International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 6- 15, 2013

Risk-Aware Response Mechanism with Extended D-S theory

G.Nirmala
Erode Sengunthar Engineering College
Thudupathi,Erode,Tamil Nadu

T. Kalai selvi
Erode Sengunthar Engineering College
Thudupathi,Erode,Tamil Nadu

Abstract: Mobile Ad hoc Networks (MANET) are having dynamic nature of its network infrastructure and it is vulnerable to all types of attacks. Among these attacks, the routing attacks getting more attention because its changing the whole topology itself and it causes more damage to MANET. Even there are lot of intrusion detection Systems available to diminish those critical attacks, existing causesunexpected network partition, and causes additional damages to the infrastructure of the network , and it leads to uncertainty in finding routing attacks in MANET. In this paper, we propose a adaptive risk-aware response mechanism with extended Dempster-Shafer theory in MANET to identify the routing attacks and malicious node. Our techniques find the malicious node with degree of evidence from the expert knowledge 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

Keywords: Mobile Adhoc Network, Black list, Aodv, Dempster Shafer theory;

1.INTRODUCTION

MOBILE Ad hoc Networks (MANET) introducing a communication in all environments without any predefined infrastructure or centralized administration Therefore, MANET is suitable for adverse and hostile environments where central authority point is not necessary. The important characteristic of MANET is the dynamic nature of its network topology which is frequently changing due to the unpredict- able 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.

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.

In Existing Wang proposed a na¨ıve fuzzy cost sensitive intrusion response solution for MANET. Their cost model took 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

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 .D-S theory has been adopted as a valuable tool for evaluating reliability and security 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 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, 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 responsemechanism to systematically cope with routing attacks in MANET, proposing an adaptive time-wise isolation meth- od. 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 proactive MANET routing protocol, Adhoc On Demand Distance Vector Routing Protocol (AODV).In addition, we attempt to demonstrate the effectiveness of our solution.

The major contributions of this paper are summarizedas follows:

We formally propose an extended D-S evidence model with importance factors and articulate ex- pected properties for Dempster's rule of combina- tion with importance factors (DRCIF). Our Dempster's rule of combination with importance factors is no associative and weighted, which has not been addressed in the literature.

We propose an adaptive risk-aware response me- chanism with the extended D-S evidence model, considering damages caused by both attacks and countermeasures. The adaptiveness of our mechan- ism allows us to systematically cope with MANET routing attacks.

2.Background

2.1 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 both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains 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 desires 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 addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may 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 case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it

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

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops

sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

2.2.Routing Attacks:

In AODV, any node can either modify the protocol messages before forwarding them, or create false messages or spoof an identity. first, it changes the contents of a discovered route, modifies a route reply message, and causes the packet to be dropped as an invalid packet; then, it validates the route cache in other nodes by advertising incorrect paths, and refuses to participate in the route discovery process; and finally, it modifies the contents of a data packet or the route via which the data packet is supposed to travel or behave normally during the route discovery process but is dropped. Thus all types of fabrication attacks can occurs.

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 , 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 may 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 and suggested a weighted combination rule to handle the second limitation. We evaluate our response mechanism against representative attack scenarios . 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. The DRC technique will be taken for finding the attacks and its counter measures and thus will be putting the attacker in a black list to avoid the same attacker while entering the network later.

3.1 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 2e denote the set of all subsets of e. D-S theory calls e, a frame of discernment. When a proposition corresponds to a subset of a frame of discernment, it implies that a particular frame discerns the proposition. First, we introduce a notion of importance factors.

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

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

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

and

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

The Belief Function is as follows

$$Bel(A)= \Sigma\, m(B) \text{ ----------}>(3)$$

3.2 Expected Properties for Our Dempster's Rule of Combination

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 q in the result of our combination rule

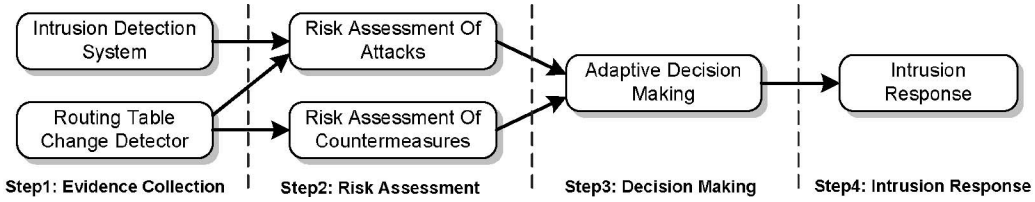


Figure. 1. Risk-aware response mechanism

Proof. It is obvious that our proposed DRCIF holds Properties . We prove that our proposed DRCIF also holds Properties

Property:

$$m'(\phi)=0 \text{ ----------}>(4)$$

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

$$\Sigma m'(A)=1 \text{ ----------}>(5)$$

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

$$m'(A,IF1,IF2)=m(A) \text{ if } IF1 = I\ F2$$

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

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

we propose a Dempster's rule of combinationwith importance factors. We prove our combination rule

$$m'(A,IF1,IF2)= m(A) \text{ if } IF1 = I\ F2$$

4. Theorem Dempster's 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 or 0.

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 (RiskA) and countermeasure (RiskC).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 AODV 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.

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, in 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 Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes.

4.1 Evidence Collection

Our proposed DRCIF is nonassociative for multiple evidences. Therefore, for the case in which sequential information is not available for some instances, it is necessary to make the result of combination consistent with multiple evidences. Our combination algorithm sup- ports this requirement and the complexity of our algorithm is 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 naïve fuzzy-based method. The algorithm for combination of multiple evi- dences is constructed as follows:

Algorithm 1.MUL-EDS-CMB

OUTPUT: One evidence

1 jEpj j sizeof(Ep);
2 While jEpj > l do
3 Pick two evidences with the least 1F in Ep, named El and E2 ;
4 Combine these two evidences, E j hml m2 , (1Fl + 1F2)/2);
5 Remove El and E2 from Ep;
6 Add E to Ep;
7 end

The Evidences are collected from the IDS and priorities assigned to each of them,thus by adding together we get the total evidences. Risk Assessment is made with attacks and its effects. Adaptive decision is taken that the node is attacker or not by comparing with with the threshold values namely upper risk tolerance and lower risk tolerance and finally Intrusion response will send a alert to other nodes.

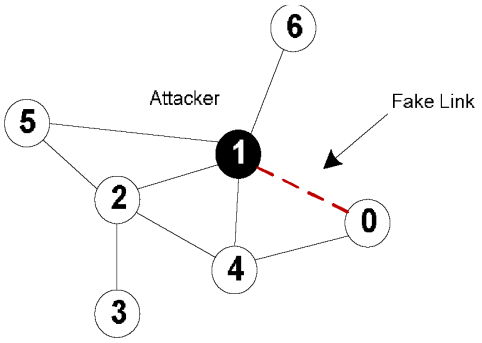


Figure. 2. Example scenario.

Intrusion response. With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isola- tion, 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 AODV 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.

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

4.3 Risk Assessment

Evidence 1: Alert confidence. The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence.

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

Evidence 3: Changing entry I. This evidence represents the proportion of changing entries in the case of next hop being the malicious node. In this case, the malicious node builds a direct link to this node possible for this.

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

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.

The probability assignments of evidences 2 to 5 1-d means the maximul value of the belief that means the status of the MANET is secure.

m(1nsecure) j c, c is confidence given by 1DS

m(Secure) j l — c (

(Secure, 1nsecure) j O

4.3.1 Combination of Evidences

For simplicity, we call the combined evidence for an attack, EA and the combined evidence for a countermeasure, EC Thus, BelA (1nsecure) and BelC (1nsecure) represent risks of attack (RiskA) and countermeasure (RiskC), respectively. The combined evidences, EA and EC are defined The entire risk value derived from RiskA and RiskC is given as

E_A j E_1 E_2 E_3 E_4 E_5 ,

E_C j E_2 E_4 E_5 ,

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

Risk j RiskA — RiskC j BelA (1nsecure)— BelC (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

4.4 Adaptive Decision

Making

Our adaptive decision-making module is based on quanti- tative risk estimation and risk tolerance, which is shown in Fig. 3. The response level is additionally divided into multiple bands. Each band is associated with an isolation degree, which presents a different time period of the isolation action.

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 dynamicallyadjusted 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

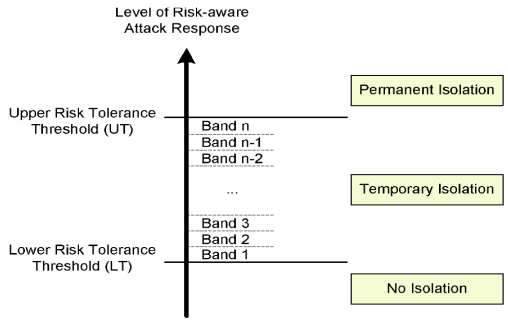


Fig 3 Decision making

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 Java with the eclipse tool Eclipse is an Integrated Development Tool 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.

In order to evaluate the effectiveness of our adaptiverisk-aware response solution, we divided the simulation process into three stages and compared the network performance in terms of several 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 for each simulation run:

. Packet delivery radio. The ratio between the number of packe ts 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.

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

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

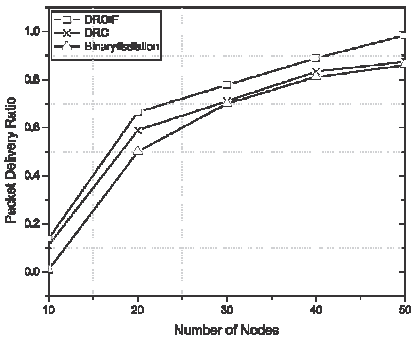
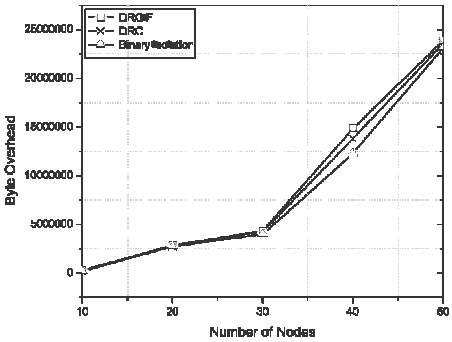


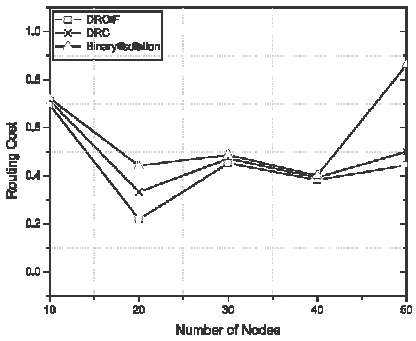
Fig 4 a Packet delivery ratio



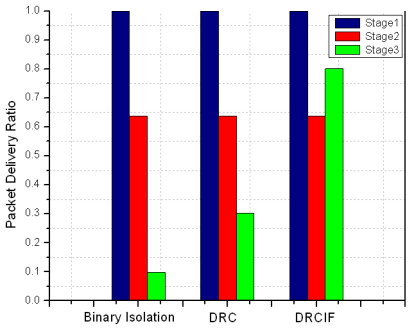
c. Byte Overhead

In Fig. 4a, as the number of nodes increases, the packet delivery ratio also increases because there are more route choices for the packet transmission. Among these three response mechanisms, we also notice the packets delivery ratio of our DRCIF risk-aware response is higher than those of the other two approaches.

In Fig. 4b, we can observe that the routing cost of our DRCIF risk-aware response is lower than those of the other two approaches. Note that the fluctuations of routing cost shown in Fig. 4b are caused by the random traffic generation and random placement of nodes in our realistic simulation



b. Routing cost



d. Packet delivery

Fig. 4c 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 next Stage , 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.

In Fig. 4d, 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. But in DRCIF mechanism the delivery is more.

7 CONCLUSION

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

8 REFERENCES

[1] Cheng.P, Rohatgi.P, Keser.C, Karger.P, Wagner.G, and Reninger.A, 2007, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy.

[2] Deng.H, Li.W, and Agrawal.D, 2002 ,"Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct..

[3] Mu.C, Li.X, Huang.H, and Tian.S, , 2008. "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," Proc. 13th European Symp. Research in Computer Security (ESORICS '08),pp. 35-48

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

[5] Refaei.M, DaSilva.L, Eltoweissy.M, and Nadeem.T, 2010 "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719.

[6] Sentz.K and Ferson.S, , 1984 "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.

[7] Agrawal, Sanjeev Jain, Sanjeev Sharma, January 2011, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of Computing, Volume 3, Issue 1, 41-48.

[8] Sun.L, Srivastava.R, and Mock.T, , 2006 "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions," Management Information Systems, vol. 22, no. 4, pp. 109-142.

[9] Sun.Y, Yu.W, Han.Z, and Liu.K, , 2002 "Information Theoretic Framework of Trust Modeling and Evaluation for Ad [8] K. Sentz and S. Ferson, "Combination of Evidence in Dempster-Shafer Theory," technical report, Sandia Nat'l Laboratories.

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

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

[12] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, , 2002, "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1.