RESEARCH ARTICLE OPEN ACCESS

# Minimizing Routing Attacks in MANET Using Extended Dempster-Shefer Theory

A. V. R. Sandesh Guptha [1], S. Reshma [2]
[1] M.Tech, Chadalawada Ramanamma Engineering College.
[2] Asst. Professor of Department of CSE, Chadalawada Ramanamma Engineering College.

**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 naïve fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naïve 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 DempsterShafer 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. Route request flooding attack is one such distributed DoS attack, launched by compromised nodes or intruders. This triggers an acute need of flooding attack prevention mechanisms for this highly vulnerable type of network. In this paper, a reputation based scheme is proposed to resist the impact of flooding attack in MANET. This scheme observes the behavior of a node in the network periodically and limits its route request sending rate accordingly.
**Index Terms**—Mobile ad hoc networks, intrusion response, risk aware, dempster-shafer theory. Flooding Attack,

## I. INTRODUCTION

MOBILE Ad hoc Networks (MANET) are 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.

Flooding attack has thus become a major security concern and has attracted the interest of many researchers [6]. However, none of the remedies proposed so far have successfully curbed the impact of flooding attack in MANET in practical scenario. In a heterogeneous environment like MANET, different types of devices exist and work together. These various devices may have different rates of data transfer. It is quite unfair to restrict all these devices with a single threshold of maximum number of RREQs sent. Choosing a perfect threshold value is quite impossible when considered in practical. If this value is chosen quite small, then devices with high data transfer requirements are bound to suffer. Conversely, malicious nodes may take advantage of a large threshold value to flood the network with fake RREQs. In this paper, a reputation based mechanism is proposed to mitigate the impact of flooding attack in MANET. *Reputation* of a node is the measure of its behavior in the network and determines the rate at which it is allowed to send route request packets. Hence, devices are restricted to send RREQs on the basis of their behavior in the network.

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, 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.
adaptive responses to routing attacks in MANET .
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 naïve 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 DempsterShafer 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.
The major contributions of this paper are summarized as follows:

We formally propose an extended D-S evidence model with importance factors and articulate ex pected 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 adaptive ness 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.

The rest of this paper is organized as follows: Section 2 overviews a MANET routing protocol OLSR and routing attacks against OLSR. Section 3 describes how our extended D-S evidence model can be integrated with importance factors. Section 4 presents the details of our risk-aware response mechanism. The evaluations of our approach are discussed in Section 5. Section 6 provides the related work in MANET intrusion detection and response systems, also reviews risk-aware approaches in different fields. Section 7 concludes this paper.

## II. BACKGROUND

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

### 2.1 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 Ad hoc On Demand Distance Vector (AODV) protocol [13], 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.

### 2.2 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 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 is 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.

## III. 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. However, previous research efforts identify several limitations of the Dempster's rule of combination

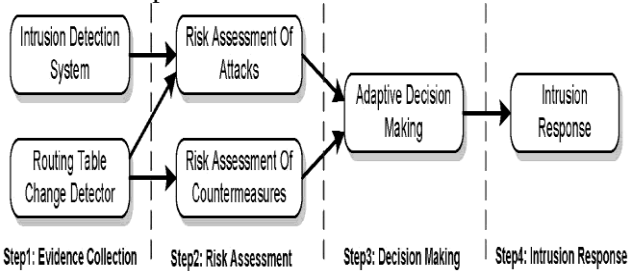
1. Associative. For DRC, the order of the information in the aggregated evidences does not impact the result. As shown in [10], a nonassociative combination rule is necessary for many cases.
2. No weighted. DRC implies that we trust all evidences equally [11]. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence Yager [10] and Yamada and Kudo [18] proposed rules to combine several evidences presented sequentially for the first limitation. Wu et al. [11] 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. Our extended Dempster-Shafer theory with importance factors can overcome both of the aforementioned limitations.

### 3.1 Importance Factors and Belief Function

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

### 3.2 .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.




Our proposed DRCIF is nonassociative 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 sup- ports this requirement and the complexity of our algorithm is Oðnþ, where n is the number of evidences. It indicates that our extended Dempster-Shafer theory demands no extra computational cost compared to a naïve fuzzy-based method. The algorithm for combination of multiple evidences is constructed as follows:

Algorithm 1. MUL-EDS-CMB
OUTPUT: One evidence
1 jEpj ¼ sizeof(Ep);
2 While jEpj > 1 do
3 Pick two evidences with the least IF in Ep, named $E_1$ and $E_2$ ;
4 Combine these two evidences,
E ¼ ℏ$m_1$ $m_2$ ; ðIF$_1$ Þ IF$_2$ Þ=2i;
5 Remove $E_1$ and $E_2$ from Ep;
6 Add E to Ep;
7 end
8 return the evidence in Ep

## IV. 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 introduced in Section 3 for both attacks and corresponding countermeasures to make more accurate response decisions illustrated in Fig. 1.

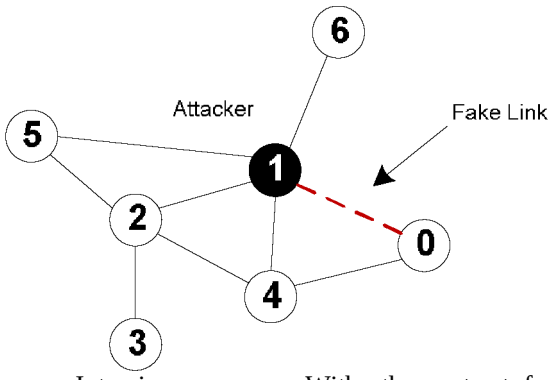
### 4.1 Overview

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 ware response mechanism is divided into the following four steps shown in Fig. 1.

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 able 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.

### 4.2 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. 2, Node

1 behaves like a malicious node. However, if every other node simply isolate Node 1, Node 6 will be disconnected from the network. Therefore, more flexible and fine-grained node isolation mechanism are 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.

### 4.3.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. BelfInsecureg is used to represent the risk of MANET.

#### 4.3.1 Selection of Evidences

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 ðRisk$_A$Þ and countermeasure ðRisk$_C$Þ.

We take the confidence level of alerts from IDS as the subjective knowledge in Evidence 1. In terms of objective evidence, we analyze 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 analyze 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.

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.

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.

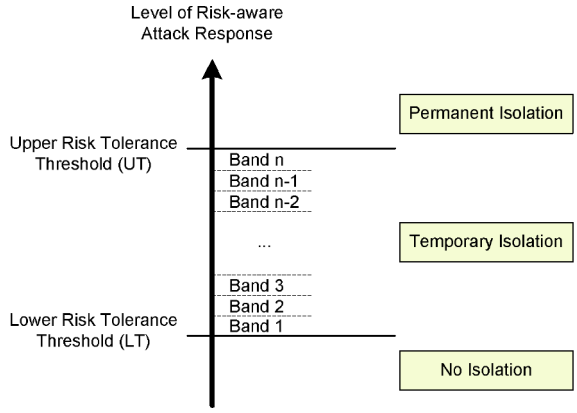
#### 4.3.2 .Combination of Evidences

For simplicity, we call the combined evidence for an attack, $E_A$ and the combined evidence for a countermeasure, $E_C$ . Thus, Bel$_A$ ðInsecureÞ and Bel$_C$ ðInsecureÞ represent risks of attack (Risk$_A$ ) and countermeasure (Risk$_C$ ), respectively. The combined evidences, $E_A$ and $E_C$ are defined in (15) and (16). The entire risk value derived from Risk$_A$ and Risk$_C$

### 4.4.Adaptive Decision Making

Our adaptive decision-making module is based on quantitative risk estimation and risk tolerance, which is shown in Fig. 3. 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 (18) and (19),

where n is the number of bands and i is the




We recommend the value of lower risk tolerance thresh-old 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, our 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 another factors, such as attack frequency. If the attack frequency is high, more severe response action should be taken to counter this attack. Our 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

## V. CASE STUDY AND EVALUATION

In this section, we first explain the methodology of our experiments and the metrics considered to evaluate the effectiveness of our approach. Then, we demonstrate the detailed process of our solution with a case study and also compare our risk-aware approach with binary isolation. In addition, we evaluate our solution with five random network topologies considering different size of nodes. The results show the effectiveness and scalability of our approach.

### 5.1 Methodology and Metrics

The experiments were carried out using NS-2 as the simulation tool from VINT Project [19] with UM-OLSR [20]. NS-2 is a discrete event network simulator which provides a detailed model of the physical and link layer behavior of a wireless network and allows arbitrary movement of nodes within the network. UM-OLS We computed six metrics [21] for each simulation run:

- Packet delivery radio. The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination.
- Routing cost. The ratio between the total bytes of routing packets transmitted during the simulation and the total bytes of packets received by the CBR sink at the final destination.
- Packet overhead. 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.
- Byte overhead. The number of transmitted bytes by routing packets, counting each hop similar to Packet Overhead.
- Mean latency. The average time elapsed from "when a data packet is first sent" to "when it is first received at its destination."
- Average path length. This is the average length of the paths discovered by OLSR. It was calculated by averaging the number of hops taken by each data packet to reach the destination.

### 5.2 Case Study

our case study scenario, where packets from Nodes 5 to 0 are supposed to go through Nodes 2 and 4. Suppose a malicious Node 1 advertises it has a direct link (fake link) to Node 0 and it would cause every node to update its own routing table accordingly. As a result, the packets from Nodes 5 to 0 traverse Node 1 rather than Nodes 2 and 4. Hence, Node 1 can drop and manipulate the traffic between Nodes 5 and 0. We assume, as Node 1's one-hop neighbors, both Node 0, Node 4, and Node 6 get the intrusion alerts with 80 percent confidence from their respective IDS modules.

We examine binary isolation approach, risk-aware approach with DRC, and risk-aware approach with DRCIF to calculate the response decisions for Nodes 0, 4, and 6. As shown in Table 1, binary isolation suggests all nodes to isolate the malicious one since it does not take countermeasure risk into account. With our risk-aware response mechanism based on our extended D-S theory, Node 1 should be isolated only by Node 0 while the original D-S theory would suggest that both Nodes 0 and 4 isolate Node 1. In Fig. 5a, due to routing attacks, the packet delivery ratio decreases in Stage 2. After performing binary isolation and DRC risk-aware response in Stage 3, the packet delivery ratio even decreases more. This is because these two

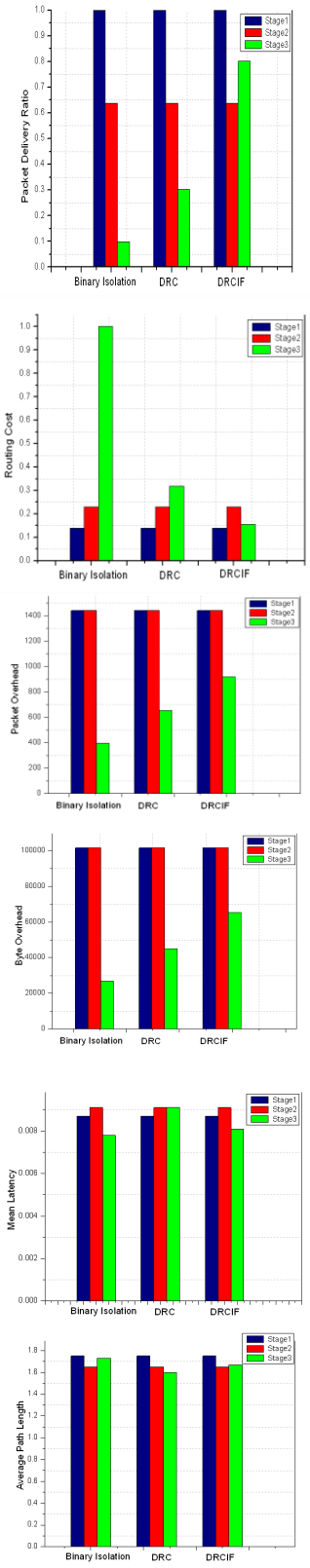



Fig. 5. Performance results in three stages comparing DRCIF with binary isolation and DRC.

response mechanisms largely destroy the topology of network. However, the packet delivery ratio using our DRCIF risk-aware response in Stage 3 is higher than those of the former two response mechanisms.

In Fig. 5b, the routing attacks increase the routing cost in Stage 2. Rather than recovering the routing cost in Stage 3, binary isolation and DRC risk-aware responses increase the routing cost. DRCIF risk-aware response, however, decreases the routing cost. Compared with other two response mechanisms, it indicates that our DRCIF risk-aware response effectively handles the attack. Figs. 5c and 5d show the packet and byte overhead,

respectively. Since the routing attacks do not change the network topology further in the given case, the packet overhead and byte overhead remain almost the same in Stage 2. In Stage 3, however, they are higher when our DRCIF risk-aware response mechanism is applied. This result meet our expectation, because the number of nodes which isolate malicious node using binary isolation and DRC risk-aware response are greater than those of our DRCIF risk-aware response mechanism. As shown in Table 1, the number of isolated nodes for each mechanism varies.

In Fig. 5e, as a consequence of the routing attacks, the mean latency increases in Stage 2. After response, we notice the mean latencies in Stage 3 for three different response mechanisms have approximately the same results. In Fig. 5f, the average path length decreases in Stage 2 due to the malicious action claiming a shorter path performed by Node 1. After response, the average path length using binary isolation is higher than those of the other two response mechanisms because more nodes isolated the malicious node based on the nature of binary isolation. Hence, some packets may be retransmitted by more hops than before.

### 5.3.Evaluation with Random Network Topologies

In order to test the effectiveness and scalability of our solution, we evaluated our risk-aware approach with DRCIF on five random network topologies. These five topologies have 10, 20, 30, 40, and 50 nodes respectively.

Fig. 6 shows the performance results in these random network topologies of our risk-aware approach with DRCIF, risk-aware approach with DRC and binary isolation approach. In Fig. 6a, as the number of nodes increases, the packet delivery ratio also increases because there are more route choices for the packet transmission. Among these three response mechanisms, we also notice the packets delivery ratio of our DRCIF risk-aware response is higher than those of the other two approaches.

In Fig. 6b, we can observe that the

routing cost of our DRCIF risk-aware response is lower than those of the other two approaches. Note that the fluctuations of routing cost shown in Fig. 6b are caused by the random traffic generation and random placement of nodes in our realistic simulation. In our DRCIF risk-aware response, the number of nodes which isolate the malicious node is less than the other two response mechanisms. As shown in Figs. 6c and 6d, that's the reason why we can also notice that as the number of nodes increases, the packet overhead and the byte overhead using our DRCIF risk-aware response are slightly higher than those of the other two response mechanisms.

In Fig. 6e, the mean latency using our DRCIF risk-aware response is higher than those of the other two response mechanisms, when the number of nodes is smaller than 20. However, when the number of nodes is greater than 20, the mean latency using our approach is less than those of the other two response mechanisms.

## VI. RELATED WORK

Intrusion detection and response in MANET. Some research efforts have been made to seek preventive solutions [21], [22], [23], [24] for protecting the routing protocols in MANET. 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 signatured based and anomaly- based IDS models for the wired network, IDSs for MANET use specification-based or statistics-based approaches. Specification-based approaches, such as DEMEM [25] and [26], [27], [28], monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. On the other hand, statistics-based approaches, such as Watchdog [29], and [30], 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. Intrusion response system (IRS) [31] for MANET is inspired by MANET IDS. In [1] and [2], malicious nodes are isolated based on their reputations. Their work fails to take advantage of IDS alerts and simple isolation may cause unexpected network partition. Wang et al. [4] brought the concept of cost-sensitive intrusion response which considers topology dependency and attack damage. The advantage of our solution is to integrate evidences from IDS, local routing table with expert knowledge, and countermeasures[40] with a mathematical reasoning approach.

Riska-ware approaches. When it comes to make response decisions [32], [33], there always exists inherent uncertainty which leads to unpredictable risk, especially in security and intelligence arena. Risk-aware approaches are introduced to tackle this problem by balancing action benefits and damage trade-offs in a quantified way. Cheng et al. [3] presented a fuzzy logic control model for adaptive risk-based access control. Teo et al. [34] applied dynamic risk-aware mechanism to determine whether an access to the network should be denied or permitted.

However, risk assessment is still a nontrivial challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Wang et al. [4] proposed a naïve 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. Mu et al. [7] adopted Dempster-Shafer theory to measure the risk of attacks and responses. However, as identified in [8], their model with Dempster's rule treats evidences equally without differentiating them from each other. To address this limitation, we propose a new Dempster's rule of combination with a notion of importance factors in D-S evidence model.

## VII. EXSISTING SYSTEM

Due to their unique characteristics, MANETs are suffering from a wide range of security threats and attacks. Among numerous possible routing attacks, the denial of service (DoS) attacks, especially the distributed denial of service (DDoS) attacks (e.g. route request flooding attack), acts as a major threat to ad hoc networks. In this paper, a behavior based reputation mechanism is proposed to identify the flooding malicious nodes in the network. Reputation of a node is the measure of its behavior in the network. The devices are restricted to send RREQs on the basis of their behavior in the network. This flooding resistance scheme can adapt to the changing trends of the node behavior. Based on the reputation value of each node, their neighboring nodes limit the RREQ packets sent by that node. If genuine node starts acting as a fake node, then its neighbors steadily block

the RREQ packets from that node. Similarly, if a malicious node decides to become genuine, then its neighbors steadily allow it to send more RREQ packets. Because of the dual nature of this scheme, it successfully rectifies false detection of genuine nodes as malicious ones. In the proposed algorithm we have assumed that while sending route reply though any malicious node, the node will maintain integrity of the route reply information passes through it. Further research can be done without such assumptions.

## VIII. Proposed future work

In the proposed mechanism, devices are restricted to send RREQs on the basis of their behavior in the network. *Reputation value is the measure of a node's behavior in the network*. Reputation of a node is defined as the ratio of the number of successful RREQs to the total number of RREQs sent by it in that network. Each node maintains the reputation values of each of its neighbors in its own routing table. The maximum number of RREQs sent by any node is proportional to the reputation value of the node maintained by its neighbors. Higher the count of successful RREQ transmissions by a node, higher is its reputation value and higher is the maximum number of RREQs it can send. For a malicious node, the reputation value is less and eventually the rate at which it can send RREQs will also be very less. Thus its maliciousness can be curbed. Similarly, for a genuine node, the reputation value is high and hence the rate at which it can send RREQs will also be high. Thus, genuine devices with high data transfer requirements are not forced to suffer.

**REPUTATION MANAGEMENT**

Reputation of *A* is calculated as follows:$\alpha$A/$\beta$A

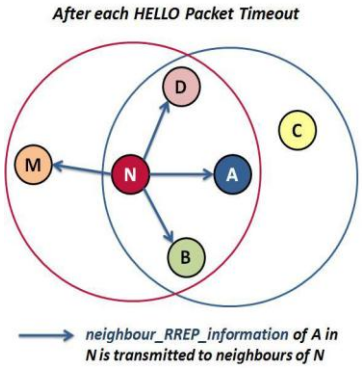



Figure 1. N *broadcasts neighbor_RREP_information* of *A*

*Flooding Resistance Algorithm*

***Case 1***

After each Hello packet interval
{If there is a recent Reputation Update timeout
{For each node Ni
{Add current neighbor_RREP_information of Ni along with updated neighbor_RREP_information received by Ni from each of its neighbors A to the Hello packet header of Ni and broadcast it to all its one hop neighbors A;}}
Else
{For each node Ni
{Add current neighbor_RREP_information of Ni to the Hello packet header of Ni and broadcast it to all its one hop neighbors A;
}}}

***Case 2:***

After each Hello packet received by Ni from each of its one-hop neighbor A
{ If there is a recent Reputation Update timeout
{ For each neighbor node A
{ Update current neighbor_RREP_information of A;
Obtain as much neighbor_RREP_information available from the Hello packets of each neighbor A and update communicated_RREPs of the neighbor table;
Calculate:
A →□ current neighbor_RREP_information of A + communicated_RREPs of A;
Recompute RA;
If RA < RTh
{ Declare A as malicious and broadcast an alarm about A along with RA throughout the network; }
If RA == 0, make RA = 0.1;}}
Else
{ For each neighbor node A
{Store/update neighbor_RREP_information of A;}}}

***Case 3:***

For every new neighbor B of Ni
{ If B is new in the network
{ New entry is made for B in the neighbor table of Ni;
Observe B's behavior for Tobs-time and calculate RB after Trep-upd timeout;}
Else if B has relocated from another position of the same network
{ New entry is made for B in the neighbor table of Ni;
If B is declared as malicious by its previous neighbors
{ RB ←□ RB as broadcasted by B's former neighbors via alarm; }
Else
{ Observe B's behavior for Tobs-time and calculate RB after Trep-upd timeout; }}}}

***Case 4:***

For every RREQ received by Ni from neighbor A
{ If RREQs received from A in current second > RA * MAX_RREQ
{ Block current RREQ and increase

corresponding A value; }
Else
{ Forward RREQ;Increase corresponding A value;
If this RREQ is acknowledged by RREP through Ni
{Increase neighbor_RREP_information of A in Ni; }}}

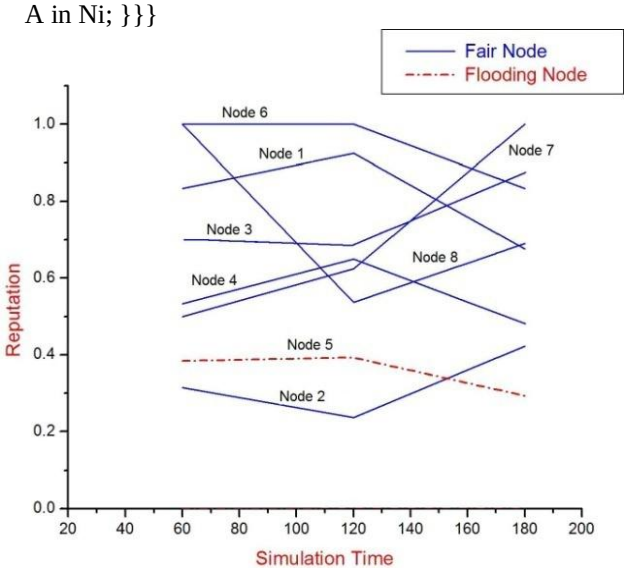



Fig: Variation of Nodes' Reputation vs. Time

## IX. CONCLUSION

We have proposed a risk-aware response solution for mitigating MANET routing attacks. Especially, our approach considered the potential damages of attacks and counter-measures. In order to measure the risk of both attacks and countermeasures, we extended Dempster-Shafer theory of evidence with a notion of importance factors. Based on several metrics, we also investigated the performance and practi-cality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our risk- aware approach. Based on the promising results obtained through these experiments, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

## REFERENCES

[1] 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.

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

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

[4] 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.

[5] 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.

[6] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET):Routing Protocol Performance Issues and Evaluation Considerations",Internet Request for comment RFC 2501, Jan 1999.

[7] Muhammad O Pervaiz, Mihaela Cardei and Jei Wu, "Routing security in ad hoc wireless networks", Department of Computer Science and Engg, Florida Atlantic University, Boca Raton, FL 33431.

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.

[9] R. H. Khokhar, M. A. Ngadi, S. Mandala, "A Review of Current Routing Attacks In Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Volume 2, Issue 3, pp. 18-29,June 2008.

[10] Prasenjit Choudhury, Subrata Nandi, Anita Pal, Narayan C. Debnath Mitigating Route Request Flooding Attack in MANET using Node Reputation "Performance Issues and Evaluation Considerations", Internet Request for comment RFC 2501, Dec 2012.

[11] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", Internet Request for comment RFC 2501, Jan 1999.

[12] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Proc. of Wireless Communications, IEEE, Oct 2007, Issue 5, pgs 85-91.

[13] R. H. Khokhar, M. A. Ngadi, S. Mandala, "A Review of Current Routing Attacks In Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Volume 2, Issue 3, pp. 18-29, June 2008.

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

[15] 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.

[16] 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.

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

[18] L. Zadeh, "Review of a Mathematical Theory of Evidence," AI Magazine, vol. 5, no. 3, p. 81, 1984.

[19] R. Yager, "On the Dempster-Shafer Framework and New Combination Rules 1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.