This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

Risk-Aware Response for Mitigating MANET Routing Attacks

Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu
Laboratory of Security Engineering for Future Computing (SEFCOM)
Arizona State University, Tempe, AZ 85281, USA
{zmzhao, hxhu, gahn, ruoyu.wu}@asu.edu

***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 Dempster-Shafer mathematical theory of evidence introducing a notion of *importance factor*. In addition, our experiments demonstrate the effectiveness of our approach with the consideration of the packet delivery ratio and routing cost.**

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.

Several work [22], [12] addressed the intrusion response actions in MANET by isolating uncooperative nodes in terms of the node reputation derived from their behaviors. Such a simple binary isolation 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 non-trivial 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 [24] 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 Dempster-Shafer mathematical theory of evidence (D-S theory), which offers an alternative to traditional probability theory for representing uncertainty [18].

D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems [19], [14] and by other engineering fields [2], 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 to combine several evidences together with probable reasoning. However, as identified in [17], Dempster's rule treats evidences equally without differentiating their priorities. To address this limitation, we introduce a new Dempster's rule of combination with a notion of *importance factor* 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). In addition, we attempt to demonstrate the effectiveness of our solution considering the following two factors, *packet delivery ratio* and *routing cost*.

The rest of this paper is organized as follows. Section II overviews MANET routing protocols and attacks against them including the related work. Section III describes how *importance factors* can be integrated in our extended D-S evidence model. Section IV presents the details of our risk-aware response mechanism. The evaluations of our solution are discussed in Section V. Section VI concludes this paper.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

II. Related Work

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 the two major categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as Ad hoc On Demand Distance Vector (AODV) protocol [15], 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 [4], nodes obtain routes by periodic exchange of topology information with other nodes and maintain route information all the time.

Based on the behavior of attackers, attacks against MANET can be classified into passive or active attacks. Attacks can be further categorized as either outsider or insider attacks. With respect to the target, attacks could be also divided into data packet or routing packet attacks. In routing packet attacks, attackers could not only prevent existing paths from being used, but also spoof non-existing paths to lure data packets to them. Several studies [7], [9], [10], [11] 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.).

Some research efforts have been made to seek preventive solutions [8], [6] 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 for defending from malicious insiders who possess the credentials to communicate in the network.

Numerous intrusion detection systems (IDS) 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 wired network, IDS for MANET use specification-based approaches and statistics-based approaches. Specification-based approaches, for example DEMEM [21], C. Tseng et al. [20] and M. Wang et al. [23], 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 [13] and Lipad [1], 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 systems (IRS) for MANET are inspired by MANET IDS. [22], [12] isolate malicious nodes based on their reputations. Their work fails to take advantage of IDS alerts and simple isolation of nodes may cause unexpected network partition. [24] brings the concept of cost-sensitive into MANET intrusion response which considers topology dependency and attack damage. The advantage of our solution is that we integrate evidences from IDS, local routing table with expert knowledge to estimate risk of attacks, and countermeasures with a mathematical reasoning approach.

III. Extended Dempster-Shafer Theory of Evidence

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

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 $\langle m, IF\rangle$, where m describes the basic probability assignment [18]. Basic probability assignment function m is defined as follows:

$$m(\phi) = 0 \tag{1}$$

and

$$\sum_{A\subset\Theta} m(A) = 1 \tag{2}$$

According to [18], a function $Bel : 2^{\Theta} \rightarrow [0, 1]$ is a belief function over Θ if it is given by (3) for some basic probability assignment $m : 2^{\Theta} \rightarrow [0, 1]$.

$$Bel(A) = \sum_{B\subset A} m(B) \tag{3}$$

$Bel(A)$ 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 (DRC), which is given by (4), enables us to compute the orthogonal sum, which describes the combined evidence.

Suppose Bel_1 and Bel_2 are belief functions over the same frame Θ, with basic probability assignments m_1 and m_2. Then the function $m : 2^{\Theta} \rightarrow [0, 1]$ defined by $m(\phi) = 0$ and

$$m(C) = \frac{\sum_{A_i \bigcap B_j = C} m_1(A_i)m_2(B_j)}{1 - \sum_{A_i \bigcap B_j = \phi} m_1(A_i)m_2(B_j)} \tag{4}$$

for all non-empty $C \subset \Theta$, $m(C)$ is a basic probability assignment which describes the combined evidence.

DEFINITION 3. Extended D-S evidence model with importance factors: Suppose $E_1 = \langle m_1, IF_1\rangle$, $E_2 = \langle m_2, IF_2\rangle$ are two independent evidences. Then, the combination of E_1 and E_2 is $E = \langle m_1 \oplus m_2, (IF_1 + IF_2)/2\rangle$, where $\oplus$ is Dempster's rule of combination with *importance factors*.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

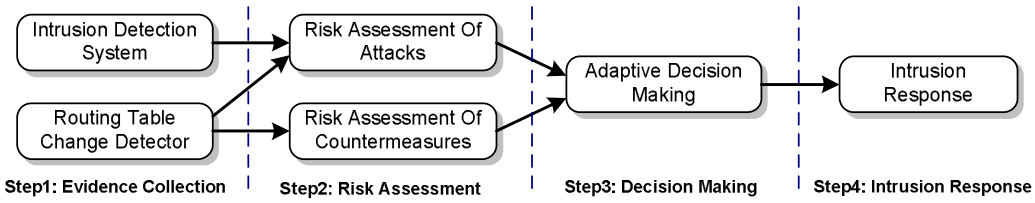


Fig. 1: Risk-Aware Response Mechanism

THEOREM 1. Dempster's Rule of Combination with Importance Factors (DRCIF): Suppose Bel_1 and Bel_2 are belief functions over the same frame of discernment Θ, with basic probability assignments m_1 and m_2. The *importance factors* of these evidences are IF_1 and IF_2. Then the function $m' : 2^{\Theta} \rightarrow [0, 1]$ defined by

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

and

$$m'(C, IF_1, IF_2) = \frac{\sum_{A_i \bigcap B_j = C} [m_1(A_i)^{\frac{IF_1}{IF_2}} \cdot m_2(B_j)^{\frac{IF_2}{IF_1}}]}{\sum_{C \subset \Theta, C \neq \phi} \sum_{A_i \bigcap B_j = C} [m_1(A_i)^{\frac{IF_1}{IF_2}} \cdot m_2(B_j)^{\frac{IF_2}{IF_1}}]}$$

for all non-empty $C \subset \Theta$, m' is a basic probability assignment for the combined evidence.

In order to make the result of combination consistent with multiple evidences, we also introduce a combination algorithm. The complexity of our algorithm is $O(n)$, where n is the number of evidences. It indicates our extended Dempster-Shafer theory demands no extra computational cost compared to naïve fuzzy method.

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 III for both attacks and corresponding countermeasures to make more accurate response decisions. Our risk-aware response mechanism is illustrated in Figure 1.

A. 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 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, binary node isolation response may result in negative impacts to the routing operations, even bringing more routing damages than the attack itself. 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 IV-C.

B. 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 $\{\phi$, {Secure}, {Insecure}, {Secure, Insecure}$\}$. Then $Bel\{Insecure\}$ is used to represent the risk of MANET.

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 ($Risk_A$) and countermeasure ($Risk_C$).

We take the confidence level of alerts from IDS as the subjective knowledge in *Evidence 1*. In terms of objective evidences, 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 entry to be missed, or any item of routing table entry to be changed. We illustrate the possible cases of routing table change and analyze the degrees of damage in *Evidences 2* to *5*.

Evidence 1: Alert Confidence. The confidence of attack detection is provided by the IDS to address the possibility of the attack occurrence. Since the false alarm is a serious problem for most IDS, 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 (5)–(7):

$$m(Insecure) = c, c\ is\ confidence\ given\ by\ IDS \quad (5)$$

$$m(Secure) = 1 - c \quad (6)$$

$$m(Secure, Insecure) = 0 \quad (7)$$

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 routing table 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 Equations 8, 9 and 10. Equations 8, 9 and 10 are piece-wise linear functions, where *a*, *b*, *c*, and *d* are constant thresholds and determined by experts.

$$m(Insecure) = \begin{cases} d & x \in [0, a] \\ (\frac{1-2d}{c-a})(x-a) & x \in (a, c] \\ 1-d & x \in (c, 1] \end{cases} \quad (8)$$

$$m(Secure) = \begin{cases} 1-d+(\frac{2d-1}{b})x & x \in [0, b] \\ d & x \in (b, 1] \end{cases} \quad (9)$$

$$m(Sec, Insec) = \begin{cases} \frac{1-2d}{b}x & x \in [0, a] \\ d - \frac{2d-1}{b}x - (\frac{1-2d}{c-a})(x-a) & x \in (a, b] \\ 1-b-(\frac{1-2d}{c-a})(x-a) & x \in (b, c] \\ 0 & x \in (c, 1] \end{cases} \quad (10)$$

2) Combination of Evidences: For simplicity, we call the combined evidence for attack, E_A and the combined evidence for countermeasure, E_C. Thus, $Bel_A(Insecure)$ and $Bel_C(Insecure)$ represent risks of attack ($Risk_A$) and countermeasures ($Risk_C$), respectively. The combined evidences, E_A and E_C are defined in Equations 11 and 12. The entire risk value derived from $Risk_A$ and $Risk_C$ is given in Equation 13.

$$E_A = E_1 \oplus E_2 \oplus E_3 \oplus E_4 \oplus E_5 \quad (11)$$

$$E_C = E_2 \oplus E_4 \oplus E_5 \quad (12)$$

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

$$Risk = Bel_A(Insecure) - Bel_C(Insecure) \quad (13)$$

C. Adaptive Decision Making

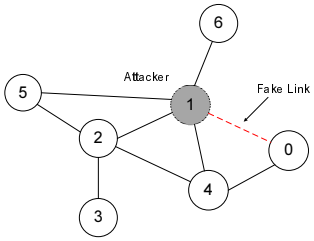
Our adaptive decision making module is based on quantitative risk estimation and risk tolerance. The response level is additionally divided into multiple bands. Each band is associated with an isolation degree, which presents a different time period of the isolation action. The response action and band 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 are associated with the temporary isolation response, in which the isolation time (T) changes dynamically based on the different response level given by Equations 14 and 15, where n is the number of bands and i is the corresponding isolation band.

$$i = \lceil \frac{Risk - LT}{UT - LT} \times n \rceil,\ Risk \in (LT, UT) \quad (14)$$

$$T = 100 \times i\ (milliseconds) \quad (15)$$

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, IRS can intuitively adjust the risk tolerance thresholds accordingly. In the case that LT is set less than 0, even if the risk of attack is not greater than the risk of isolation, IRS might 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.



(a) Attack Scenario

Des	Next	Dis
1	4	2
2	4	2
3	4	3
4	4	1
5	4	3
6	4	3

Before attack

Des	Next	Dis
1	1	1
2	1	2
3	1	3
4	4	1
5	1	2
6	1	2

After attack

Des	Next	Dis
2	4	2
3	4	3
4	4	1
5	4	3

After isolation

(b) Routing Table of Node 0

Des	Next	Dis
0	0	1
1	1	1
2	2	1
3	2	2
5	2	2
6	1	2

Before attack

Des	Next	Dis
0	0	1
1	1	1
2	2	1
3	2	2
5	2	2
6	1	2

After attack

Des	Next	Dis
0	0	1
2	2	1
3	2	2
5	2	2

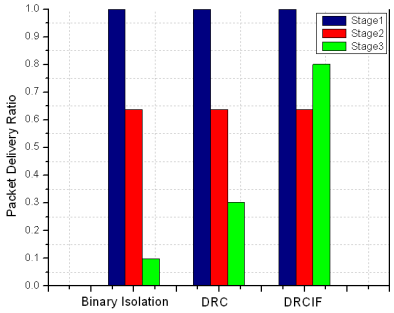
After isolation

(c) Routing Table of Node 4

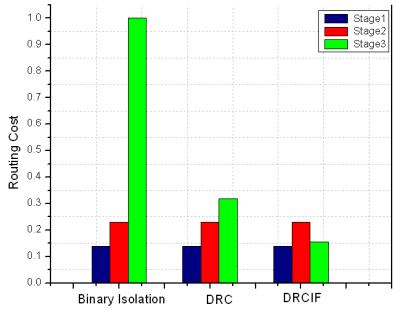
Fig. 2: Attack Scenario and Relevant Routing Tables

TABLE I: Risk Assessment

Node Number	$Bel_A^{DRC}(I)$	$Bel_C^{DRC}(I)$	$Bel_A^{DRCIF}(I)$	$Bel_C^{DRCIF}(I)$	$Risk^{DRC}$	$Risk^{DRCIF}$
0	0.00011	0.00164	0.467	0.0136	-0.00153	0.4534
4	5.7e-6	0.00164	0.00355	0.0136	-0.00163	-0.01005

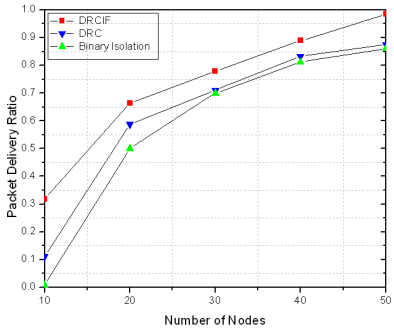


(a) Packet Delivery Ratio in Three Stages

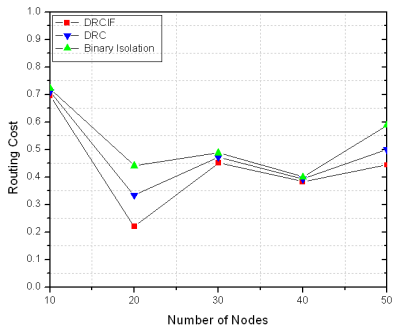


(b) Routing Cost in Three Stages

Fig. 3: Packet Delivery Ratio & Routing Cost in Three Stages



(a) Packet Delivery Ratio



(b) Routing Cost

Fig. 4: Packet Delivery Ratio & Routing Cost in Response Mechanisms: Binary Isolation, DRC and DRCIF

V. Case Study and Evaluation

Figure 2(a) shows our case study scenario, where packets from Node 5 to Node 0 are supposed to go through Node 2 and Node 4. Supposing a malicious Node 1 advertises it has a direct link (fake link) to Node 0, every node updates its own routing table accordingly. As a result, the packets from Node 5 to Node 0 traverse Node 1 rather than Node 2 and Node 4. Hence, Node 1 can manipulate the traffic between nodes. We assume, as Node 1's one-hop neighbors, both Node 0 and Node 4 get the intrusion alerts with confidence of 80% from their respective IDS modules. Figures 2(b)-(c) show the routing tables of Node 0 and Node 4 before the attack, after the attack and after the isolation, respectively. We set $a = 0.2$, $b = 0.7$, $c = 0.8$, $d = 0.05$, $IF_1 = 5$, $IF_2 = 7$, $IF_3 = 10$, $IF_4 = 3$, $IF_5 = 3$, $LT = 0$, and $UT = 1$ in our experiments. As shown in Table I, Node 1 is isolated by Node 0 based on risk assessment mechanism with our extended D-S theory, while the original D-S theory keeps Node 1 for both Node 0 and Node 4.

Our experiments adopted NS-2 simulation tool based on the

practices from VINT Project [5] with UM-OLSR [16]. *Packet Delivery Ratio* and *Routing Cost* are chosen as evaluation metrics. *Packet Delivery Ratio* is the ratio between the number of packets originated by sources and the number of packets received by destinations. *Routing Cost* is the ratio between the total bytes of routing packets transmitted and the total bytes of packets received by destinations. In order to evaluate the effectiveness of our adaptive risk-aware response mechanism, we compared the difference between attacks with response and attacks without response in three stages: *Stage1* (before the attack), *Stage2* (after the attack) and *Stage3* (after the response). Furthermore, we compared three response mechanisms: binary isolation, DRC risk-aware and DRCIF risk-aware responses.

In Figure 3(a), due to routing attacks, the packet delivery ratio decreases in the *Stage2*. After using binary isolation and DRC risk-aware response in *Stage3*, the packet delivery ratio even decreases more. This is because these two response mechanisms largely destroy the topology of network. However, the packet delivery ratio using our proposed DRCIF risk-aware response in *Stage3* is higher than those of the former two response mechanisms. In Figure 3(b), the routing attacks increase the routing cost in *Stage2*. Rather than recovering the routing cost in *Stage3*, 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 our DRCIF risk-aware response effectively handles the attack.

From Figure 4(a), as the number of nodes increases, the packet delivery ratio also increases because there are more route choices for the packet transmission. Moreover, among these three response mechanisms, we can notice the packets delivery ratio of our DRCIF risk-aware response is higher than those of the other two approaches. From Figure 4(b), we can also 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 Figure 4(b) are caused by the random traffic generation and random placement of nodes which may have more influence on the routing cost.

VI. Conclusion

We have proposed a risk-aware response solution for the mitigation of MANET routing attack considering 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 factor*. The experiment results demonstrated the effectiveness and scalability of our risk-aware approach. Based on the promising results obtained through these experiments, we would seek more systematic way to consider node reputation and attack frequency in our adaptive decision model.

Acknowledgments

This work was partially supported by the grants from National Science Foundation (NSF-IIS-0900970 and NSF-CNS-0831360) and Department of Energy (DE-SC0004308 and DE-FG02-03ER25565).

References

[1] F. Anjum and R. Talpade. Lipad: lightweight packet drop detection for ad hoc networks. In *2004 IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall*, pages 1233–1237, 2004.

[2] O. Basir and X. Yuan. Engine fault diagnosis based on multi-sensor information fusion using Dempster–Shafer evidence theory. *Information Fusion*, 8(4):379–386, 2007.

[3] P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger. Fuzzy MLS: An Experiment on Quantified Risk-Adaptive Access Control. In *IEEE Symposium on Security and Privacy*, volume 2007. Citeseer, 2007.

[4] T. Clausen and P. Jacquet. RFC3626: Optimized Link State Routing Protocol (OLSR). *RFC Editor United States*, 2003.

[5] K. Fall and K. Varadhan. The ns manual-the VINT project. *University of California, Berkeley, Calif, USA*, 2001.

[6] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1):175–192, 2003.

[7] Y. Hu and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security and Privacy magazine*, 2:28–39, 2004.

[8] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Wireless Networks*, 11(1):21–38, 2005.

[9] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto. A study of a routing attack in OLSR-based mobile ad hoc networks. *International Journal of Communication Systems*, 20(11):1245–1261, 2007.

[10] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour. A collusion attack against olsr-based mobile ad hoc networks. In *GLOBECOM*, 2006.

[11] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour. A Survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications*, page 86, 2007.

[12] J. Liu and V. Issarny. Enhanced Reputation Mechanism for Mobile Ad Hoc Networks. *LECTURE NOTES IN COMPUTER SCIENCE*, pages 48–62, 2004.

[13] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–265. ACM, 2000.

[14] C. Mu, X. Li, H. Huang, and S. Tian. Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory. In *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security*, page 48. Springer, 2008.

[15] C. Perkins, E. Belding-Royer, and S. Das. RFC3561: Ad hoc on-demand distance vector (AODV) routing, 2003.

[16] F. Ros. UM-OLSR implementation (version 0.8.8) for NS2, 2007.

[17] K. Sentz and S. Ferson. Combination of evidence in Dempster-Shafer theory. *Report No. SAND2002*, 835, 2002.

[18] G. Shafer. *A mathematical theory of evidence*. Princeton university press Princeton, NJ, 1976.

[19] L. Sun, R. Srivastava, and T. Mock. An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, 22(4):109–142, 2006.

[20] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt. A Specification-Based Intrusion Detection Model for OLSR. *LECTURE NOTES IN COMPUTER SCIENCE*, 3858:330, 2006.

[21] C. Tseng, S. Wang, C. Ko, and K. Levitt. Demem: Distributed evidence-driven message exchange intrusion detection model for manet. In *Recent Advances in Intrusion Detection*, pages 249–271. Springer, 2006.

[22] T. View. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):305–317, 2006.

[23] M. Wang, L. Lamont, P. Mason, and M. Gorlatova. An effective intrusion detection approach for OLSR MANET protocol. In *Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on*, pages 55–60, 2005.

[24] S. Wang, C. Tseng, K. Levitt, and M. Bishop. Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks. *LECTURE NOTES IN COMPUTER SCIENCE*, 4637:127, 2007.