Different Models for MANET Routing Attacks

Yuvaraj Kawale [α] & A. Raghavendra Rao [σ]

Abstract - **Mobile ad-hoc networks are becoming ever more popular due to their flexibility, low cost, and ease of deployment. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET Early proposed routing protocols were not designed to operate in the presence of attackers. There have been many subsequent attempts to secure these protocols, each with its own advantages and disadvantages. Even though there exist several intrusions response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or native fuzzy response decisions. To allow for a comparison of these secure protocols, a single common attacker model is needed. Our first contribution in this work is to develop a comprehensive attacker model categorizing attackers based on their capabilities. This is in contrast to the existing models which seek to categorize attacks and then map that categorization back onto the attackers. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and native fuzzy responses could lead to uncertainty in countering routing attacks in MANET. Our second contribution is an analysis of the SAODV routing protocol using our new model, which demonstrates the structured approach inherent in our model and its benefits compared to existing work.**

I. Introduction

Mobile ad-hoc networks (MANETs) allow for wireless devices to form a network without the need for central infrastructure. While the lack of need for infrastructure allows the network to be very flexible, it also makes routing a critical concern in the network. The original proposals for MANET routing such as DSR, DSDV, and AODV did not take security into consideration. As a result, many attacks have been found which can disrupt the functioning of a MANET. Subsequent protocol proposals were designed to address one or more of these attacks, yet no protocol has proven secure against all attackers In order to allow for an accurate comparison of the security properties of these proposals, a common attacker model is necessary which allows for proper evaluation.

Unfortunately, no suitable model has yet been developed. Instead, authors analyze their protocol in a scenario of their choice with restrictions designed to ease their proof of security. These models are typically developed by looking at the attack or attacks under consideration and trying to categorize attackers based on the characteristics of these attacks while placing topological restrictions on the network.

Due to this, unforeseen vulnerabilities can arise when the protocol is applied to real-world scenarios that cannot be molded to fit the topological constraints. In addition to bordering on contrived, each model uses a different set of restrictions, considers different topologies, or addresses different attacks. This makes accurate comparison of protocols and their security properties impossible. In contrast, developing models starting from the attackers' capabilities removes the topological constraints and the resultant overlooked networks that can present a new vulner ability. In fact, working from attacker capabilities to attacks is not only topology-agnostic, but also protocol-agnostic . In addition, once attackers are categorized by their capabilities, specific attacks can be mapped to the categories of attackers with sufficient capabilities to perform such attacks.

Similarly, the necessary capabilities for performing a specific attack can be determined by comparing categories of attackers that can and cannot perform the attack. In this work, we use this alternative approach to develop a novel attacker model focusing on categorizing attacker capabilities. To the best of our knowledge, this is the first attacker model of this form for MANET routing. Our new model allows for simplified determination of necessary and sufficient capabilities for performing specific attacks. In addition, due to the complete coverage of our model, real-world scenarios are included in the analysis, ensuring that vulnerabilities will be found during analysis and thus before deployment. Our proposed model is both topology- and protocol-agnostic. As such it allows for comparison of various protocols in one common model. Finally, the ability to combine our model with BAN logic or other formalization frameworks allows for a structured, comprehensive analysis of protocol security. In addition to our first main contribution of the new attacker model, our second main contribution is an example application of our new model to the SAODV protocol, showing how our structured approach exposes a serious, though previously known vulnerability automatically during analysis. Outline: In Section 2 we first discuss existing attacker models and their attack-based approach. Then, we focus on our first contribution, a new attacker model developed with the capabilities-based approach. We detail the attacker's communication and computation capabilities as well as the application of our model. Section 3 is our second main contribution, an example

Author α : M.Tech CSE Dept, ASRA Hyderabad.
E-mail : raj.yuvi9@gmail.com
Author σ : M.Tech (CSE), Associate Professor, Hyderabad.
E-mail : raghavamay15@gmail.com

application of our model to analyze the security mechanism of hash chains as used in the SAODV routing protocol.

MOBILE Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks.

Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated.

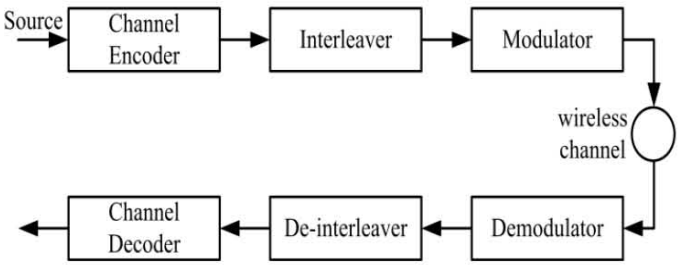
II. Risk Aware Response Mechanism Overview

a) Network System

We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in uncast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using preshared pair wise keys or asymmetric cryptography.

b) Real Time Packet Classification

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved, and decoded, to recover the original packet m.



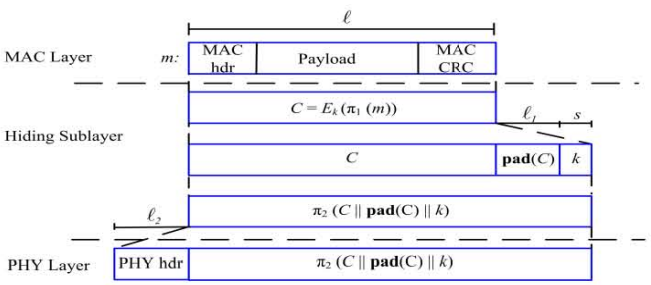
Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

c) Selective Jamming System

We illustrate the impact of selective jamming attacks on the network performance. implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block.

d) Strong Hiding Commitment Scheme (SHCS)

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.



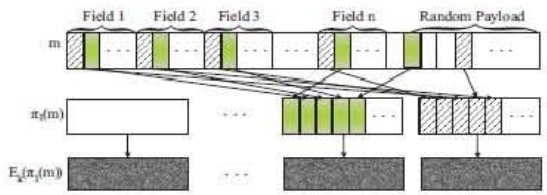
The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header Information is permuted as a trailer and encrypted, all

receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver.

e) Cryptographic Puzzle Hiding Scheme (CPHS)

We present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead.

We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.



Application of permutation π_1 on packet m.

III. Development Environment

How does the Java API support all of these kinds of programs? With packages of software components that provide a wide range of functionality. The core API is the API included in every full implementation of the Java platform. The core API gives you the following features:

a) The Essentials

Objects, strings, threads, numbers, input and output, data structures, system properties, date and time, and so on.

b) Applets

The set of conventions used by Java applets.

c) Networking

URLs, TCP and UDP sockets, and IP addresses.

d) Internationalization

Help for writing programs that can be localized for users worldwide. Programs can automatically adapt to specific locales and be displayed in the appropriate language.

e) Security

Both low-level and high-level, including electronic signatures, public/private key management, access control and certificates.

f) Software Components

Known as JavaBeans, can plug into existing component architectures such as Microsoft's OLE/COM/Active-X architecture, OpenDoc and Netscape's Live Connect.

g) Object Serialization

Allows lightweight persistence and communication via Remote Method Invocation (RMI).

h) Java Database Connectivity (JDBC)

Provides uniform access to a wide range of relational databases. Java not only has a core API, but also standard extensions. The standard extensions define APIs for 3D, servers, collaboration, telephony, speech, animation, and more.

i) How Will Java Change My Life?

Java is likely to make your programs better and requires less effort than other languages. We believe that Java will help you do the following:

i. *Get started quickly*

Although Java is a powerful object-oriented language, it's easy to learn, especially for programmers already familiar with C or C++.

ii. *Write less code*

Comparisons of program metrics (class counts, method counts, and so on) suggest that a program written in Java can be four times smaller than the same program in C++.

iii. *Write better code*

The Java language encourages good coding practices, and its garbage collection helps you avoid memory leaks. Java's object orientation, its JavaBeans component architecture, and its wide-ranging, easily extendible API let you reuse other people's tested code and introduce fewer bugs.

iv. *Develop programs faster*

Your development time may be as much as twice as fast versus writing the same program in C++. Why? You write fewer lines of code with Java and Java is a simpler programming language than C++.

v. *Avoid platform dependencies with 100% Pure Java*

You can keep your program portable by following the purity tips mentioned throughout this book and avoiding the use of libraries written in other languages.

vi. *Write once, run anywhere*

Because 100% Pure Java programs are compiled into machine-independent byte codes, they run consistently on any Java platform.

vii. *Distribute software more easily*

You can upgrade applets easily from a central server. Applets take advantage of the Java feature of allowing new classes to be loaded "on the fly," without recompiling the entire program.

We explore the java.net package, which provides support for networking. Its creators have called Java "programming for the Internet." These networking classes encapsulate the "socket" paradigm pioneered in the Berkeley Software Distribution (BSD) from the University of California at Berkeley.

IV. Related Work

Intrusion detection and response in MANET. Some research efforts have been made to seek preventive solutions for protecting the routing protocols in MANET. Although these approaches can prevent unauthorized nodes from joining the network, they introduce a significant overhead for key exchange and verification with the limited intrusion elimination. Besides, prevention-based techniques are less helpful to cope with malicious insiders who possess the legitimate credentials to communicate in the network. Numerous IDSs for MANET have been recently introduced. Due to the nature of MANET, most IDS are structured to be distributed and have a cooperative architecture. Similar to signature-based and anomaly based IDS models for the wired network; IDSs for MANET use specification-based or statistics-based approaches. Specification-based approaches, such as DEMEM monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. On the other hand, statistics-based approaches, such as Watchdog compare network activities with normal behavior patterns, which result in higher false positives rate than specification-based ones. Because of the existence of false positives in both MANET IDS models, intrusion alerts from these systems always accompany with alert confidence, which indicates the possibility of attack occurrence. Intrusion response system (IRS) for MANET is inspired by MANET IDS. In malicious nodes are isolated based on their reputations. Their work fails to take advantage of IDS alerts and simple isolation may cause unexpected network partition. Wang et al. brought the concept of cost-sensitive intrusion response which considers topology dependency and attack damage. The advantage of our solution is to integrate evidences from IDS, local routing table with expert knowledge, and countermeasures with a mathematical reasoning approach. Risk-aware approaches. When it comes to make response decisions there always exists inherent uncertainty which leads to unpredictable risk, especially in security and intelligence arena. Risk-aware approaches are introduced to tackle this problem by balancing action benefits and damage trade-offs in a quantified way. Cheng et al. presented a fuzzy logic control model for adaptive risk-based access control. Teo et al. applied dynamic risk-aware mechanism to determine whether an access to the network should be denied or permitted. However, risk assessment is still a nontrivial challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Wang et al. proposed a naı¨ve fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. Mu et al. adopted Dempster-Shafer theory to measure the risk of attacks and responses. However, as identified their model with Dempster's rule treats evidences equally without differentiating them from each other. To address this limitation, we propose a new Dempster's rule of combination with a notion of importance factors in D-S evidence model.

a) Attacks on Ad hoc Networks

An ad hoc network is a type of wireless local area network (WLAN) that is primarily characterized as dynamic and infrastructure less. Nodes in an ad hoc network have to compensate for the lack of infrastructure by cooperating in key network functionalities such as routing. Each node is assumed to function as a router for its neighbors' traffic to allow for multi-hop communication. The need for node cooperation as a key to network survival is a unique feature of ad hoc networks. Other networks, such as infrastructure-based WLANs and wire line networks, rely on existing infrastructure and special-purpose hardware to provide key network functionalities such as routing. Previous work in surveyed the security issues in ad hoc networks indicating that the significance of node cooperation in ad hoc networks makes network survival particularly sensitive to insider node behavior, making it an important security consideration. The threat model identifies and classifies types of node misbehavior in ad hoc networks into four different types: failed nodes, badly failed nodes, selfish nodes, and malicious nodes. These four classes can be differentiated with respect to the node's intent and action. A failed node exhibits unintentional passive behavior, where it is unable to participate in cooperation-based functionalities, due to power failures, for example. A badly failed node, on the

other hand, indicates unintentional active behavior, where a node may inadvertently advertise inactive routes or unnecessarily overload the network with routing updates. Selfishness is intentional passive misbehavior, where a node chooses not to fully participate in the packet forwarding functionality to conserve its resources. Selfish nodes are motivated only by their self-interest in conserving their resources and may drop some or all packets forwarded through them accordingly. Selfish nodes do not collude with each other or exert additional effort to camouflage their behavior, such as slander attacks. Finally, maliciousness is intentional active misbehavior, where a node's aim is to deliberately disrupt network operations. Malicious nodes may attack the link layer, taking advantage of the cooperative nature of the medium access control (MAC) protocol. The protocol requires each pair of communicating nodes to seek a unanimous promise from all other nodes within range to have an exclusive access to the channel. This characteristic is exploited in a number of denial-of-service (DoS) attacks including collision attacks and virtual jamming attacks. In a collision attack, a malicious node ignores the MAC protocol specifications by accessing the medium when other nodes within range are transmitting or receiving data, which causes collisions.

b) Proposed Solutions

Previous work noted the importance of securing ad hoc networks against attacks such as the ones. To address the problem of node misbehavior in ad hoc networks, three classes of solutions have been proposed: secure routing protocols, cooperation incentives, and node behavior evaluation.

i. *Secure Routing Protocols*

The merit of this class of solutions is to secure the establishment and maintenance of routes in routing protocols such as Ad hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) against tampering. The attack model classifies misbehavior on the routing functionality into passive and active attackers. A passive attacker may eavesdrop on the network, which is a threat to privacy and anonymity. An active attacker may inject incorrect routing information into the network to cause routing disruption by creating routing loops, black holes, greyholes, or even partitioning the network. An active attacker may also attempt to consume resources belonging to other nodes by injecting extra packets in the network, consuming bandwidth and other nodes' energy. ARIADNE is introduced in to protect DSR against active attacks using TESLA. Any node within the established route must meet the predetermined trust level. A protocol is introduced to protect route discovery against fabricated, compromised, or replayed routing control packets. This protocol assumes a security association exists between the source and destination nodes only and does not make any assumption about intermediate nodes (they may exhibit malicious behavior). The scheme may fail in the presence of colluding nodes. In general, securing routing protocols can protect the network against malicious misbehavior at the network layer only, in particular with respect to route discovery and maintenance. It does not protect the network against selfish misbehavior at any layer (including the network layer) or malicious misbehavior at layers other than the network layer.

ii. *Byzantine Fault Tolerance Techniques*

The Byzantine Generals Problem is an agreement problem in which a group of generals must decide independently but unanimously whether or not to attack the army of their enemy. The generals are geographically separated. Hence, they must communicate with each other using message in order to unanimously decide whether to attack or not. The problem complication stems from the assumption that some traitors may be present amongst the generals and may attempt to corrupt the generals' decision. For example, the traitors may forge messages to trick other generals into making a decision that is not consistent with their desires or that of others, or confusing some generals so that conflicting decisions are made (i.e. some generals attack and some do not). The requirements for a solution to the problem is that all loyal generals decide upon the same plan of action (i.e. attack or not) and that a small number of traitors cannot corrupt a unanimous decision by the generals.

iii. *Cooperation Incentives*

This class of solutions applies to nodes that are rational (i.e. nodes that adopt the behavior that benefits them most). The goal of this class of solutions is to provide incentives for nodes to cooperate in such a way that rational nodes lose if they do not cooperate. In an environment where nodes are autonomous, a node's cooperation level in key network functionalities is influenced by factors like energy consumption. This is shown in , where node cooperation in ad hoc networks is studied assuming that nodes' actions are strictly determined by self-interest and that each node has a minimum lifetime constraint. Credit based systems have been proposed to incentivize nodes to cooperate in packet forwarding by offering them payments in return. Every time a node forwards a packet on behalf of another node it receives a payment from that node. Nodes are also charged when they request others to forward packets on their behalf. For a node to be able to pay others it must have enough credit, and it can obtain credit by forwarding other's packets, SPRITE, a credit-based system is introduced. A node loses credit for all packets where it is the source and gains credit when it routes packets for other nodes. This system assumes a centralized server that accounts for all packets received, transmitted, and dropped in the network and takes care

of making payments to nodes for their forwarding services and collecting payments from nodes that request forwarding services. A node using this strategy will initially cooperate, and then respond in kind to other nodes' actions. The node cooperates with other nodes that were previously cooperative, but does not cooperate with others that were not. Recent work has shown that the threat of retaliation may be effective as an incentive for node cooperation. Mechanism design is a branch of game theory that studies the design of incentives for rational nodes to act in a manner that is conducive to reaching the outcome desired by the designer. Typically, each user has a utility that may be different from the overall network utility.

iv. *Behavior Assessment*

The main goal of this class of solutions is to evaluate other nodes' behavior and build a reputation for each accordingly. This reputation can then be used to build trust in other nodes, make decisions about which nodes to interaction with, and possibly punish a node when needed. Hence, systems that fall under this class of solutions are commonly known as reputation management systems. The goal of a reputation management system in ad hoc networks is to evaluate node behavior, identify misbehaving nodes, and appropriately react to their misbehavior. Reputation nature distinguishes a reputation according to the nature of the entity it is associated with (e.g. a person, a group of people, a product, a service, an event, etc.).

Reputation role identifies the roles of the entities that participate in formation and propagation of reputation. Mainly, these entities are the evaluator, the target, the beneficiaries, and the propagators. The evaluator evaluates the behavior of a target and identifies its reputation accordingly, the beneficiaries are the entities to whom the evaluation of the target is valuable, and the propagators are the ones that propagate reputation information about a target to other entities. Information source of a reputation identifies the source of information used for evaluation. We call such a metric the evaluation metric. Reputation management systems rely on two types of evaluation metrics. The authors develop a model to stimulate cooperation in autonomous ad hoc networks in the presence of selfish and malicious nodes. In an approach that mixes between a reputation-based system and a payment-based system is introduced. Nodes monitor and evaluate their neighbors' behavior. Through a localized collaborative approach, credit is issued to nodes whose neighbors agree are cooperative. Once misbehaving nodes are detected by the majority of their neighbors, they are issued no credit and hence isolated from the network. In a sequential probability ratio test based algorithm was introduced to detect uncooperative behavior at the MAC layer in ad hoc networks. The problem of misbehavior at the MAC layer is introduced and formulated as a min max robust sequential detection problem.

c) *Evaluation Metrics for Reputation Management Systems*

In this section we discuss the evaluation metrics used to assess the performance of reputation management systems. We classify the performance metrics used to evaluate reputation management systems into efficiency metrics and effectiveness metrics. Efficiency metrics measure the impact of the reputation management system on the performance of the network. Reputation management systems may require exchange of control information amongst nodes (e.g. information used by second-hand metrics). They also perform reputation related tasks (e.g. evaluation of node behavior, isolation of misbehaving nodes) and may store reputation related information. This results in communication, computational, and storage overhead which may impact node as well as network performance. On the other hand, effectiveness metrics measure the ability of a reputation management system to reduce the impact of misbehavior as well as its accuracy in detecting misbehaving nodes. In most cases, the effectiveness as well as the efficiency of evaluation metrics is only defined qualitatively.

V. Conclusion

In this paper we have proposed a risk-aware response solution for mitigating MANET routing attacks and a novel approach to modeling attackers for ad-hoc routing protocol analysis. We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Our new model looks at attacker capabilities rather than network topology and specific attack characteristics. In doing so, our approach considered the potential damages of attacks and countermeasures and for better comparison of the security properties of existing routing protocols, as well as easier, more structured analysis of protocols developed in the future. Extensive future work remains to be done including further exploring the universal implications of specific attacker capabilities, categorizing known attacks based on the minimum attacker capabilities required, analysis of additional existing protocols, and expression of the security properties of these protocols in our model for comparative purposes 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 Références Referencias

1. Y. Sun, W. Yu, Z. Han, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.
2. M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719, May 2010.
3. P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy, 2007.
4. S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks," Proc. 10th Int'l Symp. Recent Advances in Intrusion Detection.
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.
6. 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.
7. K. Sentz and S. Ferson, "Combination of Evidence in Dempster- Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002.
8. L. Zadeh, "Review of a Mathematical Theory of Evidence," AI Magazine, vol. 5, no. 3, p. 81, 1984.
9. R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93-137, 1987.
10. 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.
11. T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.
12. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.
13. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
14. 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.
15. 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.
16. 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.
17. 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.
18. K. Fall and K. Varadhan, "The NS Manual," 2010.
19. F. Ros, "UM-OLSR Implementation (version 0.8.8) for NS2," 2007.
20. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, no. 1, pp. 21-38, 2005.
21. 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.
22. 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.
23. 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.
24. 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.
25. C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt, "A Specification-Based Intrusion Detection Model for OLSR," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06), pp. 330-350, 2006.
26. N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.
27. J. Felix, C. Joseph, B.-S. Lee, A. Das, and B. Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, pp. 233-245, Mar./Apr. 2011.
28. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 255-265, 2000.

This page is intentionally left blank