Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Various Routing Attacks and Risk Aware Mechanism for MANET

Swati M. Dahekar, Yogesh Bhute
Department of Computer Science and Engineering
AbhaGaikwad Patil college of Engineering,Nagpur, India

Abstract— Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. The key feature of MANETs is the absence of a centralmanagement agency or a fixed infrastructure. Since the most devastating damage to MANET is caused by routing attacks they have received considerable attention.In this survey, initially the existing security attacks in MANET are analysed. The attacks categories fall under two stages that include internal and external attacks. The former attack is due to the malicious nodes within the network and later attack is caused by the nodes which do not belong to the network. Then the secure, efficient dynamic routing techniques which are main issues concerned with ad hoc networks are surveyed. An IDS is used to detect attempted intrusion into acomputer or network. It processes audit data, performs analysis and takes certain set of actions against the intruder. Overall, our survey mainly concentrates the existing security attacks and possible routing solution in MANET.

Keywords— Mobile Ad hoc Networks, Attacks, Routing Protocols,risk-aware approach ,Intrusion Detection System, Dempster-Shafer theory.

I. INTRODUCTION

A MANET is a self-configuring dynamic network of mobile devices connected by wireless links with the set for a specific purpose. A MANET is formed by a group of mobile wireless nodes often without the assistance of fixed network infrastructure. It is formed dynamically by autonomous systems of mobile nodes that are connected wirelessly without support of any existing network infrastructure or centralized administration. Instead of using a central base station for nodes to communicate with one another, MANETs do not rely on any pre-defined infrastructure. MANET operates in peerto- peer mode. Nodes within the communication range communicate via wireless radio links, and for those outside the communication range, use other nodes to relay their packets. Mobile nodes may move away from their current locations and re-join the network from different locations in the network, thus dynamically changing their network topology and node density. In many applications MANET could be deployed such as military tactical operations, automated battlefields, sensor networks, disaster recovery, emergency search-and rescue missions and mobile teleconferencing. MANETs have some special characteristic features such as unreliable wireless links used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc. While these characteristics are essential for the flexibility of MANETs . One of the primary concerns related to ad hoc networks is to provide a secure communication among mobile nodes in a hostile environment. The nature of mobile ad hoc networks poses a range of challenges to the security design. The main problem for MANET security resides: the ad hoc networks can be reached very easily by users, but also by malicious attackers. If a malicious attacker reaches the network, the attacker can easily exploit or possibly even disable the mobile ad hoc network. A MANET can be examined on the basis of availability, confidentiality, authentication, integrity and non-repudiation. Considering continuous discovery of new vulnerabilities, the intrusion-detection system (IDS) must be effective and efficient in identifying attacks, and then neutralizing them. The traditional IDSs developed for wired networks are difficult to use for MANETs because of their architectural differences. Without centralized audit points like routers, switches, and gateways, MANETs can only collect audit data locally and thus require a distributed and cooperative IDS. Other differences between wired networks and MANETs include traffic patterns, node mobility, and node constraints.These differences all render the traditional IDSs hard to be directly applied to MANETs. Nodes in MANETs can move freely through the network, and thus their dynamically changing network topology makes MANETs very different from the traditional wired networks. Also, nodes in MANETs usually have slower communication links, limited bandwidth, limited battery power, and limited memory. Therefore, these constraints make the design of IDS in MANETs much more challenging than in wired networks.

II. RELATED WORK

Ziming Zhao [Risk-Aware Response for Mitigating MANET Routing Attacks]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 naive fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. In this paper, propose a risk-aware response mechanism to systematically cope with the identified routing attacks. My 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.

Y. Sun, W. Yu, Z. Han, and K. Liu ,The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other nodes without centralized authorities. This paper presents an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. In the proposed framework, trust is a measure of uncertainty with its value represented by entropy. We develop four Axioms that address the basic understanding of trust and the rules for trust propagation. Based on these axioms, it presents two trust models: entropy-based model and probability-based model, which satisfy all the axioms. Techniques of trust establishment and trust update are presented to obtain trust values from observation. The proposed trust evaluation method and trust models are employed in ad hoc networks for secure ad hoc routing and malicious node detection. A distributed scheme is designed to acquire, maintain, and update trust records associated with the behaviors of nodes' forwarding packets and the behaviors of making recommendations about other nodes. Simulations show that the proposed trust evaluation system can significantly improve the network throughput as well as effectively detect malicious behaviors in ad hoc networks.

M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem ,Reputation management systems have been proposed as a cooperation enforcement solution in ad-hoc networks. Typically, the functions of reputation management (evaluation, detection, and reaction) are carried out homogeneously across time and space. However, the dynamic nature of ad-hocnetworks causes node behavior to vary both spatially and temporally due to changes in local andnetwork-wide conditions. When reputation management functions do not adapt to such changes, their effectiveness, measured in terms of accuracy (correct identification of node behavior) and promptness (timely identification of node misbehavior), may be compromised it propose an adaptive reputation management system that realizes that changes in node behavior may be driven by changes in network conditions and that accommodates such changes by adapting its operating parameters. It introduced a time-slotted approach to allow the evaluation function to quickly and accurately capture changes in node behavior. It show how the duration of an evaluation slot can adapt according to the network's activity to enhance the system accuracy and promptness. It then show how the detection function can utilize a Sequential Probability Ratio Test (SPRT) to distinguish between cooperative and misbehaving neighbors. The SPRT adapts to changes in neighbors'behavior that are a by-product of changing network conditions, by using the node's own behavior as a benchmark. It compare the proposed solution to a non adaptive system, showing the ability of the system to achieve high accuracy and promptness in dynamic environments. To the best of our knowledge, this is the first work to explore the adaptation of the reputation management functions to changes in network conditions.

P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A.Reninger,This paper presents a new model for, or rather a new way of thinking about adaptive, risk-based access control. This paper basic premise is that there is always inherent uncertainty and risk in access control decisions that is best addressed in an explicit way. We illustrate this concept by showing how the rationale of the well-known, Bell-Lapadula model based; multi-level security (MLS) access control model could be used to develop a risk-adaptive access control model. This new model is more like a fuzzylogic control system than a traditional access control system and hence the name "fuzzy MLS". The long version of this paper is published as an IBM Research Report.

III. ATTACKS IN MANET

A) CLASSIFICATION OF ATTACKS

The threats for MANETs are classified as follows

Giving security to the Mobile Ad-hoc Network is a difficult task. In order to given better solution for security attack, First we must identify and understand about the attack. Because of the unavailability of centralized coordinator in MANET, the security is a challenging task in wireless communication. The security attack classification is given below:

1. Internal Attack: The internal attacks are initiated from the compromised nodes in the mobile Ad-hoc network. In here the attacker node gets the unauthorized access and showing that as a normal mobile node. It analyses the data flows between the nodes in the network.

2. External Attack: These attacks are created by the nodes that are outside the network. It creates wrong routing information or service unavailability

The External Attacks have two different classifications. They are:

- Active Attack
- Passive Attack

Active Attacks:

The active attacks are harmful one this attacks prevent the data flows between the source and destination nodes. This active attack either may be internal or external. The active external attacks created by the nodes which belong to the outside of the network. The internal attacks are more harmful and difficult to detect. This internal active attacks are

created by the malicious nodes which are belongs to the network. These attacks are more supported for the attackers to modify the data packets and that creates the congestion in the network. In here the malicious node modify the routing information and advertise its wrong routing path as the best routing path.

Passive attacks*:*

The passive attack does not create any changes in the rouging data packet. It just monitors the network traffic. It does not affect the routing protocol operation but listen the protocol's routing functionality. In order to avoid this type of attacks we need strong encryption and decryption algorithms for data transmission .

B) TYPES OF ATTACKS ON VARIOUS LAYERS

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack [4].

Layer	**Types of Attacks**
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Evasdropping, Jamming active interference.

IV. SECURITY CONSIDERATIONS IN AD HOC NETWORKS

Security in MANETs is an essential component for basic networkfunctions like packet forwarding and routing. If countermeasures are notembedded into the basic network functions at the early stages of their design, these operations can be easily compromised. Unlike networks using dedicatednodes to support basic functions, the functions of ad hoc networks are carriedout by all available nodes. This difference is at the core of the securityproblems that are specific to ad hoc networks.The wireless channel is accessible to both legitimate users andmalicious attackers, as there is no clear line of defense (Rashid HafeezKhokhar et al 2008). The number of successful data transmissions can beimproved by trust. The higher the number of nodes that trust each other in thenetwork, the higher will be the incidence of successful communication (Wanget al 2007, Eschenauer. Let et al 2002, Zhu et al 2003, Ren et al 2004, Samian11et al 2008, Abusalah et al 2006). When compared to the dedicated nodes of aclassical network, the nodes in an ad hoc network cannot be trusted for the correct execution of critical network functions. Managing trust in a militaryapplication is based on resource constraints and dynamics. The trust metric isobtained by combining the notion of trust derived from the social, informationand communication networks (Jin-Hee Cho et al 2011).Security in ad hoc networks is a very challenging issue, because it is very difficult for the nodes to collaborate. Ad hoc networks are open todifferent types of attacks, such as modification, impersonation and fabricationthat exploit the ad hoc routing protocols. Dropping, replaying or redirection ofdata packets leading to a Denial of service (DoS) attack is possible. Classicalsecurity solutions like cryptography and key management are too expensivefor MANETs, and are not suited for them to overcome these attacks; hencesecurity services should be distributed. Therefore a universal solution could not be provided by any standard protocol.

The attacks on MANETs (Bing Wu et al 2006, Perkins 2001 and Ilyas 2003) can be broadly classified into passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, DoS, and message replay. The attacks can also be classified into external attacks and internal attacks, according to the domain of the attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and 12 secret information, and possesses privileged access rights. Some security attacks use stealth, whereby the attackers try to hide their actions, from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made stealthily. Some attacks are non-cryptography related, while others are cryptographic primitive
attacks.

A) Attacks based on Modification, Impersonation and Sleep Deprivation

Generally, during a black-hole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet (RREP) to a source node that initiates a route discovery, thereby creating a threat to the integrity of the network. An attack has been introduced called the modification attack, where the malicious attacker changes the intended destination to some other destination. This attack can harm the network very badly. A new algorithm is proposed to detect multiple attacks, such as the modification, impersonation, and sleep deprivation attacks.

Hu et al (2003) found an attack called the rushing attack, whichmodifies the intended destination, by making the request packet to reach the target faster than the request packet from non malicious nodes. Thus the target node is being mislead by the malicious route as the intended route. But, in this scenario, the malicious node changes the intended destination by sending a wrongly assigned beacon packet to the target node. The Malicious node Detection and Elimination (MDE) algorithm can completely identify the modification attack and prevent it. This modification attack can pave the way for a malicious node to get control, and induce a black hole or gray-hole attack, which makes its prevention of paramount importance. This deals only
with the modification attack.

Kurosawa et al (2007) proposed anomaly detection scheme using dynamic training method in which the training data is updated at regular intervals. Their method has claimed to eliminate only black hole attack in AODV protocol. Padilla et al (2007) introduced the network with black hole. They devised Topology Graph based Anomaly Detection (TOGBAD), a new centralized approach, using topology graphs to identify nodes attempting to create a black hole. They performed plausibility checks of the routing information propagated by the nodes in the network which triggers an alarm if the plausibility check fails. It does not deal with other attacks .

Yi Ping et al (2005) introduced a new denial of service attack, and it is called the ad hoc flooding attack. It will exhaust the communication bandwidth and node resource so that valid communication cannot be established which leads to a generic defence against it, called Flooding Attack Prevention (FAP). This algorithm fails if there are other attacks such as sleep deprivation or battery exhaustion which leads to DOS attack in the network.

Perrig et al (2003) devised a good defence against the rushing attack which resulted in denial-of-service attack. Along with the rushing attack, Rushing Attack Prevention (RAP) is also introduced which has the ability to eliminate only one type of attack and fails in case of many attacks.

Sanzgiri et al (2002) proposed a well known secure routing protocol for ad hoc network called Authenticated Routing for Ad hoc Network (ARAN). It was based on certificates and was successful in defending the network against all identified attacks related to network's authentication. Although, it can authenticate the ad hoc network very well, itgives lesser performance when used for mobile nodes because of the overheadcosts due to mobile nodes sending and receiving signatures. In addition tothis, ARAN cannot handle when an attack to authentication of network iscombined with a denial of service attack by the same malicious node.

Finally, Hu et al (2002) proposed the most secure routing protocolcalled ARIADNE, that prevents attackers or compromised nodes fromtampering with uncompromised routes consisting of uncompromised nodes,and also prevents a large number of different types of Denial-of Serviceattacks. In addition to that, Ariadne is efficient, using only highly efficient*symmetric* cryptographic primitives which makes Ariadne the only protocol of those times (to the best of our knowledge) can secure the network from DOS attack and also provides authentication. The above works are tabulated and the proposed algorithm for Modification, Impersonation, Sleep deprivation, and TTL attacks in Node Transition Probability (MIST-NTP) shows better performance.

V. OLSR PROTOCOL

The major task of the routing protocol is to discover the topology to ensure that each node can acquire a recent map of the network to construct routes to its destinations. Several efficient routing protocols have been proposed for MANET. These protocols generally fall into one of two major categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as AdhocOn Demand Distance Vector (AODV) protocol, nodes find routes only when they must send data to the destination node whose route is unknown. In contrast, in proactive routing protocols, such as OLSR, nodes obtain routes by periodic exchange of topology information with other nodes and maintain route information all the time. OLSR protocol is a variation of the pure Link-state Routing (LSR) protocol and is designed specifically for MANET. OLSR protocol achieves optimization over LSR through the use of multipoint relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. Unlike LSR, where every node declares its links and forward messages for their neighbors, only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs.
Routing Attack on OLSR

A) Flooding attack:-

The aim of the flooding attack is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance.Black hole attack:-In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in Fig. I, source node S wants to send data packets to destination node D and initiates the route discovery process. We assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately sends the response to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 2. As a result, all packets through the malicious node is consumed or lost.

B) Link with holding attack:

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This typef attack is particularly serious in the OLSR protocol.

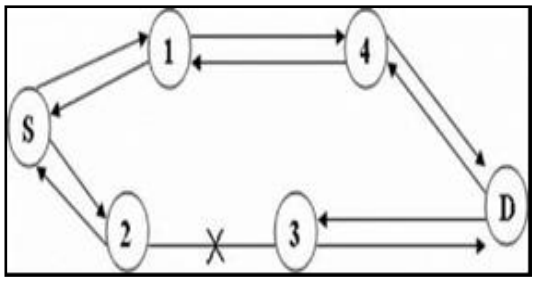

Fig I:-Black hole attack [2]

C) Wormhole attack:

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel. For example in Figure II, X and Y are two malicious nodes that encapsulate data packets and falsified the route lengths.

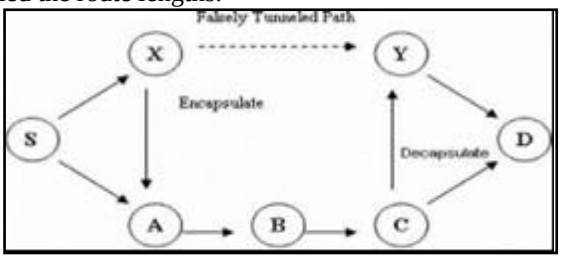

Fig II:Wormhole attack [2]

Suppose node S wishes to form a route to D and initiates route discovery. When X receives a route request from S, X encapsulates the route request and tunnels it to Y through an existing data route, in this case {X --> A --> B --> C --> Y}. When Y receives the encapsulated route request for D then it will show that it had only travelled {S --> X --> Y --> D}. Neither X nor Y update the packet header. After route discovery, the destination finds two routes from S of unequal length: one is of 4 and another is of 3. If Y tunnels the route reply back to X, S would falsely consider the path to D via X is better than the path to D via A. Thus, tunnelling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths.

D) Replay attack:

In a MANET, topology frequently changes due to node mobility. This means that current net- work topology might not exist in the future. In a replay attack, a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

VI. DEMPSTER-SHAFER THEORY FUNDAMENTALS

The Dumpsters–Shafer theory (DST) is a mathematical theory of evidence.[3] It allows one to combine evidence from different sources and arrive at a degree of belief (represented by a belief function) that takes into account all the available evidence. Dempster–Shafer theory is based on two ideas: obtaining degrees of belief for one question from subjective probabilities for a related question, and Dempster's rule for combining such degrees of belief when they are based on independent items of evidence. In essence, the degree of belief in a proposition depends primarily upon the number of answers (to the related questions) containing the proposition, and the subjective probability of each answer. Also contributing are the rules of combination that reflect general assumptions about the data. In this formalism a degree of belief (also referred to as a mass) is represented as a belief function rather than a Bayesian probability distribution. Probability values are assigned to sets of possibilities rather than single events: their appeal rests on the fact they naturally encode evidence in favour of propositions.

In existing systems, D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by various other engineering fields [7], [8], where precise measurement is impossible to obtain or expert elicitation is required. D-S theory support Dempster‟s rule of combination (DRC) to combine several evidences together with probable reasoning. However, as identified in [9], [10], [11], Dempster‟s rule of combination has limitations, such as treating equally without differentiating every evidence and considering priorities among them. To solve this limitations in MANET intrusion response scenario, a new Dempster‟s rule of combination with a notion of importance factors (IF)[3] in D-S evidence model was introduced. Here a risk-aware response mechanism was proposed to systematically cope with routing attacks in MANET, but now adaptive time-wise isolation meth- od is proposed. The risk-aware approach is based on the extended D-S evidence model. Then to simulate the proposed concept they used a proactive MANET routing protocol called Optimized Link State Routing protocol (OLSR).

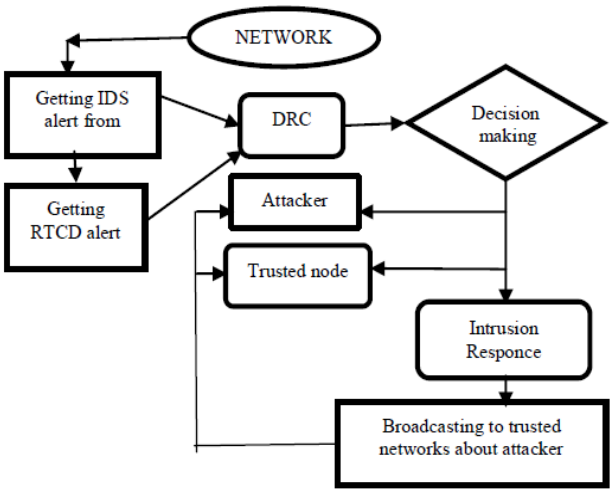

Fig III: system architecture

VII. CONCLUSIONS

This survey has elaborated the security attacks and routing principles in MANET. Initially the existing security attacks in MANET are analyzed. The attacks fall under two categories that include internal and external attacks. The former attack is due to the malicious nodes within the network and later attack is caused by the nodes which do not belong to the network. Then the secure, efficient dynamic routing techniques under proactive, reactive and hybrid protocol classes which are main issues concerned with ad hoc networks and the risk aware mechanisms are surveyed. Overall, our survey has concentrated mainly on the existing security attacks and possible routing solution in MANET.

REFERENCES

[1] Y. Sun, W. Yu, Z. Han, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2,pp. 305-317, Feb.2006.

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

[3] Ziming Zhao, Hongxin Hu, Gail-JoonAhn, Ruoyu Wu, "Risk Aware Mitigation For MANET Routing Attacks" - IEEE Trans. OnDependable and secure Computation, VOL.9, No.2, March/April 2012.

[4] S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost- Sensitive Intrusion Responses for Mobile Ad Hoc Networks," Proc. 10th Int‟lSymp. 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] L. Zadeh, "Review of a Mathematical Theory of Evidence," AI Magazine, vol. 5, no. 3, p. 81, 1984.

[8] 7R. Yager, "On the Dempster-Shafer Framework and New Combination Rules* 1," Information Sciences, vol. 41, no. 2, pp. 93- 137, 1987.

[9] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor FusionUsingDempster-Shafer Theory," Proc. IEEE Instrumentation andMeasurement Technology Conf., vol. 1, pp. 7-12, 2002.

[10] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.vol. 11, no. 1, pp. 21-38, 2005.

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

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

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

[14] 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.

[15] 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.

