Security Challenges in MANETs and the Solution to Overcome Them

Sana Fatima
M.Tech, CNE student
T.John Institute Of Technology
Bangalore, India

Mrs Suma R.
Assistant Professor
T.John Institute Of Technology
Bangalore, India

***Abstract*— The distinctive features of mobile ad hoc networks (MANETs), including dynamic topology and open wireless medium, may lead MANETs suffering from many security vulnerabilities. Using recent advances in uncertain reasoning originated from artificial intelligence community, a unified trust management scheme is proposed that enhances the security in MANETs. In the proposed trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation, also called second hand information that is obtained from neighbour nodes of the observer node, the trust value is derived using the Dempster-Shafer theory, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method. Combining these two components in the trust model, more accurate trust values can be obtained of the observed nodes in MANETs. Throughput and packet delivery ratio can be improved significantly with slightly increased average end to- end delay and overhead of messages.**

***Keywords*— MANETs, Security, Trust Management, Un- certain Reasoning.**

I. INTRODUCTION

With recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks (MANETs) [1], [2] have become popular as a key communication technology in military tactical environments such as establishment of communication networks used to coordinate military deployment among the soldiers, vehicles, and operational command centers [3]. There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium, nomadic and distributed nature, lack of centralized infrastructure of security protection [4]–[6]. Therefore, security in tactical MANETs is a challenging research topic [7]. There are two complementary classes of approaches that can safeguard tactical MANETs: *prevention-based* and *detection- based* approaches [8]. Prevention-based approaches are studied comprehensively in MANETs [9]–[12]. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields research topic [7]. There are two complementary classes of approaches that can safeguard tactical MANETs: *prevention-based* and *detection- based* approaches [8]. Prevention-based approaches are studied comprehensively in MANETs [9]–[12]. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed, then the whole network may be paralyzed [13]. Furthermore, although prevention-based approaches can prevent misbehavior, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing estab- lishment. From the experience in the design of security in wired networks, multi-level security mechanisms are needed. In MANETs, this is especially true given the low physical security of mobile devices [14], [15]. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities [16]–[18].

Although some excellent work has been done on detection based based approaches based on trust in MANETs, most of existing approaches do not exploit direct and indirect observation (also called secondhand information that is obtained from third party nodes) at the same time to evaluate the trust of an observed node. Moreover, indirect observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node [19]–[21]. Therefore, inaccurate trust values may be derived. In addition, most methods of trust evaluation from direct observation [19], [20], [22] do not differentiate data packets and control packets. However, in MANETs, control packets usually are more important than data packets.

In this paper, we interpret trust as the degree of belief that a node performs as expected. We also recognize un- certainty in trust evaluation. Based on this interpretation, we propose a trust management scheme to enhance the security of MANETs. The difference between our scheme and existing schemes is that we use uncertain reasoning to derive trust values. Uncertain reasoning was initially proposed from the artificial intelligence community to solve the problems in expert systems, which have frequent counter-factual results [23]. The elasticity and flexibility of uncertain reasoning make it successful in many fields, such as expert systems, multi- agent systems, and data fusion [23]–[26].

II. PREVIOUS WORKS

Trust-based security schemes are important detection-based methods in MANETs, which have been studied recently [19], [20], [22], [24]–[26], [28]–[31]. In [19], [20], the trust value of a node based on direct observation is derived using Bayesian methodology. The authors of [22] regard trust as uncertainty that the observed node performs a task correctly, and entropy is used to formulate a trust model and evaluate trust values by direct observation. Compared to direct observation in trust evaluation, indirect observation or second-hand information can be important to assess the trust of observed nodes. For example, the collection of testimonies from neighbor nodes can detect the situation where a hostile node performs well to one observer, while performing poorly according to another node.

The Dempster-Shafer theory (DST) is regarded as useful mechanism in uncertain reasoning and is widely used in expert systems and multi-agent systems [24], [25]. In [26], the Dempster-Shafer theory is used in sensor fusion. Intrusion detection systems [29], [30] apply the Dempster-Shafer theory to assess unreliable information from IDS sensors.

In this paper, we use uncertain reasoning theory from artifi- cial intelligence to evaluate the trust of nodes in MANETs. Uncertainty is an old problem from gambler's world. This problem can be handled by probability theory. Reasoning is another important behavior in everyday life. A lot of researchers, even Aristotle (384 BCE - 322 BCE) (Greek Philosopher), try to understand and formulate it. Reasoning based on uncertainty has been prosperous in the artificial intelligence community due to the development of probability theory and symbolic logic. Probabilistic reasoning is intro- duced to intelligence systems [23], which is used to tackle the exceptions in automatic reasoning. In order to overcome the drawbacks of traditional rule-based systems, which are
based on truth tables with no exceptions, probabilistic rea- soning is proposed, in which the uncertainty of knowledge is considered and described as subsets of "possible worlds." Probabilistic reasoning can be used to different areas, from artificial intelligence to philosophy, cognitive psychology, and management science. In the area of security in MANETs, we find that this theory is very suitable for trust evaluation based on the trust interpretation in this paper. Bayesian inference and Dempster-Shafer evidence theory are two approaches in uncertain reasoning. We adopt them to evaluate trust of nodes by direct and indirect observation.

Trust based security systems are also studied in different network architectures, e.g., wireless sensor networks [32], [33], vehicular ad hoc networks (VANETs) [34], coopera- tive wireless networks [35], etc. Although different types of networks have different specific characteristics, the proposed trust model based on direct and indirect observation is general enough and can be customized to a particular network.

III. TRUST MODEL IN MANETS

In this section, we describe the definition and properties of trust in MANETs. Based on the definition, we depict the trust model that is used to formulate the trust between two nodes in MANETs, and present a framework of the proposed scheme. The main notations that are used in this paper are summarized in Table I.

TABLE I
MAIN NOTATIONS

Notation	Definition
T_{AB}	The total trust value that Node A gives Node B
T^S_{AB}	The trust value that Node A gives Node B based on direct observation of Node A
T^N_{AB}	The trust value that Node A gives Node B based on indirect observation of Node A
T^D_{AB}	The trust value that Node A gives Node B based on data packets
T^C_{AB}	The trust value that Node A gives Node B based on control packets
λ	The weight for the trust value based on direct observation
ρ	The weight for the trust value based on data packets
γ	A factor of punishment which is larger than or equal to 1

A. Definition and Properties of Trust

Trust has different meanings in different disciplines from psychology to economy [28]. The definition of trust in MANETs is similar to the explanation in sociology, where trust is interpreted as degrees of the belief that a node in a network (or an agent in a distributed system) will carry out tasks that it should [28]. Due to the specific characteristics of MANETs, trust in MANETs has five basic properties: subjectivity, dynamicity, non-transitivity, asymmetry, and context-dependency [28]. Subjectivity means that an observer node has a right to determine the trust of an observed node. Different observer nodes may have different trust values of the same observed node. Dynamicity means that the trust of a node should be changed depending on its behaviors. Non-transitivity means that if node A trusts node B and node B trusts node C, then node A does not necessarily trust node C. Asymmetry means that if node A trusts node B, then node B does not necessarily trust node A. Context -dependency means that trust assessment commonly bases on the behaviors of a node. Different aspects of actions can be evaluated by different trust. For example, if a node has less power, then it may not be able to forward messages to its neighbors. In this situation, the trust of power in this node will decline, but the trust of security in this node will not be changed due to its state. Reputation is another important concept in trust evaluation. Reputation reflects the public opinions from members in a community [41]. In MANETs, reputation can be a collection of trust from nodes in the network. Reputation is more global than trust from the perspective of the whole network [41].

B. Trust Model

Based on the definition and properties of trust in MANETs, we evaluate trust in the proposed scheme by a real number, T , with a continuous value between 0 and 1. Although trust and trustworthiness may be different in contexts, in which the trustor needs to consider risk [28], trust and trustworthiness

are treated the same for simplicity in the proposed scheme. In this model, trust is made up of two components: direct observation trust and indirect observation trust. These components are similar to those used in [42]. In direction observation trust, an observer estimates the trust of his one-hop neighbor based on its own opinion. Therefore, the trust value is the expectation of a subjective probability that a trustor uses to decide whether or not a trustee is reliable. It is similar to firsthand information defined by [19], [20]. We denote T_S as a trust value from direct observation and can be calculated by Bayesian inference.

If we only consider direct observation, there would be prejudice in trust value calculation. In order to obtain less biased trust value, we also consider other observers' opinions in this paper. Although opinions of neighbors are introduced in [42], the method that simply takes arithmetic mean of all trust values is not sufficient to reflect the real meaning of other unreliable observers' opinions because there are two situations that may severely disturb the effective evidence from neighbors: unreliable neighbors and unreliable observation [29]. Unreliable neighbors themselves are suspects. Even though neighbors are trustworthy, they may also provide unreliable evidence due to observation conditions. The Dempster-Shafer theory [25], [29] is a good candidate to aid in this situation, in which evidence is collected from neighbors that may be unreliable. Therefore, We denote the trust value derived from indirect observation of one-hop neighbors as T_N. Combining the trust value, T_S, from direct observation and the trust value, T_N, from indirect observation, we can get a more realistic and accurate trust value of a node in MANETs.

$$T = \lambda T_S + (1 - \lambda) T_N, \quad (1)$$

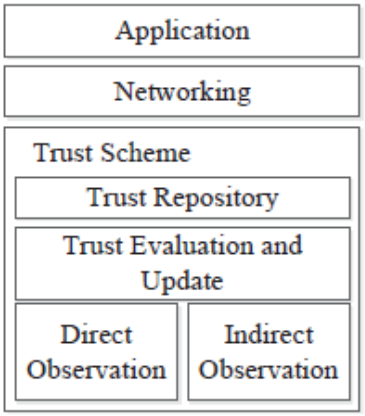

Fig. 1. The framework of the proposed scheme.

C. Framework of the Proposed Scheme

Based on the trust model, the framework of the proposed scheme is shown in Fig. 1. In the trust scheme component, the module of trust evaluation and update can obtain evidence from direct and indirect observation modules and then utilize two approaches, Bayesian inference and DST, to calculate and update the trust values. Next, the trust values are stored in the module of trust repository. Routing schemes in the networking component can establish secure routing paths between sources and destinations based on the trust repository module. The application component can send data through secure routing paths. The trust from direct observation between an observer node A and an observed node B in this trust scheme can be defined further as

$$T_{AB}^{S} = \rho T_{AB}^{D} + (1 - \rho) T_{AB}^{C}, \quad (2)$$

where ρ ($0 \leq \rho \leq 1$)is the weight for data packets; T_{DAB} is the trust value based on data packets; T_{CAB} is the trust value based on control packets. Trust from indirect observation between an observer node A and an observed node B, denoted as T_{NAB}, can be obtained by DST, which will be explained in Section V.

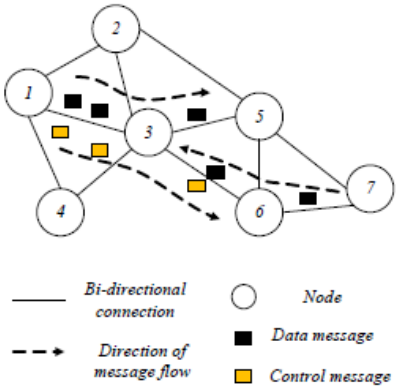

Fig. 2. An example mobile ad hoc network.

In order to explain the basic procedure of trust evaluation in our scenario, an example network is shown in Fig. 2. In this example, node 1 is an observer node and node 3 is an observed node. Node 1 sends data messages to node 5 through node 3. When node 3 receives data messages and forwards to node 5, node 1 can overhear it. Then node 1 can calculate the trust value of node 3 based on data messages. The same idea is applied to the control message situation. In the meanwhile, node 1 can collect information from node 2 and node 4, which Have interactions with node 3 in order to evaluate the trust value of node 3. This information collected from third party nodes is called indirection observation. In another situation, node 7 sends data messages to node 3, which is the destination node. Node 1 cannot overhear the data messages sent to node 3 in this situation.

IV. TRUST EVALUATION WITH DIRECT OBSERVATION

Based on the model presented in the last section, we evaluate trust values with direct observation on two malicious behaviors: dropping packets and modifying packets [40]. In the direct observation, we assume that each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviors of the observed node. Therefore, the observer node can calculate trust values of its neighbors by using Bayesian inference, which is a general framework to deduce the estimation of the unknown probability by using observation. As mentioned in the last section of trust model, the degree of belief is a random variable, denoted by Θ and 0

$\leq \theta \leq 1$. From Bayes' theorem, we can derive the following formulation

$$f(\theta, y|x) = \frac{p(x|\theta, y)f(\theta, y)}{\int_0^1 p(x|\theta, y)f(\theta, y)\,\mathrm{d}\theta}, \quad (3)$$

where x is the number of packets is forwarded correctly; y is the number of packets is received by a node; $p(x|\theta, y)$ is the likelihood function, which follows a binomial distribution

$$p(x|\theta, y) = \binom{y}{x}\theta^x(1-\theta)^{y-x}. \quad (4)$$

We assume that the prior distribution, $f(\theta, y)$, follows Beta distribution,

$$Beta(\theta; \alpha, \beta) = \frac{\theta^{\alpha-1}(1-\theta)^{\beta-1}}{\int_0^1 \theta^{\alpha-1}(1-\theta)^{\beta-1}\,\mathrm{d}\theta}, \quad (5)$$

where $0 \leq \theta \leq 1, \alpha > 0, \beta > 0$. Then we have

$$f(\theta, y|x) \sim Beta(\alpha + x, \beta + y - x). \quad (6)$$

The expectation of Beta distribution is

$$E[\Theta] = \frac{\alpha}{\alpha + \beta}. \quad (7)$$

Due to reproductivity of (6), the trust value is calculated iteratively. At the beginning, there are no observation. The prior distribution $f(\theta, y)$ is $Beta(\theta; 1, 1)$ at the beginning. Then we have

$$E_n[\Theta] = \frac{\alpha_n}{\alpha_n + \beta_n}, \quad (8)$$

where $\alpha_n = \alpha_{n-1} + x_{n-1}$, $\beta_n = \beta_{n-1} + y_{n-1} - x_{n-1}$, $\alpha_0 = \beta_0 = 1$, $n \in Z_+$. Intuitively, this situation is explained that the trust value of a node is 0.5 at the beginning. That means the node is seemed as neutral when no history records behaviors is established. The value trust can be revised continuously through follow-up observation. Past experience is also an important factor when trust values are calculated. Recent activities of a node can seriously affect the trust evaluation. Consider the case where a node has a good history of past experience, but it drops or modifies packets recently. In order to handle this, a windowing scheme is proposed. Using weighted evidence from observation is another method [19]. In our scheme, we introduce a punishment factor for reputation fading, which focuses on recent activities. The punishment factor is used to give more weights on misbehavior in the Bayesian framework. Firstly, this can lower the trust of an attacker when it misbehaves. Secondly, the trust of the attack will not recover quickly even if it forwards a large number of packets correctly due to the impact of the punishment factor. This can help the proposed scheme distinguish the malicious node quickly and avoid them disrupting the normal traffic between benign nodes again. The punishment factor is inspired by our daily lives in human society, where a scandal can badly affect a person who has a good reputation. What's more, it is hard to quickly recover a good reputation. The factor of punishment makes the trust evaluation more realistic. The punishment factor, γ, in the formula of trust evaluation in (8) is described as follows:

$$E_n[\Theta] = \frac{\alpha_n}{\alpha_n + \gamma\beta_n}, \quad (9)$$

where $\gamma \geq 1$. As the value of γ becomes larger, the trust value declines more. This is because the punishment factor gives more weight to misbehavior. Based on this deduction, TS is defined as:

$$TS = En[\Theta]. \quad (10)$$

V. TRUST EVALUATION WITH INDIRECT OBSERVATION

In this section, indirect observation from neighbor nodes used to evaluate the trust value of the observed node will be discussed. Although direct observation from an observer is important in assessing the trust value of the observed node, the testimonies from neighbor nodes are also helpful to judge the trustworthiness of the observed node. Collection of neighbors' opinions can help in justifying whether or not a node is hostile. This mechanism may reduce the bias from an observer. A situation in which a node is benign to one node but malicious to others may be mitigated. In order to implement this method, the Dempster-Shafer theory, which is a mathematical theory of evidence, is used as it is well developed for coping with uncertainty or ignorance, and it provides a numerical measurement of degrees of belief about a proposition from multiple sources [26], [30]. The core of this theory is the belief function that is based on two essential ideas: degrees of belief about a proposition can be obtained from subjective probabilities of a related question, and these degrees of belief can be combined together on condition that they are from independence evidence [24], [29]. In the indirect observation, we assume that there are more than one neighbor nodes between an observer and an observed node when the ttrust evaluation is performed with DST. We also assume that evidence provided by different neighbors is independent. First, we will introduce the theory of belief functions. Then we will discuss the rule of combining belief functions that are used to accommodate testimonies from one-hop neighbor nodes in order to assess trust values of nodes in MANETs.

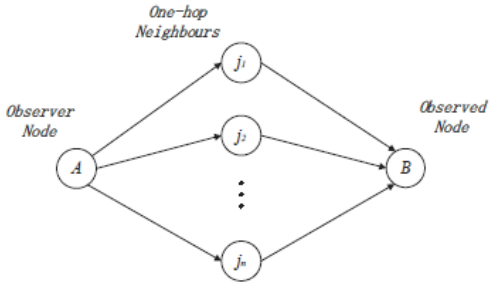

Fig. 3. A scenario for indirect observation.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a unified trust management scheme that enhances the security of MANETs. Using recent advances in uncertain reasoning, Bayesian inference and Dempster-Shafer theory, we evaluate the trust values of observed nodes in MANETs. Misbehaviors such as dropping or modifying packets can be detected in our scheme through are listed as the viewpoint of the system designers. trust values by direct and indirect observation. Nodes with low trust values will be excluded by the routing algorithm. Therefore, secure routing

path can be established in malicious environments. Based on the proposed scheme, more accurate trust can be obtained by considering different types of packets, indirect observation from one-hop neighbors and other important factors such as buffers of queues and states of wireless connections, which may cause dropping packets in friendly nodes. The results of MANET routing scenario positively support the effectiveness and performance of our scheme, which improves throughput and packet delivery ratio considerably, with slightly increased average end-to-end delay and overhead of messages. In our future work, we will extend the proposed scheme to MANETs with cognitive radios [46].

REFERENCES

[1] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations," *IETF RFC 2501*, Jan. 1999.
[2] F. R. Yu, *Cognitive Radio Mobile Ad Hoc Networks*. New York: Springer, 2011.
[3] J. Loo, J. Lloret, and J. H. Ortiz, *Mobile Ad Hoc Networks: Current Status and Future Trends*. CRC Press, 2011.
[4] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Tech.*, vol. 61, pp. 2674 –2685, July 2012.
[5] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J. Wireless Commun. Networking*, vol. 2013, pp. 188–190, July 2013.
[6] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 1616–1627, March 2014.
[7] J. Chapin and V. W. Chan, "The next 10 years of DoD wireless networking research," in *Proc. IEEE Milcom'11*, (Baltimore, MD, USA), Nov. 2011.
[8] S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," *IEEE Trans. Veh. Tech.*, vol. 60, pp. 1025 –1036, Mar. 2011.
[9] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: distributed key management for security," in *Proc. 2nd OLSR Workshop*, (Domaine de Voluceau, France), Dec. 2005.
[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable and Secure Computing*, vol. 3, pp. 386–399, Oct.–Dec. 2006.
[11] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Comm.*, vol. 16, no. 2, pp. 24–30, 2009.
[12] F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Trans. on Network and Service Management*, vol. 7, pp. 258 – 267, Dec. 2010.
[13] S. Marti, T. Giuli, K. Lai, and M. Maker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MobiCom'00*, (New York, NY, USA), Aug. 2000.
[14] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: improving network security by multipath routing in mobile ad hoc networks," *ACM Wireless Networks*, vol. 15, no. 3, pp. 279–294, Mar. 2009.
[15] R. Zhang, Y. Zhang, and Y. Fang, "AOS: An anonymous overlay system for mobile ad hoc networks," *ACM Wireless Networks*, vol. 17, no. 4, pp. 843–859, May 2011.
[16] P. Albers, O. Camp, J.-M. Percher, B. Jouga, and L. M. R. S. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in *Proc. 1st Int'l Workshop on Wireless information Systems*, (Ciudad Real, Spain), Apr. 2002.
[17] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Comm.*, vol. 11, pp. 48–60, Feb. 2004.
[18] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 3064 –3073, Sept. 2011.
[19] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems*, (Bologna, Italy), Nov. 2004.
[20] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. 3rd ACM Workshop on SASN'05*, (Alexandria, VA, USA), Nov. 2005.
[21] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol," in *Proc. ACM MOBIHOC'02*, (Lausanne, Switzerland), Jun. 2002.
[22] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, 2006.
[23] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann, 1988.
[24] G. Shafer and J. Pearl, *Readings in Uncertain Reasoning*. Morgan Kaufmann, 1990.
[25] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proc. ACM AAMAS'02*, (Bologna, Italy), Jul. 2002.
[26] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using Dempster-Shafer theory," in *Proc. IEEE Instrumentation and Measurement Technology Conf.*, (Alaska, USA), May 2002.
[27] T. Clausen, C. Dearlove, and P. Jacquet, "The optimized link state routing protocol version 2," *IETF draft-ietf-manet-olsrv2-13*, Oct. 2011.
[28] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.
[29] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 35–41, 2005.
[30] S. Bu, F. Yu, P. Liu, P. Mason, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high security mobile ad-hoc networks," *IEEE Trans. Veh. Tech.*, vol. 60, no. 3, pp. 1025–1036, 2011.
[31] R. Changiz, H. Halabian, F. R. Yu, I. Lambadaris, and H. Tang, "Trust establishment in cooperative wireless relaying?networks," *Wireless Communications and Mobile Computing*, 2012.
[32] H. Deng, Y. Yang, G. Jin, R. Xu, and W. Shi, "Building a trust-aware dynamic routing solution for wireless sensor neworks," in *Proc. IEEE GLOBECOM'10 Workshop on Heterogeneours, Multi-hop Wireless and Mobile Networks*, (Miami, FL, USA), Dec. 2010.
[33] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM SASN'04*, (Washington, D.C., USA), Oct. 2004.
[34] M. Raya, P. Papadimitratos