www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 3 March 2013 Page No. 605-614

REDUCING ATTACK FREQUENCY IN MANET ROUTING

Janaranjani.C, Kavieyanchale.R, Muthusamy.A, Nataraj.S, Krishnakumar.R
Final Year, Department of Computer Science and Engineering
K.S.R College of Engineering,

Mrs.V.Sharmila, M.E,[Ph.D].,
Associate professor, Department of Computer Science and Engineering,
K.S.R College of Engineering,

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.

Index Terms—Mobile ad hoc networks, intrusion response, risk aware, dempster-shafer theory.

1 INTRODUCTION

MOBILE Adhoc 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. 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.

The major contributions of this paper are summarized as follows: 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. 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.

2 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 Adhoc 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 seriousnetwork dysfunctions.

3 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. **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.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. 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 $\sum m(A)=1$ (1) and $\sum m(A)=1$ (2)

According to [5], a function $Bel:2^{\theta} \rightarrow [0,1]$,a belief function over θ if it is given by (3) for some basic probability assignment $m:2^{\theta}\rightarrow[0,1]$

$Bel(A)=\sum m(B)$ 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 $m : 2^{\theta}\rightarrow[0,1]$; defined by $m(\theta)=0$ and

$m(C)=(\sum A_i \cap B_j = C m_i (A_i) m_2 (B_j))/(1-\sum A_i \cap B_j=\Phi m_1(A_i)m_2(B_j))$ (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.

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. Property 1. No belief ought to be committed to in the result of our combination rule

$m'(\Phi)=0$ (5)

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

$\sum m'(A)=1$ (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 $A \epsilon \theta$, where m(A) is the original Dempster'sCombination Rule.

Property 4. Importance factors of each evidence must not beexchangeable

$m'(A_1, IF1, IF2) \neq m'(A,IF2,IF1)$ if $(IF1 \neq IF2)$ (8)

3.3 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:

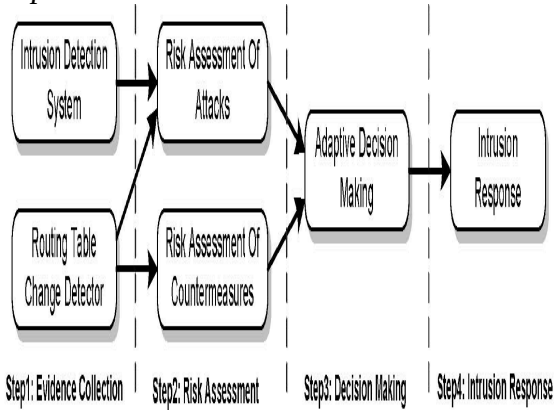


Fig. 1. Risk-aware response mechanism.

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 jEpj ¼ sizeof(Ep);
2 While jEpj > 1 do
3 Pick two evidences with the least IF in Ep, named E1 and E2;
4 Combine these two evidences,
E =<m1 Θm2, (IF1 + IF2)/2>;
5 Remove E1 and E2 from Ep;
6 Add E to Ep;
7 end
8 return the evidence in Ep

4 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 moreaccurate 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 riskaware 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 table changing information would be further considered an 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. 1. Risk-aware response mechanism.

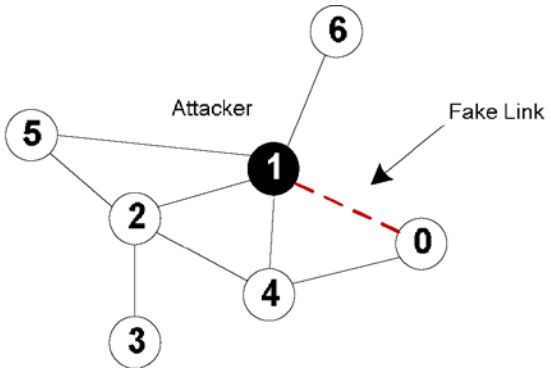


Fig. 2. Example scenario.

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.

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.

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.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. The basic probability assignments of Evidence 1 are based on three equations given below:

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. 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. Fig. 2. Example scenario.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

4.3.2 Combination of Evidences

For simplicity, we 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 in (15) and(16). The entire risk value derived from RiskA and RiskC is given in (17)

EA = E1 ΘE2 Θ E3 Θ E4 ΘE5 (15)

EC=E2 ΘE4 Θ E5 (16)

where Θ is Dempster's rule of combination with important factors defined in Theorem 1

Risk = RiskA _ RiskC = BelA(Insecure) _ BelC(Insecure) (17)

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 theisolation 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 corresponding isolation band

I= [[risk-LT/UT-LT]*n], Risk ϵ (LT,UT)(18)

T=100*i(milliseconds) (19)

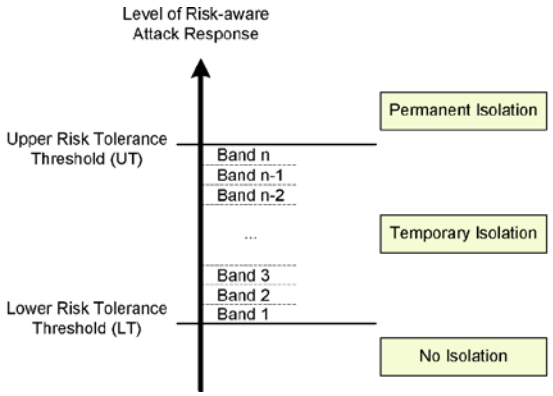


Fig. 3. Adaptive decision making.

We recommend the value of lower risk tolerance threshold 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.

5 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-OLSR is implementation of Optimized Link State Routing protocol for the NS-2, which complies with [12] and supports all core functionalities of OLSR plus the link-layer feedback option.In our experiments, we constructed MANET scenarios in a topology of 1,000 m _1,000 m area. The total simulation time was set to 1,200 seconds, and the bandwidth was set to 2 Mbps. Constant Bit Rate (CBR) traffic was used to send 512 byte-UDP packets between nodes. The queuing capacity of every node was set to 15. We adopted a random traffic generator in the simulation that chose random pairs of nodes and sent packets between them. Every node kept track of all packets sent by itself and the entire packet received from other nodes in the network.In order to evaluate the effectiveness of our adaptive risk-aware response solution, we divided the simulation process into three stages and compared the network performance in terms of six metrics. The following describes the activities associated with each stage:

Stage 1—Before attack. Random packets were generated and transmitted among nodes without activating any of them as attackers. This simulation can present the traffic patterns under the normal circumstance.

Stage 2—After attack. Specific nodes were set as attackers which conducted malicious activities for their own profits.However, any detection or response is not available in this stage. This simulation process can present the traffic patterns under the circumstance with malicious activities.

Stage 3—After response. Response decisions for each node were made and carried out based on three different mechanisms.We computed six metrics [21] for each simulation run:

Packet delivery ratio. 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.

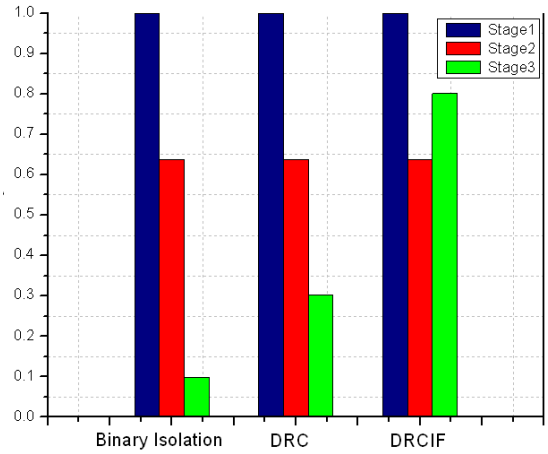
Byte overhead. The number of transmitted bytes by routing packets, counting each hop similar to Packet Overhead.

Mean latency. The average time elapsed from "when a data packet is first sent" to "when it is first received at its destination."

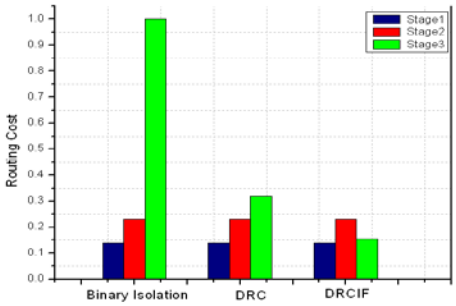
Average path length. This is the average length of the paths discovered by OLSR. It was calculated by averaging the number of hops taken by each data packet to reach the destination.

5.2 Case Study

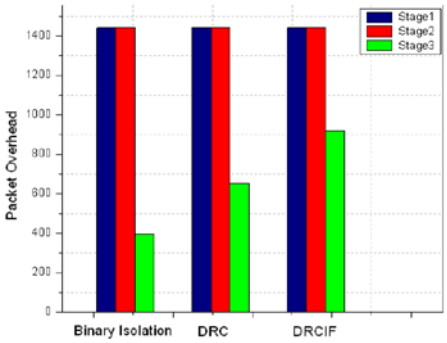
Fig. 2 shows our case study scenario, where packets from Nodes 5 to 0 are supposed to go through Nodes 2 and 4. Suppose a malicious Node 1 advertises it has a direct link (fake link) to Node 0 and it would cause every node to update its own routing table accordingly. As a result, the packets from Nodes 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. Figs. 4a, 4b 4c show the routing tables of Nodes 0, 4, and 6 before the attack, after the attack and after the isolation, respectively. We set a = 0.2,b =0.7, c = 0.8, d = 0.05, IF1 = 5, IF2 = 7, IF3=10,IF4 =3, IF5 =3, LT =-0.0017, UT =1, and n = 5 in our experiments.



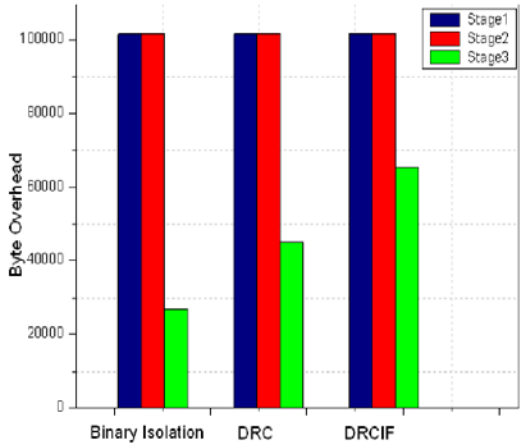
a)Packet Delivery Ratio



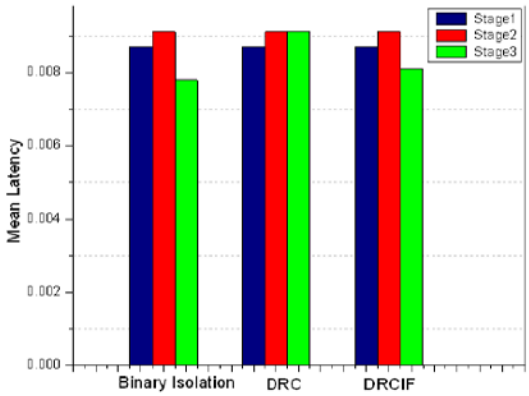
b)Routing cost



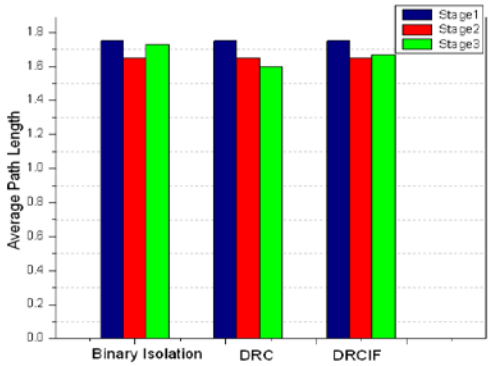
c)Packet Overhead



d)Byte Overhead(Bytes)



e)Mean Latency(Seconds)



f)Average path Length

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 Node1.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. 4. Routing tables.TABLE 1Risk Assessment and Decision Making 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.

5.3 Evaluation with Random Network Topologies

In order to test the effectiveness and scalability of our solution, we evaluated our risk-aware

6 RELATED WORK

Intrusion detection and response in MANET. Someresearch 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 anomalybased 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 .

Risk-aware 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. Chenget al. [3] presented a fuzzy logic control model for adaptiverisk-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

CONCLUSION

We have proposed a risk-aware response solution for reducing MANET routing attacks. Especially, our approach considered the potential damages of attacks and countermeasures.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 practicality of our approach and the experiment results clearly demonstrated the effectiveness and scalability of our riskaware 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] 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.