ISSN 2319 – 1953
International Journal of Scientific Research in Computer Science Applications and Management Studies

Mitigating Routing Attacks with Evidence Algorithm

Ms. G.Nirmala[#1] Mrs. T. Kalaiselvi[*2]

#1 M.E (CSE) Second Year, Erode Sengunthar Engineering College,Erode,Tamil Nadu,India

**2 Assistant Professor (SG), CSE Department, Erode Sengunthar Engineering College, Erode, Tamil Nadu, India*

[1]gnirmalacs17@gmail.com

[2] kalai.selvi.t@gmail.com

Abstract—**Mobile Ad hoc Networks (MANET) are having dynamic nature of its network infrastructure and it is vulnerable to all types of attacks. Between these attacks, the routing attacks getting more attention because it's changing the whole topology it and it causes more damage to MANET. Still there are lot of intrusion detection Systems available to diminish those critical attacks, existing system detect the malicious nodes only on binary or naïve fuzzy decisions response. Even though , it may result in the unexpected network partition, and reasons additional damages to the infrastructure of the network , and it leads to uncertainty in finding routing attacks in MANET. In this paper, we offer an adaptive risk-aware response mechanism with extended Dempster-Shafer theory in MANET to identify the routing attacks and malicious node. Our technique is finds the malicious node with degree of evidence or degree of belief from the expert knowledge and decisions and detect the important factors for each node. It creates black list and all those malicious nodes so that it may not enter the network again.**

Key words: **Mobile Adhoc Network, Black list, Aodv, Dempster Shafer theory**

I. INTRODUCTION

MOBILE Ad hoc Networks (MANET) does not have a predefined infrastructure or centralized administration and thus introduces a communication in all environments. Therefore, MANET is suitable for all types of environment where central access point is not needed. Furthermore, in MANET, every mobile node plays a router role while they are transmitting data in the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since its consequences would propagate in performing routing tasks. The specific characteristic of MANET is the dynamic nature of its network topology that is frequently and continuously changing due to the sudden movement of nodes

Many work, isolated the nodes that are not cooperative addressed by the intrusion response actions in MANET by, based on the node reputation derived from their behaviours. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET, we introducing a new extended Dempster's rule of combination with a notion of importance factors (IF) in D-S evidence model.

In this paper, a risk-aware response mechanism is proposed to systematically cope with routing attacks scenario; the improper countermeasures may cause the unexpected network partition, and thus brings additional damages to the network infrastructure. More flexible and adaptive response should be investigated to address the above-mentioned critical issues. The notion of risk can be adopted to support more adaptive responses to routing attacks in MANET. AODV 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.

However, risk assessment is still a nontrivial, demanding problem due to its involvements of subjective knowledge, objective proof, and logical reasoning. Subjective information 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 acquires subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. In this paper, we look for 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.

D-S theory has been adopted as a powerful tool for evaluating security, reliability and integrity in information systems and by other engineering fields , where precise measurement is impossible to obtain or expert elicitation is required. D-S theory has several characteristics. First, it enables us to collect the subjective and objective evidences with basic probability assignment and belief function. Second, it hold Dempster's rule of combination (DRC) algorithm to combine several evidences together with probable reasoning. However, as identified in, Dempster's rule of combination encounter several boundaries, such as treating evidences equally without differentiating each evidence and considering priorities among them. To

address these limitations in MANET we proposing an adaptive time-wise isolation technique. Our risk-aware approach is based on the extended D-S evidence model. In order to estimate our mechanism, we carry out a series of simulated experiments with a reactive MANET routing protocol, Adhoc on Demand Distance Routing Protocol (AODV) [12]. In addition, we attempt to demonstrate the effectiveness of our solution.The most important contributions of this paper are summarized as follows:

- We propose an extended D-S evidence model with notion of 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 non associative also 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 origined by both attacks and countermeasures. The adaptiveness of our mechanism permits us to systematically cope with MANET routing attacks.
- We evaluate our response mechanism against representative attack scenarios and experiments. Our results evidently 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 AODV and routing attacks against AODV. Section 3 describes how our extended D-S evidence model can be integrated with significance factors. Section 4 presents the details of our risk-aware response mechanism and provides the related work in MANET intrusion detection and response systems, as well reviews risk-aware approaches in different fields. Section 5 concludes this paper.

II. AODV PROTOCOL

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of together unicast and multicast routing. It is a demanding algorithm, meaning that it builds routes between nodes only as desired by source nodes. It preserves these routes as long as they are needed by the sources AODV builds routes using a route request / route reply query cycle. When a source node needs a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In count to the source node's IP address, present sequence number, also broadcast ID, the RREQ also contains the most latest sequence number for the destination of which the source node is aware. A node receiving the RREQ might send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the situation, it unicasts a RREP back to the source. Or else, it rebroadcasts the RREQ. Nodes maintain track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have previously processed, they discard the RREQ also do not forward it.

As the RREP propagates back to the source, nodes put up forward pointers to the destination. Formerly the source node receives the RREP it might begin to forward data packets to the destination. If the source afterward receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hopcount, it might update its routing information for that destination and begin using the better route.

As long as the route remains vigorous, it will continue to be maintained. A route is considered vigorous as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops distribution data packets, the links will time out also eventually be deleted from the intermediate node routing tables. If a link break happens while the route is active, the node upstream of the split propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). Subsequent to receiving the RERR, if the source node still needs the route, it can reinitiate route discovery.

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 faith models the proof, while Dempster's rule of combination is the procedure to combine and summarize a series of collected evidences. However, previous research efforts identify several limitations of the Dempster's rule of combination

1. Associative. For DRC, the order of the evidences in the collected evidences in evidence pool does not impact the result. As shown in, a nonassociative combination rule is necessary for many cases.
2. Nonweighted. DRC implies that we trust all evidences equally. However, in reality, our trust on different evidences might differ. In other words, it means we should consider various factors for each evidence.

We proposed rules to combine several evidences presented sequentially for the first limitation. We suggested a weighted combination rule to handle the second limitation. Our extended Dempster-Shafer theory with importance factors can overcome both of the aforementioned limitations.

A Importance Factors and Belief Function

In D-S theory, propositions are represented as subsets

of a given set. Suppose e is a finite set of states, and let 2^e denote the set of all subsets of e. D-S theory calls e, a frame of discrimination. When a proposition corresponds to a subset of a frame of discernment, it means that a particular frame discerns the proposition. First, we initiate a notion of importance factors.

Definition 1. Importance factor (IF) is a positive real number associated with the importance of evidence. IF s are resulting from historical observations or expert experiences.

Definition 2. An evidence E is a 2-tuple hm, I F), where m describes the basic probability assignment . Basic prob- ability assignment function m is defined as follows:

$$m(\phi)=0 \quad \text{----}\rightarrow \quad (1)$$

and

$$\Sigma\, m(A)=1 \quad \text{----}\rightarrow \quad (2)$$

According to [2], a function Bel : 2^e ! ½O, 1] is a belief function over e if it is given by (3) for some basic probability assignment m : 2^e ! ½O, 1]

$$Bel(A)= \sum_{B \in A} m(B) \quad \text{----}\rightarrow \quad (3)$$

Given several belief functions over the same frame of discernment and based on distinct bodies of evidence, Dempster's rule of combination, which is 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 e, with basic probability assignments m_1 and m_2 . Then, the function m : 2^e ! ½O, 1] defined by m(q)) O and

$$m(c)= \Sigma AiBj=Cm1(Ai)m2(Bj) \quad \text{----}\rightarrow \quad (4)$$
$$1- \Sigma AiBj= Cm1(Ai)m2(Bj)$$

Suppose IF_1 and IF2 are importance factors of two independent evidences named E_1 and E_2, respectively. The combination of these two evidences implies that our total belief to these two evidences is 1, but in the same time, our independent evidences. Then, the combination of E_1 and E_2 is E hm1 m2 , $(IF_1 + IF_2)/2$), where is Dempster's rule of combination with importance factors.

B. 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 explain four properties that a candidate Dempster's rule of combination with importance factors should track. Properties 1 and 2 ensure that the combined result is suitable 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 similar priority. Property 4 ensures that significance factors of the evidences are also independent from each other.

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

$$m'(\phi)=0 \quad \text{----}\rightarrow \quad (1)$$

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

$$\Sigma m'(A)=1 \quad \text{----}\rightarrow \quad (2)$$

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

$$m'(A,IF1,IF2)=m(A) \text{ if } IF_1 = IF2$$

Property 4. Importance factors of each evidence must not be exchangeable

$$M'(A, IF_1, IF_2) = m'(A, IF_2, IF_1) \text{ if } (IF_1 = IF_2):$$

C. 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

$$m'(A,IF1,IF2)= m(A) \text{ if } IF_1 = IF_2$$

D. Theorem Dempster rule of combination

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 is 0, which models a Factors: Suppose Bel_1 and Bel_2 are belief functions

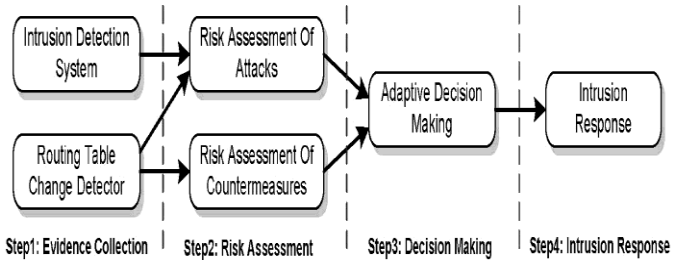

Fig. 1. Risk-aware response mechanism.

Proof. It is obvious that our proposed DRC1F holds Properties. We prove that our proposed DRC1 F also holds Properties Property Our evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. We suggest a unified analysis approach for evaluating the risks of both attack ($Risk_A$) and countermeasure ($Risk_C$).

The evidence collection algorithm collects the evidences of each node and thus combine all the evidence and put in evidence pool. It may be positive or negative evidence it will collect and sends the alert message to all the trusted nodes in the network. Thus the decision making may separate the

trusted nodes and untrusted nodes in the network by comparing the subjective and objective evidence collected. And finally the untrusted node is put in the black list.

Two independent evidences named E_1 and E_2, respectively. The combination of these two evidences implies that our total belief to these two evidences is 1, but in the identical time, our belief to either of these evidences is less than 1. This is straightforward because if our belief to one evidence is 1, it would signify our belief to the other is 0, which models Routing table recovery includes local routing table revitalization and global routing improvement. Local routing recovery is performed by victim nodes

Our proposed DRCIF is non associative for multiple evidences. hence, for the case in which sequential information is not available for a few instances, it is necessary to make the result of combination consistent with multiple evidences. Our combination algorithm support this requirement and the complexity of our algorithm is O(n), where n is the number of evidences. It signifies that our extended Dempster-Shafer theory demands no extra computational cost compared to a naïve fuzzy-based technique. The algorithm for combination of multiple evidences and putting them in evidence pool is constructed as follows:

Algorithm 1. MUL-EDS-MB

To calculate the total evidence this algorithm is used. Thus finding the attacker and stopping any actions from that node.

OUTPUT: One evidence

1 jEpj = sizeof(Ep);
2 While jEpj > 1 do
3 Pick two evidences with the least 1F in Ep, named E_1 and E_2;
4 Combine these two evidences, E = hm1 m2, (1F1 + 1F2)/2);
5 Remove E_1 and E_2 from Ep;
6 Add E to Ep;
7 end

When the risk of attack is greater than the risk of isolation response, the isolation is desirable. If other information is accessible, it could be used to adjust thresholds. For instance, node reputation is one of important factors in MANET security, our adaptive supervisory module could take this factor into account as fine. That is, if the compromised node has a high or low reputation level, the response module can intuitively alter the risk tolerance thresholds accordingly.

IV.OVERVIEW OF RISK AWARE RESPONSE MECHANISM

The overview of Risk aware response mechanism involves the following, Evidence collection. In this step, Intrusion discovery 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 calculation and combined with the extended D-S theory. Risk of extended measure is calculated as well during risk assessment phase. Decision making. The adaptive decision module provides a flexible response decision-making method, which takes risk estimation and risk tolerance into account. To amend temporary isolation level, a user can set dissimilar thresholds to fulfil her goal. Broadcasting the Attacker. In this module the attacker can be detected by with the help of decision making module and then we secure the network. Then broadcast to all nodes about attackers and then band the attacker service.

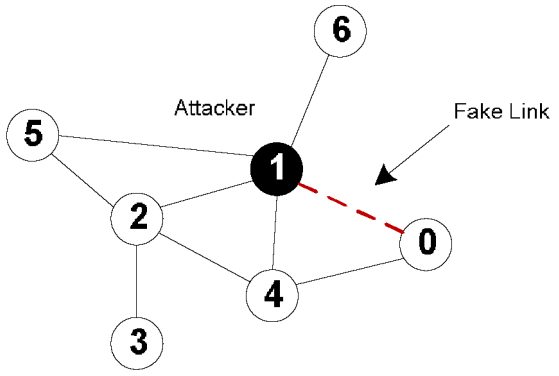

Fig. 2. Example scenario.

Intrusion response. With the output from risk assessment and supervisory module, the corresponding responding actions, including routing table recovery and node isolation, are passed out to mitigate attack damages in a distributed manner.

A. Response to Routing Attacks

In our approach, we use two different responses to deal with different attack methods: routing table mending and node isolation. Routing table mending includes local routing table recovery and global routing mending. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table. Global routing mending 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 reactive routing protocols like AODV, routing table recovery does not bring any additional overhead since it periodically goes with routing organize messages. Also, as long as the detection of attack is positive, this reaction 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 carry out a node

isolation response, the neighbours 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 separation response may result in negative impacts to the routing operations, still bringing more routing damages than the attack itself.

For example, in Fig. 2, Node 1 behaves like a malicious node. Though, if every other node simply isolate Node 1, Node 6 will be detached from the network. hence, more flexible and fine-grained node isolation mechanism are required. In our risk-aware reply mechanism, we accept two types of time-wise isolation responses: temporary isolation and permanent isolation.

Since the attack response actions may cause more damages than attacks, the risks of both attack also response should be estimated. We categorize the security states of MANET into two categories: {Secure, Insecure}. In other words, the frame of discernment would be {q, {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. Belf1nsecureg is used to represent the risk of MANET.

B. Selection of Evidences

Our evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. We suggest 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 evidence, we analyse different routing table modification cases. There are three basic items in AODV routing table (destination, next hop, distance). Therefore, routing attack can origin existing routing table entries to be missed, or some item of a routing table entry to be changed. We illustrate the probable cases of routing table change and analyze the degrees of damage in Evidences 2 through 5.

Evidence 1: attentive confidence. The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence. because the false alarm is a serious problem for most IDSs, the confidence factor should be considered for the risk assessment of the attack. The essential probability assignments of Evidence 1 are based on three equations given below:

Evidence 2: Missing entry. This proof indicates the proportion of missing entries in routing table. Link with-holding assault or node isolation countermeasure can cause possible deletion of entries from routing table of the node.

Evidence 3: Changing entry I. This proof represents the proportion of changing entries in the case of next hop being the malicious node. In this case, the wicked node builds a direct link to this node. So, it is highly likely for this node to be the attacker's target. Malicious node could drop every one of the packages to or from the target node, or it can act as a normal node and wait for future attack actions

Evidence 4: Changing entry II. This evidence shows proportion of changed entries in the case of different next hop (not the malicious node) and the same distance. We consider the impacts on the node communication should be very minimal in this case. Mutually attacks and countermeasures could cause this case.

Evidence 5: Changing entry III. This proof points out the proportion of changing entries in the case of different next hop (not the malicious node) and the different distance. alike to Evidence 4, both attacks and countermeasures could result in this evidence. The path change may also gets changed.

Basic probability assignments of Evidences 2 to 5 are based on Equations are piecewise linear functions, where a, b, c, and d be constants and determined by experts. d is the least value of the belief that implies the status of MANET is insecure. On the other hand, 1-d is the greatest value of the belief that means the status of MANET is safe. a, b, and c are the thresholds for minimum belief or maximum belief for each respective mass function.

C. 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 (1nsecure) and Bel_C (1 nsecure) represent risks of attack ($Risk_A$) and countermeasure ($Risk_C$), respectively. The combined evidences, E_A and E_C are defined . The entire risk value derived from $Risk_A$ and $Risk_C$ is given in

$$E_A = E_1 \quad E_2 \quad E_3 \quad E_4 \quad E_5,$$

$$E_C = E_2 \quad E_4 \quad E_5,$$

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

$$Risk = Risk_A - Risk_C = Bel_A(1nsecure) - Bel_C(1nsecure).$$

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

We recommend the value of lower risk tolerance threshold be 0 initially if no additional information is obtainable. It implies when the risk of attack is greater than the risk of isolation reaction, the isolation is needed. If other information is available, it could be utilized to adjust thresholds. For instance, node reputation is one

of important factors in MANET security, our adaptive supervisory module could take this factor into account as fine. That is, if the compromised node has a high or low reputation level, the reply module can intuitively adjust the risk tolerance thresholds consequently. In the case that LT is less than 0, still if the risk of attack is not greater than the risk of isolation, the response could as well perform an isolation task to the malicious nodes.

The risk tolerance thresholds could also be dynamically adjusted by other factors, such as attack frequency. If the attack frequency is high, more severe response action should be taken to counter this attack.

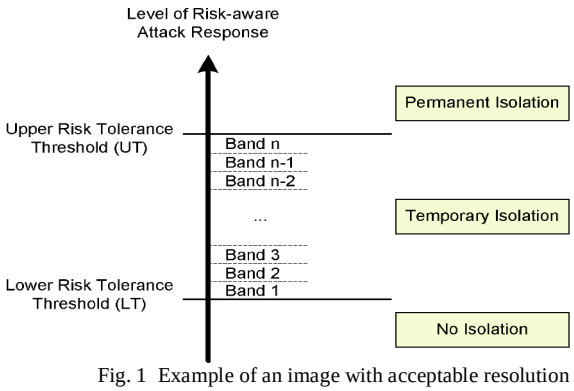

Fig. 1 Example of an image with acceptable resolution

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.

D. Adaptive Decision Making

Our adaptive decision-making module is based on quantitative risk estimation and risk tolerance, which is shown in Fig. 3. The reaction level is additionally divided into multiple bands. every band is associated with an isolation degree, which presents a dissimilar time period of the isolation action. The reply 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 among 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.

V. BLACK LIST

To mitigate routing misbehaviour, we try to reduce the number of attack by putting the node in black list by predicting its IP address. If a node is detected to be misreporting, by changing any routing information it should be blacklisted and should not receive packets from others. And cannot be able to sent further packets. The trusted node should not receive the packet from the attacker because the attacker is black listed.

.

VI. 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 practicality 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] 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 Condi- tions 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," AI Magazine, 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.

[14] H. Deng, W. Li, and D. Agrawal, "Routing Security in

Wireless Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[15] 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.

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

[17] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315, 2003.

[18] M. Yamada and M. Kudo, "Combination of Weak Evidences by D-S Theory for Person Recognition," Knowledge-Based Intelligent Information and Engineering Systems, pp. 1065-1071, Springer, 2004.

[19] K. Fall and K. Varadhan, "The NS Manual," 2010.

[20] F. Ros, "UM-AODV Implementation (version 0.8.8) for NS2,"2007

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

[22] B. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02), pp. 78-88, 2002.

[23] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.

[24] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and . H Rubens, "ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks," ACM Trans. Information and System Security, vol. 10, no. 4, pp. 1-35, 2008.

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