basic probability assignment which describes the combined evidence.Suppose IF1 and IF2 are importance factors of two independent evidences named E1 and E2, respectively. The combination of these two evidences implies that our total belief to these two evidences is 1, but in the same time, our belief to either of these evidences is less than 1. This is straightforward since if our belief to one evidence is 1, it would mean our belief to the other is 0, which models a meaningless evidence. And we

define the importance factors of the combination result equals to (IF1 + IF2)=2.

*Definition 3*.

Extended D-S evidence model with importance factors: Suppose E1=<m1,IF1> and E2 =< m2, IF2> are two independent evidences. Then, the combination of E1 and E2 is E = <m1 Θ m2,(IF2+IF2)/2>, where Θ is Dempster's rule of combination with importance factors.

**Expected Properties for Our 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 a 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 in the result of our combination rule m'(Φ)=0 (5) Property 2. The total belief ought to be equal to 1 in the result of our combination rule Σm'(A)=1 (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,IF1,IF)= m(A); if IF1= IF2 (7) for all Aϵθ, where m(A) is the original Dempster'sCombination Rule. Property 4. Importance factors of each evidence must not beexchangeable m'(A1, IF1, IF2) ≠ m'(A,IF2,IF1) if (IF1 ≠ IF2) (8)

**Dempster's Rule of Combination with Importance Factors**

In this section, we propose a Dempster's rule of combination with importance factors. We prove our combination rule follows the properties defined in the previous section.

***Theorem 1. Dempster's Rule of Combination with Importance Factors:***

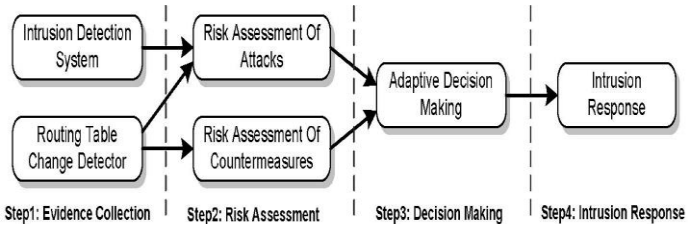


**Fig. 2. Risk-aware response mechanism**

Suppose Bel1 and Bel2 are belief functions over the same frame of discernment , with basic probability assignments m1 and m2. The importance factors of these evidences are IF1 and IF2. Then, the function m defined by Our proposed DRCIF is non associative for multiple evidences. Therefore, for the case in which sequential information is not available for some instances, it is necessary to make the result of combination consistent with multiple evidences. Our combination algorithm supports this requirement and the complexity of our algorithm is O(n), where n is the number of evidences. It indicates that our extended Dempster-Shafer theory demands no extra computational cost compared to a naı¨ve fuzzy-based method. The algorithm for combination of multiple evidences is constructed as follows:

Algorithm 1. MUL-EDS-CMB

INPUT: Evidence pool Ep

OUTPUT: One evidence

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

**Risk-Aware Response Mechanism**

In this section, we articulate an adaptive risk-aware response mechanism based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. We perform risk assessment with the extended D-S evidence theory.

**Overview**

Because of the infrastructure-less architecture of MANET, our risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships. Our risk aware response mechanism is divided into the following four steps shown in Fig. 3. 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.

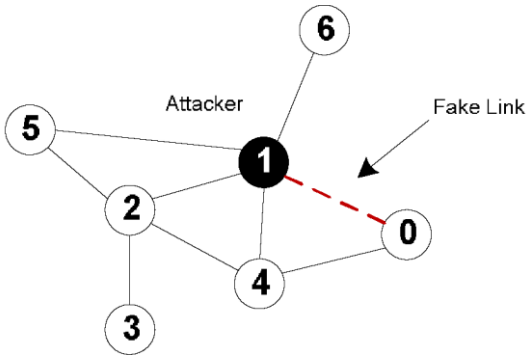


**Fig. 3. Example scenario**

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.

**Response to Routing Attacks**

In our approach, 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 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. For example, in Fig, 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 our risk-aware response mechanism, we adopt two types of time-wise isolation responses: temporary isolation and permanent isolation, which are discussed in Section 4.4.

**Risk Assessment**

Since the attack response actions may cause more damages than attacks, the risks of both attack and response should be estimated. We classify the security states of MANET 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.

**Selection of evidence**

Evidence choice approach considers subjective proof from experts' information and objective proof from routing table modification. we have a tendency to propose a unified analysis approach for evaluating the risks of each attack (RiskA) and step (RiskC). Take the arrogance level of alerts from IDS because the subjective information conspicuous one. In terms of objective proof, analyze whole completely different routing table modification cases. There area unit staple items in OLSR routing table (destination, next hop, distance). Thus, routing attack can cause existing routing table entries to be unintelligible, or any item of a routing table entry to be changed. We illustrate the possible cases of routing table change and analyze the degrees of damage in Evidences 2 through 5.

Evidence 1: Alert confidence. the boldness of attack detection by the IDS is provided to deal with the likelihood of the attack incidence.

Evidence 2: Missing entry. This proof indicates the proportion of missing entries in routing table. Link withholding attack or node isolation step will cause potential deletion of entries from routing table of the node.

Evidence 3: ever-changing entry I. This proof represents the proportion of fixing entries within the case of next hop being the malicious node.

Evidence 4: ever-changing entry II. This proof shows the proportion of modified entries within the case of various next hops (not the malicious node) and therefore the same distance.

Evidence 5: ever-changing entry III. This proof points out the proportion of fixing entries within the case completely different of various} next hop (not the malicious node) and therefore the different distance. like proof four, each attacks and countermeasures might end in this proof.

***Combination of evidance***

Call the combined evidence for an attack, EA and the combined evidence for a countermeasure, EC. Thus, BelA(Insecure) and BelC(Insecure) represent risks of attack (RiskA) and countermeasure (RiskC), respectively. The combined evidences, EA and EC are defined and the entire risk value derived from RiskA and RiskC

$EA = E1 \oplus E2 \oplus E3 \oplus E4 \oplus E5$,

$EC = E2 \oplus E4 \oplus E5$,

where $\oplus$ is Dempster's rule of combination with important factors defined in Theorem 1

Risk = RiskA - RiskC = BelA(Insecure) –BelC(Insecure).

***Adaptive decision making***

The response level is as well divided into multiple bands. each band is said to academic degree isolation degree, that presents a special amount of your time of the isolation action. The response action and band boundaries unit all determined in accordance with risk tolerance and may be changed once risk tolerance threshold changes. the upper risk tolerance threshold (UT) would be associated with permanent isolation response. The lower risk tolerance threshold (LT) would keep each node intact. The band between the upper tolerance threshold and lower tolerance threshold is said to the temporary isolation response, inside that the isolation time (T) changes dynamically supported the assorted response level given by following equation where n is that the vary of bands which i is that the corresponding isolation band.

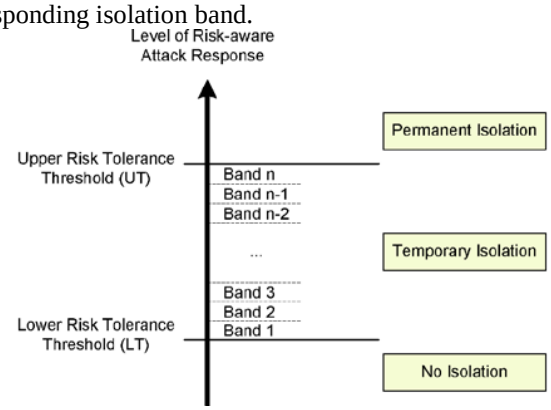


**Fig. 4. Adaptive decision making**

**Result**

The performance ends up in these random network topologies of our risk-aware approach with DRCIF, risk-aware approach with DRC and binary isolation approach. In Fig. 5, because the range of nodes will increase, the packet delivery magnitude relation conjointly will increase as a result of their square measure a lot of route decisions for the packet transmission. Among these 3 response mechanisms, we have a tendency to conjointly notice the packets delivery magnitude relation of our DRCIF risk-aware response is on top of those of the opposite 2 approaches.

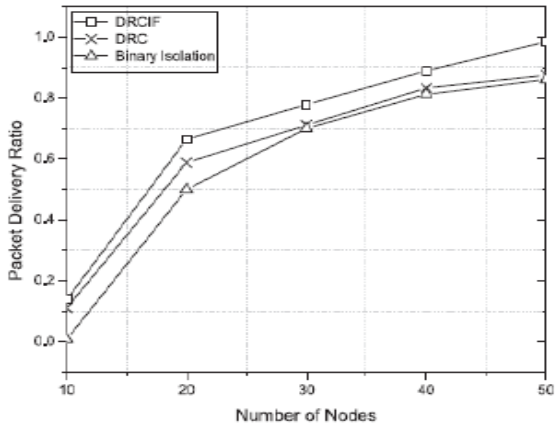


**Fig. 5 Packet delivery ratio**

In Fig. 6, we are able to observe that the routing price of our DRCIF risk-aware response is under those of the opposite 2 approaches. Note that the fluctuations of routing price shown in Fig. three are caused by the random traffic generation and random placement of nodes in our realistic simulation. In our DRCIF risk-aware response, the amount of nodes that isolate the malicious node is a smaller amount than the opposite 2 response mechanisms.

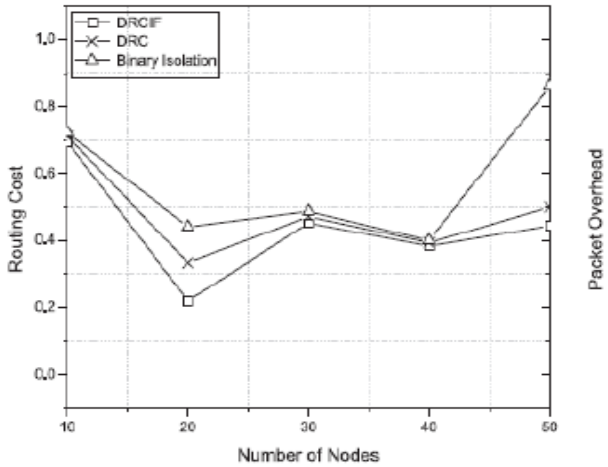


**Fig 6. Routing cost**

In Fig 7 , that's the reason why we can also notice that as the number of nodes increases, the packet overhead and the using our DRCIF risk-aware response are slightly higher than those of the other two response mechanisms.

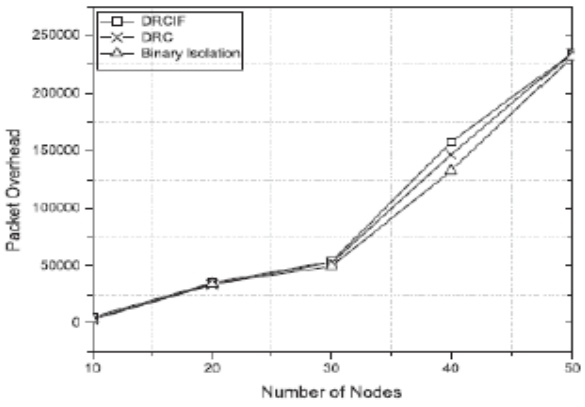


**Fig. 7 Packet Overhead**

In Fig. 8 The mean latency victimization our DRCIF risk-aware response is over those of the opposite 2 response mechanisms, once the amount of nodes is smaller than twenty. However, once the amount of nodes is bigger than twenty, the mean latency victimization our approach is a smaller amount than those of the opposite 2 response mechanisms.

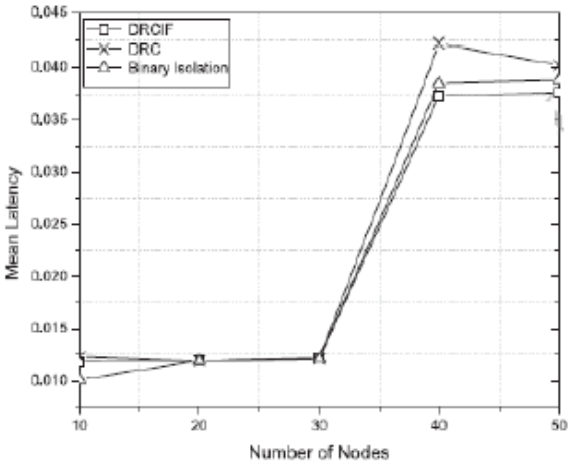


**Fig.8 Mean Latency**

**Conclusion**

Risk-aware response answer for mitigating Manet routing attacks. Especially, our approach considered the potential damages of attacks and countermeasures. so as to live the danger of each attacks and countermeasures, we tend to extended Dempster- Shafer theory of proof with a notion of importance factors. supported many metrics, we tend to additionally investigated the performance and utility of our approach and also the experiment results clearly incontestable the effectiveness and quantifiable of our risk aware approach. supported the promising results obtained through these experiments.

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

[6] L. Sun, R. Srivastava, and T. Mock, "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions," J. Management Information Systems,vol. 22, no. 4, pp. 109-142, 2006. [7] C. Mu, X. Li, H. Huang, and S. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," Proc. 13th European Symp. Research in Computer Security (ESORICS '08),pp. 35-48, 2008.

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

[9] L. Zadeh, "Review of a Mathematical Theory of Evidence," AIMagazine, vol. 5, no. 3, p. 81, 1984. [10] R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.

[11] 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.
[12] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.
[13] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group,vol. 3561, 2003.