A Survey on Trust Management for Mobile Ad Hoc Networks

Jin-Hee Cho, *Member, IEEE,* Ananthram Swami, *Fellow, IEEE,* and Ing-Ray Chen, *Member, IEEE*

***Abstract*—Managing trust in a distributed Mobile Ad Hoc Network (MANET) is challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability, availability, scalability, and reconfigurability. In defining and managing trust in a military MANET, we must consider the interactions between the composite cognitive, social, information and communication networks, and take into account the severe resource constraints (e.g., computing power, energy, bandwidth, time), and dynamics (e.g., topology changes, node mobility, node failure, propagation channel conditions). We seek to combine the notions of "social trust" derived from social networks with "quality-of-service (QoS) trust" derived from information and communication networks to obtain a composite trust metric. We discuss the concepts and properties of trust and derive some unique characteristics of trust in MANETs, drawing upon social notions of trust. We provide a survey of trust management schemes developed for MANETs and discuss generally accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs. Finally, we discuss future research areas on trust management in MANETs based on the concept of social and cognitive networks.**

***Index Terms*—Trust management, mobile ad hoc networks, social networks, cognitive networks, trust, trust metrics.**

I. Introduction

IN AN INCREASINGLY networked world, increased connectivity could lead to improved information sharing, facilitate collaboration, and enable distributed decision making, which is the underlying concept in Network Centric Operations. In mobile ad hoc networks (MANETs), the distributed decision making should take into account trust in the elements: the sources of information, the processors of information, the elements of the communications network across which the information is transmitted, etc. This trust must often be derived under time-critical conditions, and in a distributed way.

A. Design Challenges in MANET Protocols

A mobile ad hoc network [1] consists of wireless mobile nodes forming a temporary network without the help of centralized infrastructure, and where nodes communicate through multi-hops.

Security protocol designers for MANETs face technical challenges due to severe resource constraints in bandwidth, memory size, battery life, computational power, and unique wireless characteristics such as openness to eavesdropping, lack of specific ingress and exit points, high security threats, vulnerability, unreliable communication, and rapid changes in topologies or memberships because of user mobility or node failure [1][2][3]. In addition, compared with designing security protocols for civilian MANETs, designing security protocols for military MANETs requires additional caution, since battlefield communication networks must cope with hostile environments, node heterogeneity, often stringent performance constraints, node subversion, high tempo operations leading to rapid changes in network topology and service requirements, and dynamically formed communities of interest wherein participants may not have predefined trust relationships [4]. To cope with these dynamics, networks must be able to reconfigure seamlessly, via low-complexity distributed network management schemes [3]. Security in a tactical network includes notions of communication security which can be easily quantified as opposed to the perception of security which is hard to quantify.

B. Motivation for Trust Management in MANETs

The concept of "Trust" originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [5]. Blaze *et al*. [6] first introduced the term "Trust Management" and identified it as a separate component of security services in networks and clarified that "Trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships."

Trust management in MANETs is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves. Examples would be in building initial trust bootstrapping [7], coalition operations without predefined trust, and authentication of certificates generated by another party when links are down or ensuring safety before entering a new zone [8]. In addition, trust management has diverse applicability in many decision making situations including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes.

Trust management, including trust establishment, trust update, and trust revocation, in MANETs is also much more challenging than in traditional centralized environments. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only

Manuscript received 29 September 2009; revised 1 March 2010, 28 June 2010, and 7 July 2010.

Jin-Hee Cho and Ananthram Swami are with the Computational and Information Sciences Directorate, U.S. Army Research Laboratory, 2800 Powder Mill Rd., Adelphi, Maryland 20783, USA (e-mail: {jinhee.cho, ananthram.swami}@us.army.mil).

Ing-Ray Chen is with the Department of Computer Science, Virginia Polytechnic Institute and State University, 7054 Haycock Road, Falls Church, VA 22043, USA (e-mail: irchen@vt.edu).

Digital Object Identifier 10.1109/SURV.2011.092110.00088

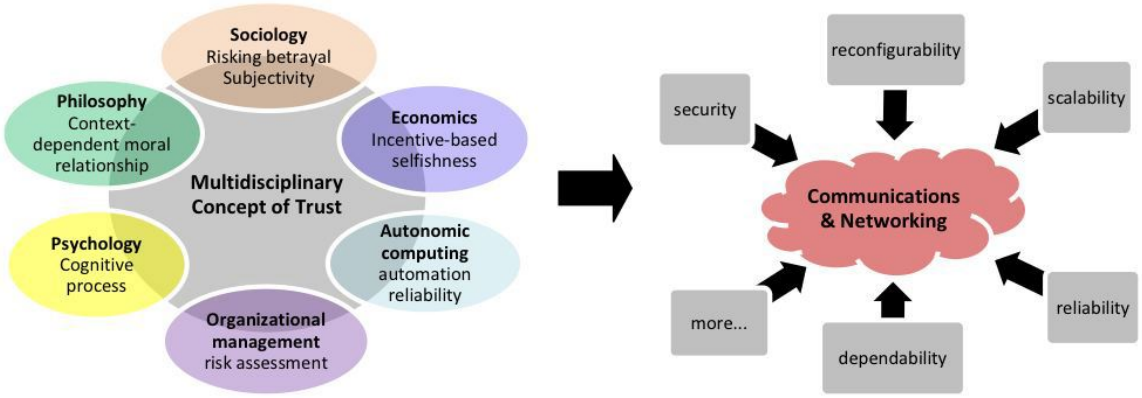

Fig. 1. The multidisciplinary concept of trust and its application in communications and networking.

to local information. The dynamic nature and characteristics of MANETs result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time [8] [9]. Despite a couple of surveys of trust management [10] [11] [12], a comprehensive survey of trust management in MANETs does not exist and is the main aim of this paper. A short version of this paper was presented at ICCRTS 2009 [13]. The contributions of this paper are: (1) to give a clear definition of trust in the communication and networking field, drawing upon definitions from different disciplines; (2) to extensively survey the existing trust management schemes developed for MANETs and investigate their general trends; and (3) to discuss future research areas based on the concept of social and cognitive networks.

The rest of this paper is organized as follows. In Section 2, we discuss the concept of *trust* in diverse disciplines, give a clear distinction between trust and trustworthiness, and discuss the relationship between trust and risk. We also introduce the main properties of trust in MANETs. Section 3 surveys generally accepted classifications of trust management, attacks considered in existing trust management schemes for MANETs, and metrics used to measure the performance of existing MANET trust management schemes. Section 4 surveys trust management schemes that have been developed for specific purposes, including secure routing, authentication, intrusion detection, access control, key management, and trust evidence distribution and evaluation. In Section 5, we discuss design concepts that designers of MANET trust management systems should keep in mind and suggest trust metrics based on the concepts of social trust and quality-of-service (QoS) trust. Section 6 concludes this paper.

II. Concepts and Properties of Trust

In this section, we review how trust is defined in different disciplines and how these trust concepts can be applied in modeling trust in MANETs. Further, we examine the relationship between trust and risk, and how trust should be defined in order to realistically reflect the unique characteristics of MANETs.

A. Multidisciplinary Concept of Trust

According to *Merriam Webster's Dictionary* [14], trust is defined as "assured reliance on the character, ability, strength, or truth of someone or something." Despite the subjective nature of trust, the concept of trust has been very attractive to network security protocol designers because of its diverse applicability as a decision making mechanism. We examine the literature to study how trust is defined in various disciplines including sociology, economics, philosophy, psychology, organizational management, and autonomic computing in industrial and system engineering. Finally, we also examine how trust can be defined in communications and networking with the help of definitions in other fields.

Trust in sociology: Gambetta's notion of trust [15] is popularly called *sociological trust* and is defined as an assessor's a priori subjective probability that a person (or agent, or group) will perform specific actions that affect the assessor. That is, Gambetta [15] describes the nature of trust as subjectivity, an indicator for future actions, and dynamicity based on continuous interactions between two entities. Luhmann [16] also emphasized the importance of trust in society as a mechanism for building cooperation among people to extend human interactions for future collaboration. Adams *et al*. [17] rephrased Gambetta's trust concept in applying the sociological concept of trust in computer science; they represented trust as a continuous variable, quantifying trust in the light of context or acceptance of risk. They further stressed that risking betrayal is an important aspect in building trust. To be useful, network trust models must capture this subjective aspect of social trust.

Trust in economics: Economists distinguish between the personal, informal trust that comes from being friendly with your neighbors and the impersonal, institutionalized trust that lets you give your credit card number out over the Internet [18]. Both notions of trust are important in military MANETs. In economics, trust is represented as an expectation that applies to situations in which trustors take risky actions under uncertainty or information incompleteness [19]. However, as illustrated in the *Prisoner's Dilemma (PD) game* [20], trust in economics is based on the assumption that humans are rational and strict utility maximizers of their own interest or incentives. In this sense, when we apply a human trust model to a network trust model, the assumption of selfish nodes seems reasonable. But altruistic behaviors can emerge from mechanisms that may be initially purely selfish [21], and thus making an argument for redemption mechanisms. Economic models are used in

conjunction with trust-based encryption primitives in [22] to develop a trust management paradigm for securing information flows across organizations.

Trust in philosophy: According to the *Stanford Encyclopedia of Philosophy* [23], trust is important but dangerous. Since trust allows us to form relationships with others and to rely on others for love, advice, help, etc., trust is regarded as a very important factor in our life that compels others to give us such things with no outside force such as the law. On the other hand, since trust requires taking a risk that the trustee may not behave as the trustor expects, trust is dangerous implying the possible betrayal of trust. In his comments on Lagerspetz's book titled *Trust: The Tacit Demand, Lahno* [24] describes the author's view on trust as a moral relationship in human society. Langerspetz believes that investigations of trust reveal that "human individuals, their beliefs, desires and actions are only intelligible against the background of existing social practices and social ties" [24]. This implies that depending on the nature of personal relationships between a trustor and a trustee (i.e., moral relationship between them), trustful actions or betrayal can occur.

Trust in psychology: According to the *Wikipedia* definition of trust in psychology [25], trust starts from the birth of the child. As the child grows older, trust also grows stronger. However, the root of trust derives from the relationship between mother (or caregiver) of the child since the strength of the family relies on trust, if the child is raised in a family which is very accepting and loving, the child also returns those feelings to others by trusting them. But if trust is lost, it is hard to regain it. In this sense, trust in psychology emphasizes the cognitive process that human beings learn trust from their experiences. Deutsch [26] defines trust as the confidence that one will find what is desired from another rather than what is feared. An individual may be said to have trust in the occurrence of an event if he expects its occurrence and his expectation leads to the behavior which he perceives to have greater negative consequences if the expectation is not confirmed than positive consequences if it is confirmed. In addition, Hardin [27] and Rotter [28] observed in their experiments that past experience may strikingly affect later capacity for trust. For example, bad experience with people will lower the trust level, leading to fewer trusted relationships with people, and thus fewer opportunities for mutual gain. Further, they recognized that the gains obtained by having high trust relationships exceed the loss by having low trust relationships. For instance, high trustors are less likely to lie or cheat or steal. Also they are less likely to be unhappy, conflicted, or unstable, and sought by more friends. Even though high trustors are deceived more often in novel situations, low trustors are also fooled equally by distrusting trustworthy people, thereby losing the advantages that high trustors may have [28].

Trust in organizational management: In this field, the concept of trust is also defined as the extent to which one party is willing to count on someone or something with a feeling of relative security in spite of possible negative consequences, emphasizing the possibility of facing risk [29]. Schoorman *et al*. [30] defined trust as the willingness to take a risk or willingness to be vulnerable in the relationship in terms of ability, integrity, and benevolence. They also explained that trust is not necessarily mutual and is not reciprocal. Trust concepts in organizational management can give us insights on how to measure trust by investigating methods to measure ability, integrity, and benevolence of each networked node, as well as on assessing risk. They can also give us insights on defining group trust (i.e., between a person and a group or between groups) which is important for dynamic communities of interest.

Trust in autonomic computing: As technology becomes more complex, fully understanding automation becomes infeasible, if not impossible, and trust in automation becomes critical, particularly when unexpected situations arise and system responses cannot be predicted. Researchers studying autonomic computing in industrial systems engineering have sought to develop models of trust to understand how trust in automation develops and how it may be misplaced. Lee and See [31] define trust as the attitude that an agent will help accomplish an individual's goals in a situation with uncertainty and vulnerability. In this sense, an agent can be automation or another person that actively interacts with the environment on behalf of the person. Parasuraman [32] links the level of trust with automation reliability stating that "Trust often determines automation usage. Operators may not use a reliable automated system if they believe it to be untrustworthy." The notion of automation reliability as a trust metric is one that is applicable in MANETs, where the user's trust in reliability on technology is an important aspect.

Trust in communications and networking: The concept of trust also has been attractive to communication and network protocol designers where trust relationships among participating nodes are critical in building cooperative and collaborative environments to optimize system objectives in terms of scalability, reconfigurability, and reliability (i.e., survivability), dependability, or security. According to Eschenauer *et al*. [9], trust is defined as "a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities." Capra [34] proposes to use a human trust model based on human interactions in a trust model for fully distributed network environments such as MANETs. Capra defines trust as the degree of a belief about the behavior of other entities (or agents). Li and Singhal [35] define trust as the belief that an entity is capable of performing reliably, dependably, and securely in a particular case; hence, different levels of trust exist *in different contexts*. For example, Alice may trust her physician to give her advice on her health concerns but may not trust her physician's advice on fixing her car. Aivaloglou *et al*. [36] describe trust as the quantified belief of a trustor regarding competence, honesty, security, and dependability of a trustee in a specific context.

Recently, researchers have recognized the importance of *social networks* in building trust relationships among entities. Golbeck [37][38][39] introduces the concept of social trust by suggesting the use of social networks as a bridge to build trust relationships among entities. Golbeck proposes the application of a trust concept derived from a sociological

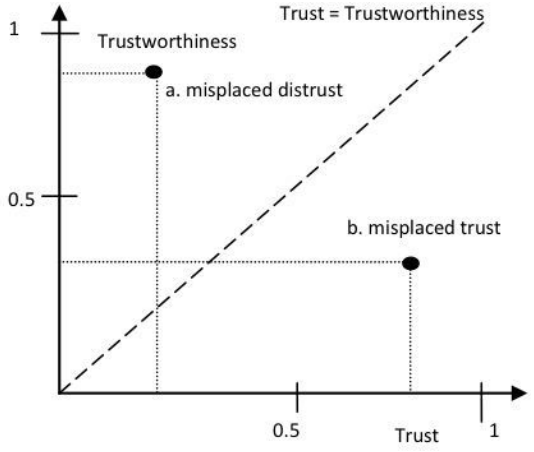

Fig. 2. Trust level [42].

viewpoint to computer science, and describes trust as a well-defined descriptor of security and encryption as a metric to reflect security goals. Wong and Sycara [40] introduce security mechanisms to establish trust in multi-agent systems. They are concerned with both authenticating agents as well as ensuring that agents do not misbehave. Trustworthiness emerges from the security features in their system.

From the definitions of trust derived from various fields as reviewed above, we can construct a trust metric having the following characteristics: (1) trust should be established based on potential risks; (2) trust should be context-dependent; (3) trust should be based on each party's own interest (e.g., selfishness); (4) trust is learned (i.e., a cognitive process); and (5) trust may represent system reliability.

B. Trust, Trustworthiness, and Risk

In the literature, the terms trust and trustworthiness seem to be used interchangeably without clear distinction. Josang *et al.* [41] clarified the difference between trust and trustworthiness based on definitions provided by Gambetta [15]. *Level of trust* is defined as the belief probability varying from 0 (complete distrust) to 1 (complete trust) [41]. In this sense, trustworthiness is a measure of the actual probability that the trustees will behave as expected. Solhaug *et al.* [42] define *trustworthiness* as the objective probability that the trustee performs a particular action on which the interests of the trustor depend.

Figure 2 [42] explains how trust (i.e., subjective probability of trust level) and trustworthiness (i.e., objective probability of trust level) can differ and how the difference affects the level of risk the trustor needs to take. The diagonal dashed line is assumed to be marks of well-founded trust in which trust is equivalent to trustworthiness.

Depending on the extent to which the trustor is ignorant about the difference between the believed (i.e., trust) and the actual (i.e., trustworthiness) probability, there is a miscalculation of the involved risk. That is, the subjective aspect of trust results in incorrect risk estimation and improper risk management accordingly. Figure 2 shows the cases in which the probability is miscalculated. In the area below the diagonal line, there is *misplaced trust* to various degrees that the perceived trust is higher than the actual trustworthiness. Even though risk is an intrinsic characteristic of trust even in well-founded trust, misplaced trust increases risk and thus enhances the chance of deceit as well, as shown in the example marked with *b* in Figure 2. On the other hand, when the perceived trust is lower than the actual trustworthiness as shown in the example marked with *a*, the trustee is distrusted more than warranted. In this case, the trustor may lose potentially good opportunities to cooperate with partners with high trustworthiness.

From the above discussions, we can conclude that careful risk estimation is closely linked with building accurate trust relations among participating entities in networks. However, Josang *et al.* [41] argue that objective trust may not be applicable to decision making in real situations. They define two interesting types of trust: 1) a context independent *reliability trust* which measures the perceived reliability by another party regardless of the situations which the trustor might face by recognizing possible risk; 2) *decision trust* as "the extent to which a given party is willing to depend on something or somebody in a given situation with a feeling of relative security even though negative consequences are possible." Decision trust deals with components such as utility and risk attitude. As an example, one may not trust an old rope for climbing down from the 3rd floor of a building during a fire exercise (i.e., reliability trust) while trusting the rope in a real fire (i.e., decision trust).

The relationship between trust and risk has been investigated in [41][42]. Figure 3 shows an example of three different risk values: low, medium, and high. The value of risk is low for all trust values when the stake is close to zero. Similarly, if the stake is too high, risk is regarded as high regardless of the estimated trust value. Risk is generally low when the trust value is high. However, the risk value should be determined based on the value at stake (e.g., risk probability) since as shown in Figure 3, high risk exists even for the case of trust value = 1. Also important are the aspects (or probability) of opportunity and prospect (or the positive consequence of an opportunity) [41][42]. To buy rubber is to do risky business, but it also gives the opportunity of selling refined products with net profit. The purchaser of rubber should estimate her/his acceptable risk level in terms of the calculated prospects. Josang *et al.* [41] and Solhaug *et al.* [42] conclude that trust is generally neither proportional nor inversely proportional to risk.

Some researchers have commented that trust and uncertainty are intimately linked - trust is a mechanism to cope with uncertainty. The level of uncertainty in the information used as trust evidence will also considerably influence the accuracy of trust evaluation [43].

C. Trust Properties in MANETs

Due to the unique characteristics of MANET environments and the inherent unreliability of the wireless channel, the concept of trust in MANETs should be carefully defined. The main properties of trust in MANET environments can be summarized as follows (see Figure 4):

First, trust is *dynamic*, not static. Trust establishment in MANETs should be based on temporally and spatially local

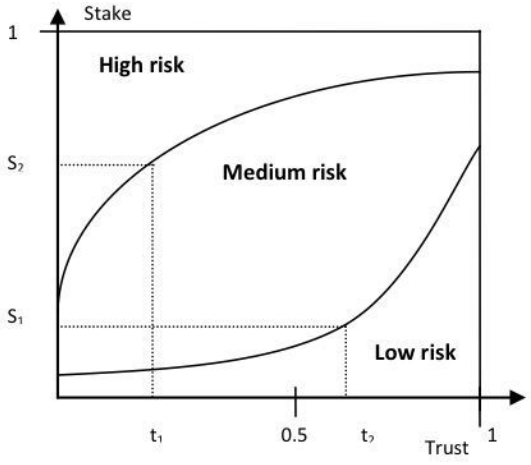

Fig. 3. Risk and trust [41].

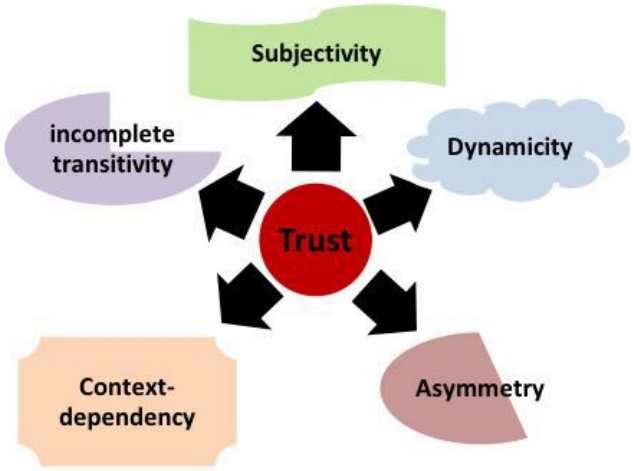

Fig. 4. Trust properties in MANETs.

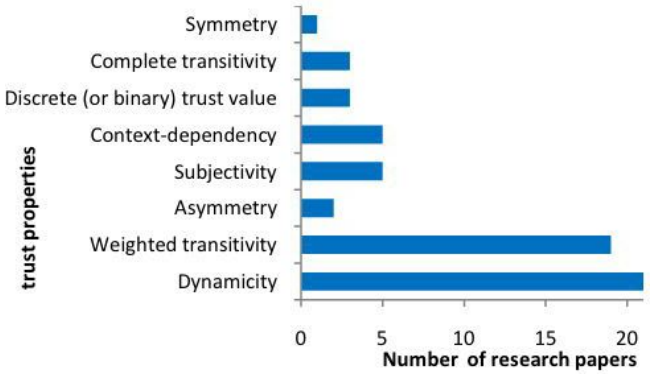

Fig. 5. Trust properties in trust management schemes in MANETs.

information: due to node mobility or failure, information is typically incomplete and can change rapidly [8][32]. Adams *et al*. [44] point out that in order to capture the dynamicity of trust, trust should be expressed as a continuous variable, rather than as a binary or even discrete-valued entity. A continuous valued variable can represent uncertainty better than a binary variable.

Second, trust is *subjective* [45]. In MANET environments, a trustor node may determine a different level of trust against the same trustee node due to different experiences with the node derived from a dynamically changing network topology.

Third, trust is *not necessarily transitive* [46]. For example, if A trusts B, and B trusts C, it does not guarantee A trusts C. In order to use the transitivity of trust between two entities to a third party, a trustor should maintain two types of trust: trust in a trustee and trust in the trustee's recommendation of the third party. For example, Alice may trust Bob about movies, but not trust him at all to recommend other people whose opinion about movies is worth considering or not trust other people that Bob recommended as much as she trusts Bob.

Fourth, trust is *asymmetric*, not necessarily reciprocal [44]. In heterogeneous MANETs, nodes with higher capability (e.g., more energy or computational power) may not trust nodes with lower capability at the same level that nodes with lower capability trust nodes with higher capability. As a typical example in organizational management, a supervisor tends to trust an employee less than the employee trusts the supervisor.

Fifth, trust is *context-dependent* [33]. For example, A may trust B as a wine expert but not as a car fixer. Similarly in MANETs depending on the given task, different types of trust (e.g., trust in computational power or trust in unselfishness, trust in forwarding versus trust in reporting) are required.

Figure 5 shows how several trust properties are considered in the literature. Dynamicity and weighted transitivity are most often considered. However, we notice that some existing work does not even consider trust properly; some represent trust as a discrete variable, while others assume that trust is symmetric or completely transitive. As such they do not capture characteristics of trust in a MANET. Further, we could not find any prior work that comprehensively considers all five properties of trust shown in Figure 5. Note that Figure 5 is based on 36 papers and each work may consider multiple trust properties.

In order to properly take into account these unique characteristics of trust in MANETs as described above, any trust-based framework for MANETs should consider the following as well:

First, a decision procedure to determine the trust of an entity should be *fully distributed* based on cooperative evaluation with uncertain and incomplete evidence, since one cannot rely on a trusted third party such as a trusted centralized certificate authority to take care of trust management as in wired networks [8][9][34].

Second, trust should be determined in a *highly customizable way* (e.g., flexible to membership changes and to deployment scenarios) without causing disruption to the device computation and communication resources while capturing the various and complicated natural components of an individual's trust into a network model [34][47].

Third, a trust decision framework should not assume that all nodes are cooperative [34]. In resource-restricted environments, *selfishness* is likely to be prevalent over cooperation, for example, in order to save battery life or computational power. Thomas *et al*. [48] discuss the tradeoff between selfishness and altruism of participating nodes in MANETs in terms of prolonging system lifetime (e.g., with system lifetime defined

as the time to a node's death due to energy exhaustion) versus reducing selfish behaviors to enhance system throughput.

Finally, trust should be established in a *self-organized reconfigurable way* in order not to be disrupted by the dynamics of MANET environments [8][48]. In addition to the characteristics mentioned above, trust-based frameworks for MANETs should consider the tradeoff issues between security and performance including reliability, fault tolerance, scalability, and energy consumption where resources are restricted but security vulnerability is relatively high.

III. Classifications, Potential Attacks, and Metrics for MANET Trust Management

This section discusses classifications, attacks and performance metrics for MANET trust management. Before reviewing the literature, we would like to clarify some terminologies that have been used interchangeably but sometimes confusingly in the context of trust management.

In general, the term *trust management* is interchangeably used with the term *reputation management* [35]. However, there is a slight difference between trust and reputation. According to Liu *et al*. [49], trust is active while reputation is passive. That is, *trust* is a node's belief in the trust qualities of a peer, thus being extended from a node to its peer. *Reputation* is the perception that peers form about a node. Further, Ruhomaa *et al*. [10] distinguish trust from reputation, noting that trust puts an emphasis on risk and incentives while reputation focuses on a perception that a party creates through past actions about its intentions in the context of the norms effective within a community. Also, recommendation is frequently used as a way to measure trust or reputation. *Recommendation* is simply an attempt at communicating a party's reputation from one community context to another [45][10].

A working definition of trust for Internet applications, and a survey of trust management schemes for such applications may be found in [12].

In most of the literature, reputation management is regarded as part of trust management. Further, the terms *trust management* and *trust establishment* are also interchangeably used. To clarify these two terms, according to Aivaloglou *et al*. [36], trust establishment is a process to deal with the representation, evaluation, maintenance, and distribution of trust among nodes.

Trust management deals with problems such as the formulation of evaluation rules and policies, representation of trust evidence, and evaluation and management of trust relationships among nodes. As Figure 6 explains, trust establishment is one of several trust management tasks.

A. Classifications

According to Solhaug *et al*. [42], trust management is a special case of risk management with a particular emphasis on authentication of entities under uncertainty and decision making on cooperation with unknown entities. However, the application of trust management has been extended from authentication to various aspects of communications and networking, including secure routing for isolating malicious or selfish nodes, intrusion detection, key management, access control, and other decision making mechanisms. Trust management includes trust establishment (i.e., collection of appropriate trust evidence, trust generation, trust distribution, trust discovery, and evaluation of trust evidence), trust update, and trust revocation [50] [42]. This section surveys popularly used classifications of trust management (or establishment).

Li *et al*. [51] and Li *et al*. [52] classify trust management as *reputation-based framework* and *trust establishment framework*. A reputation-based framework uses direct observations and second-hand information distributed among nodes in a network to evaluate a node. A trust establishment framework evaluates neighboring nodes based on direct observations while trust relations between two nodes without prior direct interactions are built through a combination of opinions from intermediate nodes.

Yonfang [53] suggests two different approaches to evaluate trust: *policy-based trust management* and *reputation-based trust management*. Policy-based trust management is based on strong and objective security schemes such as logical rules and verifiable properties encoded in signed credentials for access control of users to resources. In addition, the access decision is usually on the basis of mechanisms having a well-defined trust management language that has strong verification and proof support. Such a policy-based trust management approach usually makes a binary decision according to which the requester is trusted or not, and accordingly the access request is allowed or not. Due to the binary nature of trust evaluation, policy-based trust management has less flexibility. Furthermore, the availability of (or access to) trusted certificate authorities (CA) cannot always be guaranteed, particularly for distributed systems such as MANETs. On the other hand, reputation-based trust management utilizes numerical and computational mechanisms to evaluate trust. Typically, in such a system, trust is calculated by collecting, aggregating, and disseminating reputation among the entities.

According to Li and Singhal [35], trust management can be classified as *evidence-based trust management* and *monitoring-based trust management*. Evidence-based trust management considers anything that proves trust relationships among nodes: these could include public key, address, identity, or any evidence that any node can generate for itself or other nodes through a challenge and response process. Monitoring-based trust management rates the trust level of each participating node based on direct information (e.g., observing the benign or malicious behaviors of neighboring nodes, such as packet dropping, and packet flooding leading to excessive resource consumption in the network, or denial of service attacks) as well as indirect information (e.g., reputation ratings, such as recommendations forwarded from other nodes).

Aivaloglou *et al*. [36] classify two types of trust establishment frameworks for MANETs: *certificate-based framework* versus *behavior-based framework*. In the former, mechanisms are defined for pre-deployment knowledge of trust relationships within the network, using certificates which are distributed, maintained and managed, either independently or cooperatively by the nodes. Trust decisions can be made based on a valid certificate that proves trustworthiness of the target node by a certificate authority or by other nodes that the issuer

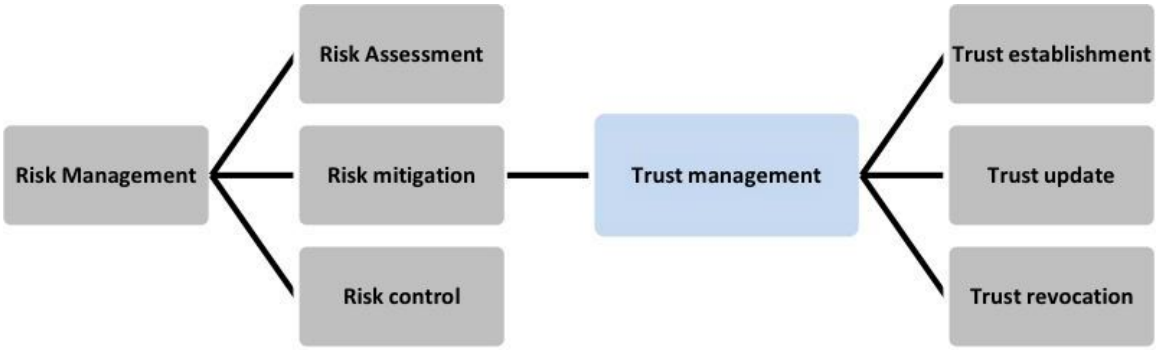

Fig. 6. Definition of trust management.

trusts. In behavior-based framework, each node continuously monitors behaviors of its neighboring nodes in order to evaluate trust. The behavior-based framework is a reactive approach, operating under the assumption that the identities of nodes in the network are ensured by preloaded authentication mechanisms. For example, if a node uses network resources in an unauthorized way, it will be regarded as a selfish or malicious node, and will finally be isolated from other nodes.

Aivaloglou *et al*. [36] also classify trust establishment schemes in terms of the type of architectures used: *hierarchical framework* versus *distributed framework*. In the former, a hierarchy exists among the nodes based on their capabilities or levels of trust. In this framework, centralized certificate authorities or trusted third parties are usually provided for on-line or off-line evidence. Such a centralized infrastructure does not exist in a distributed framework; hence, each node has some, possibly equal, responsibility for acquiring, maintaining, and distributing trust evidence.

Even though reputation management is part of trust management, many researchers further classify reputation management schemes. Adams *et al*. [44] propose three types of reputation systems: positive reputation, negative reputation, and a combination of the two. Positive reputation systems only consider observations or feedback of the positive behaviors of a node. Negative reputation systems only record complaints or observations of the negative behaviors of a node. Peers are assumed to be trusted and so feedback on behaviors is used to negatively reflect a node's reputation. To complement the drawbacks of these mechanisms, hybrid reputation systems have been proposed [53]. For more information on reputation management, the readers may refer to [11].

B. Potential Attacks

It is important to ensure that a trust management system itself should not be easily subverted, attacked or compromised. In this section, we discuss various common attacks and describe features important from the viewpoint of trust management. A survey of threat models and specific attacks on ad hoc routing protocols are described by Argyroudis *et al*. [54] and Djenouri *et al*. [55].

Liu *et al*. [49] describe the characteristics of attacks in MANETs by both the nature of attacks and the type of attackers. One classification of attacks is *passive attack* versus *active attack*. A passive attack occurs when an unauthorized party gains access to an asset but does not modify its content. Passive attacks include eavesdropping and traffic analysis (e.g., traffic flow analysis). *Eavesdropping* indicates that the attacker monitors transmissions of message content. *Traffic analysis* refers to analyzing patterns of data transmission. An active attack occurs when an unauthorized party modifies a message, data stream, or file. Active attacks usually take the form of one of the following four types or combinations: masquerading (i.e., impersonation attack), replay (i.e., retransmitting messages), message modification, and denial-of-service (DoS) (leading to excessive resource consumption in the network).

Yet another way to characterize attacks is based on the legitimacy of an entity in a network: *insider attack* versus *outsider attack* [56]. If an entity is authorized to access system resources but employs them in a malicious way (e.g., in a way not approved by the authorizer), it is classified as an insider attack. More specifically, inside attackers exploit bugs in privileged system programs or poorly configured privileges, and then they may install backdoors or Trojan horses or other such mechanisms to facilitate subsequent acquisition of privileged access. On the other hand, an outsider attack is initiated by an unauthorized or illegitimate user. They usually acquire access to an authorized account and try to perpetrate insider attacks. Both attackers may spoof network protocols to effectively acquire access to an authorized account.

Many trust management schemes are devised to detect misbehaving nodes, both selfish nodes as well as malicious nodes. Specific attack examples are described as follows (the list is representative, not exhaustive):

- ***Routing loop attacks***: A malicious node may modify routing packets in such a way that packets traverse a cycle and so do not reach the intended destination [56].
- ***Wormhole attacks***: A group of cooperating malicious nodes can pretend to connect two distant points in the network with a low-latency communication link called a wormhole link, causing disruptions in normal traffic load and flow [57][58][59].
- ***Blackhole attacks***: A malicious node, the so called black hole node, may always respond positively to route requests even when it does not have proper routing information. The black hole can drop all packets forwarded to it [60].
- ***Grayhole attacks***: A malicious node may selectively drop packets [61], as a special case of a black hole attack. For

example, the malicious node may forward routing packets but not data packets. Similarly, a *sinkhole attacker* attracts nodes to route through it and then selectively routes packets [49].

- ***DoS attacks***: A malicious node may block the normal use or management of communications facilities, for example, by causing excessive resource consumption [62].
- ***False information* or *false recommendation***: A malicious node may collude and provide false recommendations/information to isolate good nodes while keeping malicious nodes connected. In the *stacking attack*, a malicious node keeps complaining about a peer node and creates the peer's negative reputation [44][63].
- ***Incomplete information***: A malicious node may not cooperate in providing proper or complete information. Usually compromised nodes collude to perform this attack. However, node mobility or link failure, prevalent in MANETs, may also result in the same phenomenon [8][34].
- ***Packet modification/insertion***: A malicious node may modify packets or insert malicious packets such as packets with incorrect routing information [64].
- ***Newcomer attacks***: A malicious node may discard its bad reputation or distrust by registering as a new user. The malicious node simply leaves the system and joins again for trust revocation, flushing out its previous bad history and starting to accumulate new trust [65].
- ***Sybil attacks***: A malicious node can use multiple network identities which can affect topology maintenance and fault tolerant schemes such as multi-path routing [61][49][46].
- ***Blackmailing***: A malicious node can blackmail another node by disseminating false information that another node is malicious or misbehaving. This can generate significant amount of traffic and ultimately disrupt the functionality of the entire network [49]. This attack can be seen as false accusation plus DoS attacks in the sense that false information is disseminated leading to a significant amount of resource consumption.
- ***Replay attacks***: A malicious node may replay earlier transmitted packets. If the packets include data, this should not cause trouble, and the receiving node just discards erroneous packets. However, if the adversary replays route requests, routing table information would become erroneous, and old locations and routing information might make nodes unreachable [56].
- ***Selective misbehaving attacks***: A malicious node behaves badly but selectively to other nodes [66].
- ***On-off attacks***: A malicious node may alternatively behave well and badly to stay undetected while disrupting services [66].
- ***Conflicting behavior attacks***: A malicious node may behave differently to nodes in different groups to make the opinions from the different good groups conflicting, and ultimately lead to non-trusted relationships [52].

Figure 7 shows various attacks considered in a survey of 43 papers. Note that the "general selfish" category means no specific information is given in the work except that it deals with selfish nodes. Also papers in the "general misbehaving" category deal with a broad range of misbehaving nodes, including malicious and selfish nodes, but do not provide detailed information. "Packet related" attacks include packet dropping, packet modification, packet insertion, and selective packet forwarding. "Identity related" attacks include impersonation, masquerading, and Sybil attacks. Except for the "general selfish" and "general misbehaving" categories, we notice that "false information" (e.g., including false recommendation or reputation) and "packet related" attacks are dominantly considered in the literature on trust management schemes for MANETs. Figure 7 illustrates that most of the attacks considered in the literature on trust management are general attacks often targeted at other aspects of MANETs. Hence, the trust evaluation engine should be robust and degrade gracefully if some information or evidence does not provide a certain level of trust based on partial or potentially corrupted information.

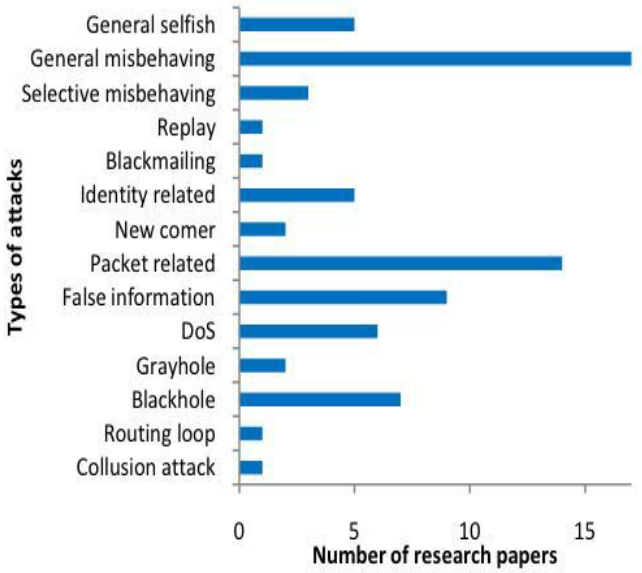

Fig. 7. Attacks considered in existing trust management systems in MANETs.

C. Metrics for MANET Trust Management

Although many trust management schemes have been proposed to evaluate trust values, no work clearly addresses what should be *measured* to evaluate network trust. Liu *et al.* [49] defined trust in their model as reliability, timeliness, and integrity of message delivery to the intended next-hop. Also most trust-based protocols for secure routing calculated trust values based on the characteristics of nodes behaving properly at the network layer. Trust measurement can be application-dependent and will be different based on the design goals of proposed schemes.

Based on 31 papers, Figure 8 shows various performance metrics that have been used to evaluate trust management schemes for MANETs. Note that a single work may use multiple performance metrics. Figure 8 shows standard system performance metrics typically used to evaluate trust management systems; these metrics include overhead (e.g., control

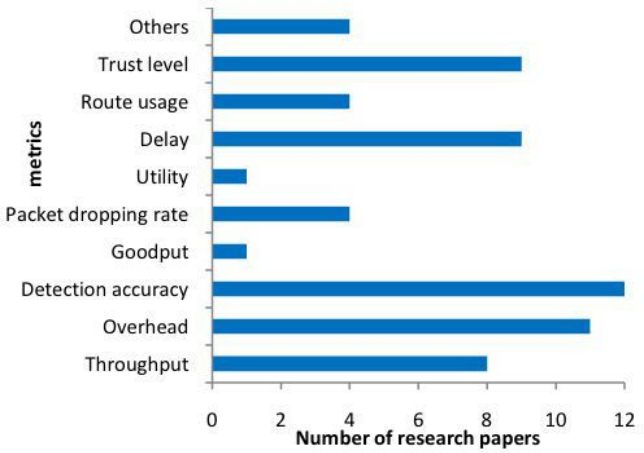

Fig. 8. Metrics considered by MANET trust management systems.

packet overheads), throughput, goodput, packet dropping rate, and delay. "Route usage" refers to the number of routes selected particularly when the purpose is for secure routing. "Trust level" is a recently used system metric. Example metrics using the trust level include confidence level of the trust value, trustworthiness, opinion values about other nodes, and trust level per session. "Others" indicates metrics that consider system tolerance based on incorrect reputation threshold, availability, convergence time to reach steady state in trustworthiness of all participating nodes, and percentage of malicious nodes.

IV. MANET Trust Management Schemes

This section summarizes trust management schemes that have been developed for MANETs.

We describe trust management schemes based on specific design purposes such as secure routing, authentication, intrusion detection, access control (authorization), and key management. Further, we also describe existing general frameworks for trust (or reputation) evidence distribution and evaluation. Figure 9 summarizes 45 trust management schemes proposed for MANETs during 2000-2009 based on their design purposes. Note that under each research category, we will survey existing works in chronological order.

A. Secure Routing

Most reputation-based trust management schemes are devised for collaborative secure routing by detecting misbehaving nodes, both selfish and malicious ones. Marti *et al*. [67] proposed a reputation-based trust management scheme that consists of a *watchdog* that monitors node behaviors and a *pathrater* that collects reputation and takes response actions (e.g., isolating misbehaving nodes as a result of misbehavior detection). This work is an initiative to dynamically incorporate direct observations into trust values for secure routing. It extends DSR (Dynamic Source Routing) but trust evaluation is based only on direct observations.

Buchegger *et al*. [68] initiated a new design to develop a routing protocol by introducing a "trust manager" in their scheme. They determined trust levels based on self-monitored information while employing reputation collected from both direct and indirect observations and experiences. They did not show any experimental results, but pose several interesting questions such as what is a sustainable relationship between the total number of nodes in the network, the maximum number of malicious nodes the system can tolerate, and the minimum number of friends per node needed to achieve high tolerance, and a prescribed level of trust. Buchegger *et al*. [69] also developed a reputation-based trust management scheme called CONFIDANT (Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks) based on both direct and indirect observations to detect misbehaving nodes. The unique feature in this work is an incentive mechanism for altruistic nodes to be paid as a result of cooperation.

Paul and Westhoff [70] proposed a context-aware mechanism for detecting selfish nodes by extending DSR with a context-aware inference scheme to punish the accused and the malicious accuser. However, the use of digital signatures to disseminate information about the accused and the malicious accuser may not be viable in a resource-constrained MANET environment.

Michiardi *et al*. [71] proposed CORE (COllaborative REputation) that has a monitoring mechanism complemented by a reputation functionality that differentiates between direct reputation, indirect reputation, and functional reputation (task-specific behavior). The proposed protocol is developed to make decisions about cooperation or gradual isolation of a node. A unique characteristic of this mechanism is that it exchanges only positive reputation information. However, this may limit its reliance on positive reports without the facility to submit negative feedback.

He *et al*. [72] proposed a reputation-based trust management scheme using an incentive mechanism, called SORI (Secure and Objective Reputation-based Incentive). This scheme encourages packet forwarding and discourages selfish behaviors based on quantified objective measures and reputation propagation by a one-way hash chain based authentication. The performance of this scheme in the presence of malicious nodes, as may be expected in a hostile environment, has not been investigated.

Nekkanti and Lee [73] extended AODV (Ad hoc On-demand Distance Vector) using trust factor and security level at each node. Their approach deals differently with each route request based on the node's trust factor and security level. In a typical scheme, routing information for every request would be encrypted leading to large overheads; they propose to use different levels of encryption based on the trust factor of a node, thus reducing overhead. This approach adjusts the security level based on the recognized hostility level and hence can conserve resources; however, the approach does not treat evaluation of trust itself. Li *et al*. [74] also extended AODV and adopted a trust model to guard against malicious behaviors of nodes at the network layer. They represented trust as *opinion* stemming from *subjective logic*. The opinion reflects the characteristics of trust in MANETs, particularly dynamicity. The key feature is to consider system performance aspects by dealing with each query based on its level of trust. Depending on the level of trust of nodes involved in the query, there is no need for a node to request and

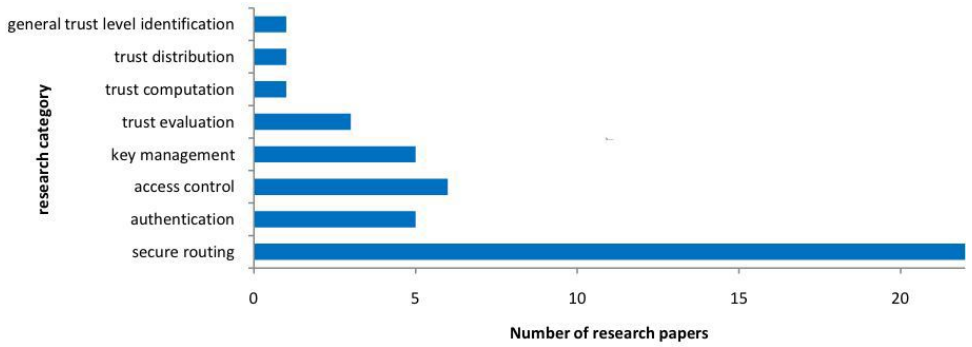

Fig. 9. Metrics considered by MANET trust management systems.

verify certificates all the time, thereby leading to significant reduction of computation and communication overhead. This work advances trust management by considering a generic trust management framework for MANETs.

Pisinou *et al.* [75] devised a secure AODV-based routing protocol for multi-hop ad hoc networks for discovering a secure end-to-end route free of any compromised nodes. Their trust-based routing protocol calculates trust values based only on direct observations, assuming that trust is transitive. As a continuation of [68], Buchegger *et al.* [76] also proposed a fully distributed reputation system in order to cope with false information propagation. The proposed design maintains a reputation and trust rating system about individual nodes by designing a modified Bayesian approach. Recognizing the dynamic nature of trust and reputation, the authors introduced reevaluation and reputation fading as well as redemption mechanisms. Nevertheless, no other characteristics of trust are addressed except for dynamicity.

Ghosh *et al.* [77] enhanced trust management by considering the confidence level of trust. Their use of the confidence level as a weight on the computed trust value and the method for calculating trust in a fully distributed way provide a general framework that can be applied to non-trust-aware routing protocols. In [77], SORI [72] is extended to alleviate the problem of selfish nodes, by considering the number of forwarding packets to evaluate the confidence level.

Wang *et al.* [78] proposed a mechanism to distinguish selfish peers from cooperative ones based solely on local observations of AODV routing protocol behaviors. They use a finite state machine model of locally observed AODV actions to construct a statistical description of each peer's behavior. In order to distinguish between selfish and cooperative peers, a series of well-known statistical tests are applied to features obtained from the observed AODV actions. An interesting extension of this work would be to consider various patterns of node mobility which can give additional insights.

Zouridaki *et al.* [79] proposed a trust establishment mechanism for MANETs called *Herms* to improve the reliability of packet forwarding over multi-hop routes in the presence of potentially malicious nodes. Essentially, direct observations are used to evaluate opinions about others. Also, confidence level is used as a weight to evaluate trust of other nodes based on a Bayesian approach. They also introduced a windowing scheme to systematically expire old data to maintain accuracy of the opinion metric in the face of dynamics. However, this scheme is vulnerable to attacks that can exploit the windowing scheme to disseminate false information to accuse good nodes and to keep bad nodes in the system (such as badmouthing attacks).

As an extension, Zouridaki *et al.* [80] employed both first-hand trust information based on direct observations and second-hand trust information forwarded from neighboring nodes about non-neighboring nodes. This trust establishment scheme can cope with more attacks, including propagation of false recommendations or information, identifying bad nodes among neighboring nodes, colluding attacks, replay attacks, and duplicate attacks. It is noteworthy that they used only security related metrics to evaluate their scheme, such as trustworthiness and the percentage of nodes recognized as bad.

Pirzada *et al.* [81] proposed and examined the efficacy of trust-based reactive routing protocols in the presence of attacks. This work only considers first hand information to evaluate other nodes' trust values. Thus, trust evaluation is restricted to direct neighboring nodes.

Sun *et al.* [46] proposed trust modeling and evaluation methods for secure ad hoc routing and malicious node detection. The unique part of their design is to consider trust as a measure of uncertainty that can be calculated using *entropy*. In their definition, trust is a continuous variable, and does not need to be transitive, thus capturing some of the characteristics of trust in MANETs. However, this work considers packet dropping as the only component of direct observations to evaluate trust.

Abusalah *et al.* [82] proposed a trust-aware routing protocol (TARP) and developed a trust metric based on six trust components including software configuration, hardware configuration, battery power, credit history, exposure and organizational hierarchy. However, no consideration was given to trust decay over time and space to reflect uncertainty due to dynamics and incomplete information in MANET environments.

Sen *et al.* [83] proposed a trust-based mechanism to detect malicious packet dropping nodes based on reputation of neighboring nodes, and take into account the decay of trust over time. This work assumes that a pair of public/private keys can be preloaded to prevent identity-related attacks. However, this may not be scalable for a large network.

Soltanali *et al.* [84] proposed a distributed mechanism to deal with selfish nodes as well as to encourage cooperation in

MANETs based on the combination of reputation-based and currency-based incentive mechanism mitigating their defects and improving their advantages. Compared to existing works, this work considers more aspects of trust such as dynamicity, weighted transitivity, and subjectivity. However, it used only packet forwarding behaviors to evaluate a node's trust and standard performance metrics to evaluate the proposed trust scheme.

Balakrishnnan *et al*. [85] developed a trust model to strengthen the security of MANETs and to deal with the issues associated with recommendations. Their model utilizes only trusted routes for communication, and isolates malicious nodes based on the evidence obtained from direct interactions and recommendations. Their protocol is described as robust to the recommender's bias, honest-elicitation, and free-riding. This work uniquely considered a context-dependency characteristic of trust in extending DSR.

Li *et al*. [52] stated that using only a reputation-based trust framework gives only an incomplete partial solution for trust management. They proposed an objective trust management framework (OTMF) for MANETs based on both direct and indirect information for reputation management and showed the effectiveness of OTMF. This work used the term "objective" trust to refer to trust evaluated based on second-hand information. However, this work did not consider node collusion in obtaining second-hand information, which may lead to incorrect recommendations.

Mundinger and Boudec [86] were the first to analyze the robustness of a reputation system based on a deviation test. Using a mean-field approach in their stochastic model, they showed that liars have no impact unless the number of liars exceeds a certain threshold (a phase transition). They provided precise formulas for the critical values and guidelines for an optimal choice of parameters. This work is unique in that it evaluates a system's tolerance to untrusted nodes; however, the reputation evaluation is based only on the "fake" information.

Moe *et al*. [87] proposed a trust-based routing protocol as an extension of DSR based on an incentive mechanism that enforces cooperation among nodes and reduces the benefits that selfish nodes can enjoy (e.g., saving resources by selectively dropping packets). This work is unique in that they used a hidden Markov model (HMM) to quantitatively measure the trustworthiness of nodes. In this work, selfish nodes are benign and selectively drop packets. Performance characteristics of the protocol when malicious nodes perform active attacks such as packet modifications, identity attacks, etc., need to be investigated further.

In quorum or threshold schemes, a node must successfully interact with at least k of n distributed trusted authority (TA) nodes. Finding k such nodes can be resource intensive. Reidt *et al*. [88] prioritize the TA nodes and find a route to connect to k desirable TA nodes so as to minimize a performance metric such as overhead, taking into account reliability and energy consumption of individual nodes. Significant savings over a standard system were shown. An interesting aspect, not considered yet, would be to incorporate trustworthiness into the TA selection and routing scheme.

Ayachi *et al*. [89] formalized implicit trust relations in AODV and demonstrated that a node can utilize these trust relations to isolate malicious nodes for secure routing. Nodes overhear neighbors' transmissions from which they can build a neighbor routing table and check for deviation from normal behaviors for AODV. This scheme can detect malicious behaviors such as message replication, message forgery and some instances of message modification. However, it is not amenable to incorporation of other trust metric components, such as intimacy and competence but monitored behaviors could feed into a trust evaluation scheme.

Adnane *et al*. [90] proposed trust-based countermeasures to isolate malicious nodes extending OLSR (Optimized Link State Routing). Their protocol provides secure routing paths by identifying malicious nodes. The focus of the protocol is to prevent usurpation of node identities. Performance analysis under other types of attacks remains to be investigated.

Although many researchers have developed secure routing protocols using trust, most of the approaches have focused on monitoring routing behaviors and the evaluation of trust has been in the context of communication networks. Further steps should be taken to refine issues such as (1) how to quantify trust in a MANET node; (2) how to employ (a continuous-valued) trust in a routing decision; and (3) how to develop a composite trust metric incorporating task performance goals, taking into account the social aspects of a MANET node.

B. Authentication

There have been efforts to establish trust relationships to ensure authentication in MANETs. Weimerskirch *et al*. [91] developed a trust model based on human behavior, noting that society can be properly considered as an ad hoc network. They used recommendations from a distributed trust model to construct trust relationships and extended it by a request for recommendations. Based on models derived from observations of human society, recommendations are used to calculate trust, with weights based on the distance of relationships. Their definition does not assume symmetry or complete transitivity, thus capturing essential features of trust in MANETs. The assumption of low-value transactions does not require any evidence-based mechanism to ensure trust such as authentications using public/private keys. Consequently, it is not applicable to systems where hostility may be high, or where consequences of misplaced trust can be severe.

Verma *et al*. [92] presented an overview of a trust negotiation scheme using DSR and ZRP (Zone Routing Protocol). Their scheme consists of two components. The peer-to-peer component deals with secure communications with neighbors in a lightweight manner. The heavyweight remote component performs trust negotiation and establishes secure end-to-end communication. The main goal of this work is to add robustness in the process of trust negotiation, rather than trust evaluation.

Pirzada and McDonald [93] proposed a trust-based communication model that, based on a notion of a *belief*, provides a dynamic measure of reliability and trustworthiness in MANETs. The merit of this work is to incorporate utility as general trust and time as situational trust into the overall trust metric to evaluate an agent in the network. However, the situational trust considered is limited to monitoring dynamics of packet forwarding behaviors.

Davis [47] proposed a reliable and structured hierarchical model for trust management in MANETs that is robust to malicious accusation exploits. The scheme deals with explicit revocation of certificates in a distributed way, eliminating the case in which revoked certificates can be accepted as valid., This work assumes that the initial certificates and public keys of all nodes are distributed by a centralized trust authority to each node before the network is deployed which may not be scalable in a large scale MANET. The paper does not discuss the issue of false positives which can lead to continual eviction of nodes, and eventually loss of network connectivity. To counteract this, dynamic reissue of certificates may be needed which may incur extra overhead.

Ngai and Lyu [94] proposed a secure public key authentication service based on their trust model to prevent propagation of false public keys in the presence of malicious nodes. Trust is evaluated based on direct monitoring as well as recommendation. However, this work does not consider group membership changes, the distance from the evaluator, and their effect on the performance of their trust management scheme.

In summary, there has been quite a bit of work on using trust for authentication. However, as in the case of trust-based secure routing, the models and protocols used are based solely on monitoring packet forwarding behaviors.

C. Intrusion Detection

Trust can be used as a basis for developing an intrusion detection system (IDS). Also, IDS itself can help nodes measure trust of other nodes when they cooperate with each other to detect malicious nodes. Albers *et al.* [95] proposed a general architecture for an intrusion detection system (IDS) called a Local IDS (LIDS) such that intrusion detection can be performed locally among trustworthy participating nodes. Here, trust is used to detect intrusions in the system. In Ahmed *et al.* [96], IDS provides audit and monitoring capabilities that offer local security to a node and helps perceive the specific trust levels of other nodes. Hence, evaluating trust and identifying intrusions may not be totally separated processes.

D. Access Control

Trust also can be applied in determining whether or not to grant access to certain resources or rights. Gray *et al.* [97] integrated trust-based admission control with standard role-based access control. By doing this, an access control decision is effectively made without being affected by incomplete information collected in MANETs. A simple distributed blackjack card game application is described, in which the trust-based admission control system is used to assign roles to users based on their trust-based admission rights. It is not clear how the approach can be extended to a general framework applicable to MANETs.

Luo *et al.* [98] presented a ubiquitous and robust access control solution (URSA) for MANETs based on a localized group trust model so that only well behaving nodes will have access rights to network resources. Their localized group trust model for MANETs is based on threshold cryptography: a node is globally trusted only if it is individually trusted by any k trusted nodes where k is a system-wide trust threshold. This work assumes that the node density is large enough so that any node can find k trusted nodes, perhaps by moving to another location. Interesting extensions of the work include consideration of mobility models other than random waypoint, and trust evaluation under high node mobility situations.

Adams and Davis [17] presented a decentralized access control system implementing sociological trust constructs in a quantitative system to evaluate the relationships between entities. A distributed, node-centric approach to reputation management considers a node's behavior feedback and gives a reputation index that nodes can use to determine the trustworthiness of their peers before establishing trust relationships. This work further assessed risk using a Bayesian approach to evaluate trust. Interestingly, this work used reputation as a weight to evaluate direct observations, which is a different approach from most existing works. Extensions of the scheme to handle network dynamics would be useful.

Yunfang [53] proposed an integrated mechanism of policy proof and reputation evolution into trust management for decision-making on access control with the goal of providing firm/objective security as well as social/subjective security. However, this work is based on the assumption that trust is completely transitive, and it is not clear how a more realistic transitivity model can be incorporated into the trust management system.

E. Key Management

Virendra *et al.* [99] proposed a trust-based security architecture for key management in MANETs. This architecture aims to establish keys between nodes based on their trust relationships, and to build secure distributed control using trust as a metric. In their self-organizing trust-based architecture, nodes are organized into trust-based clusters called Physical-Logical Trust Domains (PLTDs), a group of trusted nodes sharing a group key. Nodes can belong to multiple PLTDs. The unique part of this work is that it considers the trust level of each node in a physical as well as a logical sense, e.g., it considers both one-hop nodes as well as previously trusted nodes that are not currently one-hop neighboring nodes. The significant merit of this work is in formalizing a trust metric reflecting trust decay over time and updating trust as dynamics of the network change. However, establishing pair-wise keys based on pair-wise trust may not be feasible in terms of scalability and in the presence of high network dynamics in a large MANET.

Hadjichristofi *et al.* [63] presented a key management framework that provides redundancy and robustness in the establishment of Security Association (SA) between pairs of nodes. Their proposed key management system (KMS) adopts a modified hierarchical Public Key Infrastructure (PKI) model where nodes can dynamically take management roles. The scheme is designed to provide high service availability based on trust-based SA among nodes. However, trust relationships are derived solely from certificate chains. Adams *et al.* [44] also extended their prior work [63] with a node-centric reputation management approach that considers feedback about a node's behavior in generating a reputation index to determine the trustworthiness of its peers before establishing

IPSec security associations. They considered the decay of trust over time using a three-window weighted average. They also derived reputation values from past experiences and current observations and introduced a rehabilitation mechanism to give a second chance to bad nodes. However, no details were given on the type of information that should be directly observed to derive reputation.

Li *et al*. [100] demonstrated an on-demand, fully localized, and hop-by-hop public key management protocol for MANETs. In this protocol each node generates its own public/private key pairs, issues its certificate to neighboring nodes, keeps received certificates in its certificate repository, and provides authentication service by adapting to the dynamic network topology, without reliance on any centralized server. However, only certificate chains are used to derive trust.

Chang and Kou [101] proposed a Markov chain trust model to obtain the trust values (TVs) for 1-hop neighbors. They designed a trust-based hierarchical key management scheme by selecting a certificate authority server (CA) and a backup CA with the highest TVs. This work gives a rigorous analysis of TVs and considers a variety of attacks. However, it computes TVs only based on direct observations and does not consider trust decay due to using recommendations from remote nodes.

A survey of key management techniques for network-layer security may be found in the work by Hegland *et al*. [102].

In contrast to secure routing that produces an operational MANET, authentication, intrusion detection, access control, and key management are general trust contexts that also exist outside the area of MANETs. In these applications, it is useful to abstract out the properties of MANETs and consider only the influence of MANETs on any information/evidence gathering, aggregation, and other computation, and design a trust management scheme that considers influences such as the cost/likelihood of obtaining a piece of information in computing trust.

F. Trust Evidence Distribution and Evaluation

Several trust management schemes have been proposed in order to provide a general framework for trust evidence distribution or evaluation in MANETs.

Yan *et al*. [64] proposed a trust evaluation based security solution for data protection, secure routing, and other network activities. This trust evaluation model called Personal Trusted Bubble (PTB) considers many factors including experience statistics, data value (the higher the value of the data, the higher is the trust needed from other PTBs to transfer it), intrusion black list, reference (reputation/recommendation), personal preference, and PTB policy (related to the entire network's security requirements and policy). Interestingly, personal preference and PTB reflect the subjective characteristic of trust in deriving trust values. Yan *et al*. [64] do not validate whether their proposed trust management is correct or useful compared to the actual trust levels, say, based on trustworthiness in Josang and Solhaug's terminology. In general, validation of trust models is difficult, given the inherent subjectivity in the trust metric, but it is also critical. Jiang and Baras [103] proposed a trust distribution scheme called ABED (Ant-Based trust Evidence Distribution) based on the swarm intelligence paradigm, which is highly distributed and adaptive to mobility. The swarm intelligence paradigm is widely used in dynamic optimization problems (e.g., the traveling salesman problem, routing in communication networks). The key principle in swarm interaction is called stigmergy, indirect communication through the environment. In ABED, "pheromones" are deposited at nodes by mobile agents called "ants" and provide the mechanism for information exchange and interactions. These "ants" can identify the optimal path toward their food, resembling trust evidence in this case. The pheromone regulation process is known to be suitable for dynamically changing environments such as MANETs. However, no specific attackers are considered to prove the robustness of the proposed scheme in the presence of attacks.

In the continuing work, Baras and Jiang [104] addressed distributed trust computation and establishment using random graph theory. This work uses the theory of dynamic cooperative games and identifies how a phase transition from a distrusted state to a trusted state can occur in a dynamic MANET. This work is unique in that it describes how phase transitions occur in MANETs and how these are related to node mobility and network topology in the process of initial trust establishment. Trust relationships are ternary (yes, no, don't care) and the emphasis is on understanding steady-state behaviors. Incorporating continuous valued trust variables, dynamics, and transient behaviors in this framework would be useful.

Theodorakopoulos and Baras [50] proposed a trust evidence evaluation scheme for MANETs. The evaluation process is modeled as a path problem in a directed graph where vertices represent entities and edges represent trust relations. The authors employed the theory of Semirings to show how two nodes can establish trust relationships without prior direct interactions. Their case study uses the PGP web of trust to express an example trust model based on *Semirings* and shows that their scheme is robust in the presence of attackers. However, their work assumes that trust is transitive. Further, trust and confidence values are represented as binary rather than continuous values. Even though no centralized trusted third party exists, their work makes use of a source node as a trusted infrastructure, which introduces vulnerability in MANETs.

Recently, Boukerche and Ren [105] proposed a distributed reputation management mechanism called GRE (Generalized Reputation Evaluation), using a comprehensive computational reputation model. GRE seeks to prevent malicious nodes from entering a trusted community. However, no specific attack model was addressed.

Moloney and Weber [106] presented a trust-based security system that generates appropriate trust levels based on the consideration of the main characteristics of MANETs as well as context-awareness. The scheme leverages two existing projects at Trinity College, Dublin, called *SECURE* and *Aithe*. SECURE is used for trust management using a trust engine and a risk engine while Aithe collects and manages context information forwarded from sensors. It is worthwhile to extend this work to consider attacks that can propagate incorrect information to generate trust levels.

Very recently, Cho *et al*. [107] proposed a trust management scheme for group communication systems in MANETs. This

work proposed a composite trust metric reflecting various aspects of a MANET node such as sociability (i.e., social trust) and task performance capability (i.e., QoS trust), and investigated the effect of the trust chain length used by a node to establish acceptable trust levels through subjective trust evaluation. They also discussed the concept of objective trust evaluation based on global knowledge as the basis of validating subjective trust evaluation. More work remains to be done to ascertain feasibility.

The Appendix summarizes trust management schemes surveyed in this section. In the Appendix, the methodology explains how trust evidence is collected and performance metrics refer to the metrics used to evaluate various trust management schemes.

V. Future Research Discussion

It is clear that sooner or later intelligence will be embedded in each node with cognitive functionality, adopting recent ideas about cognitive networks in wireless networks [108]. Mahmoud [108] defines a cognitive network as having a *cognitive process* that is capable of perceiving current network conditions and then planning, deciding, and acting on those conditions. Cognitive networks are able to reconfigure the network infrastructure based on past experiences by adapting to continuously changing network behaviors to improve scalability (e.g., reducing complexity), survivability (e.g., increasing reliability), and QoS (e.g., facilitating cooperation among nodes) as proactive mechanisms [48][108]. We suggest using this concept of cognitive networks so that nodes can adapt to changing network behaviors, such as attacker behaviors, degree of hostility, node disconnection due to physical environment such as terrain, energy depletion, or voluntary disconnection for energy saving. Cognition is more than adaptation; it incorporates learning and reasoning.

Another potentially fruitful research direction is to use social relationships in evaluating trust among collaborators in a group setting by employing the concept of *social networks*. Golbeck *et al*. [37][38][39] define a social network as a social structure of individuals who may be related directly or indirectly to each other in order to pursue common interests. Yu *et al*. [109] and Maheswaran *et al*. [110] use social networks to evaluate the trust value of a node. Examples of social networks are strong social relationships including colleagues or relatives, membership in the same platoon, and loose social relationships including school alumni or friends with common interests or membership in coalition activities. Social trust may include friendship, honesty, privacy, and social reputation or recommendation derived from direct or indirect interactions for "sociable" purposes. In MANETs, metrics used to measure these social trust properties can be frequency of communications, malicious or benign behaviors (e.g., false accusation or recommendation, impersonation), private information revealed, and quality of reputation. The notion of social trust is being incorporated into communication networks. Trust propagation models, some based on notions of social networking, have been proposed in multi-agent systems [114] [115] [116].

An important and interesting research direction is to construct a composite trust metric based on social trust and other trust components representing quality-of-service (QoS) to successfully perform tasks to meet both performance and trust requirements. We have seen some work in the literature moving in this direction. Cho *et al*. considered honesty and intimacy (for social trust), and unselfishness and energy (for QoS trust) for trust evaluation [107]. Kohlas *et al*. [111] used honesty, competency, reliability, and maliciousness and their corresponding negations as trust components to define trust relationships. Yin *et al*. [112] computed composite reputation values of peers based on evidences from various domains such as customers' reputation scores or ranks in commercial sites or the certified roles in certain organizations with different weights indicating the importance and robustness of the reputation computation processes. Boursas and Hommel [113] considered QoS aspects such as the visual quality in multimedia and commitment in interactions to calculate node trust levels in large distributed systems. More work remains to be done to understand the best combination of social trust versus QoS trust components used to construct the composite trust metric, as well as the best weights associated with social trust and QoS trust, especially when given application context information for critical mission executions in MANETs.

Not much work has been done in trust management for mobile vehicular systems. A trust architecture for vehicular networks is proposed in [117] that incorporates a policy control model, a proactive trust model, and a social network based system, and takes into account dynamics. When the environment is volatile, associating trust with data becomes even more challenging; a solution is provided in [117] and a case study is discussed in the context of vehicular networks.

The overall qualities of trust in decision making depends on complex interactions between the information, social/cognitive, and communications networks. Trust metrics might be separately defined in each of the networks, but the key issue is to elucidate the mapping of qualitative and quantitative metrics across the networks, to define an end-to-end notion of composite trust, to determine the attributes (presumably many others than trust) in the different networks that affect this composite metric, and identify those that can be controlled and those that cannot [118], especially for trust management in a coalition environment [119].

We suggest that the following design concepts be considered for building MANET trust management systems:

- A trust metric must reflect the unique properties of trust in MANETs, including possibly imperfect transitivity, asymmetry, subjectivity, non-binary nature, decay over time and space, dynamicity, and context-dependency.
- A trust metric must incorporate adequate trust components (e.g., social trust and QoS trust) capable of reflecting mission difficulty (e.g., high risk upon task failure), changing network environments (e.g., lack of bandwidth, increasingly hostile environment as attackers' strength increases, high communication load), and conditions of participating nodes (e.g., low energy, compromised status).
- A trust management design must support cognitive functionality for each node to achieve adaptability to changing network conditions and MANET environments including

node density, node mobility patterns, scheduling algorithms, and traffic patterns.

- A trust management system should be situation specific or situation aware [120][121][122]. Situational awareness includes mission contexts and requirements in terms of security, performance and reliability. Depending on the required levels of security, performance and/or reliability, a different level of trust can be adopted reflecting mission contexts and situations.
- A trust metric must adequately reflect tradeoffs in altruism versus selfishness, trust versus reliability, availability, survivability, or security so as to contribute to improved system performance. In addition, since gathering information from spatially remote areas will consume more resources (e.g., time or energy) but improve decision making, one should investigate the tradeoff between resource consumption and decision making accuracy and timeliness. One may utilize aggregation technique to reduce resource consumption in obtaining information from distant nodes.
- A trust management design must allow optimal settings to be identified under various network and environmental conditions so as to maximize the overall trust of the system for successful mission executions. Equally important is an understanding of sensitivity to deviations from the optimal settings.
- There has been no comparison of trust management schemes versus conventional security schemes in terms of metrics of interest in MANETs. One example could be the comparison of trust management schemes to cryptographic schemes in detecting misbehaving nodes.
- Local trust is easy to understand and compute, since it only involves tracking behaviors of neighboring nodes. Local trust is easy to defend from malicious attacks. Global trust is harder to compute and update; Eigentrust [123] is an example of a global trust metric. But a non-local definition of trust is subject to subversion and manipulation by colluding nodes. Zhang *et al*. [124] provide a robust version of the Eigentrust algorithm. A critical question is: is trust inherently local? How can a global trust metric be computed and distributed reliably?
- Recently, social trust derived from social networks has received considerable attention for establishing trust in various applications. MANET designers may also want to take into account social trust.
- The survey has focused on a trust value associated with individual nodes. But often we may be interested in associating trust with data or with a group of nodes or entities. Many of the concepts discussed here will extend naturally.

VI. Concluding Remarks

Trust is a multidimensional, complex, and context-dependent concept. Although trust-based decision making is in our everyday life, trust establishment and management in MANETs face challenges due to the severe resource constraints, the open nature of the wireless medium, the complex dependence between the communications, social and application networks, and, hence, the complex dependency of any trust metric on features, parameters, and interactions within and amongst these networks.

In this paper, we surveyed and analyzed existing trust management schemes in MANETs to provide MANET trust network protocol designers with multiple perspectives on the concept of trust, an understanding of trust properties that should be observed in developing trust metrics for evaluating trust, and insights on how a trust metric can be customized to meet the requirements and goals of the targeted system. A composite trust metric that captures aspects of communications and social networks, and corresponding trust measurement, trust distribution, and trust management schemes are interesting research directions. For dynamic networks, such as military MANETs, these schemes should have desirable attributes such as ability to adapt to environmental dynamics, scalability, reliability, and reconfigurability.

Acknowledgment

This project is supported in part by an appointment to the U.S. Army Research Laboratory Postdoctoral Fellowship Program administered by the Oak Ridge Associated Universities through a contract with the U.S. Army Research Laboratory. The authors appreciate the many discussions with and critical insights provided by our internal ARL staff including Elizabeth Bowman, Kevin Chan, Natalie Ivanic, and Brian Rivera. The authors also give special thanks to Dakshi Agrawal and Mudhakar Srivatsa from IBM T. J. Watson Research Center for their valuable comments.

Appendix

A survey on existing trust management schemes in MANETs

See Tables I-VI.

References

[1] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.

[2] J. Jubin and J. Tornow, "The DARPA Packet Radio Network Protocols," *Proc. IEEE*, vol. 75, no. 1, Jan. 1987, pp. 21-32.

[3] A. J. Tardiff and J.W. Gowens, Editors, "ARL Advanced Telecommunication and Information Distribution Research Program (ATIRP)," *Final Report*, 1996-2001, June 2001.

[4] T. Plesse, J. Lecomte, C. Adjih, M. Badel, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, and A. Plakoo, "OLSR Performance Measurement in a Military Mobile Ad Hoc Network," *Proc. 24th Int'l Conf. on Distributed Computing Systems*, 2004, pp. 704-709.

[5] K. S. Cook (editor), *Trust in Society,* vol. 2, Feb. 2003, Russell Sage Foundation Series on Trust, New York.

[6] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," *Proc. IEEE Symposium on Security and Privacy*, 6-8 May, 1996, pp. 164 - 173.

[7] R. B. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh, "Bootstrapping Security Associations for Routing in Mobile Ad Hoc Networks," *Proc. IEEE GLOBECOM*, San Francisco, CA, Dec. 2003, pp.1511-1515.

[8] L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," *Proc. 10th Int'l Security Protocols Workshop,* Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.

[9] J. S. Baras and T. Jiang, "Managing Trust in Self-Organized Mobile Ad Hoc Networks," *Proc. 12th Annual Network and Distributed System Security Symposium Workshop*, Feb. 2005, San Diego, CA.

[10] S. Ruhomaa and L. Kutvonen, "Trust Management Survey," P. Herrmann *et al*. (Eds.), *iTrust* 2005, *Lecture Notes in Computer Science*, vol. 3477, pp. 77-92.

TABLE I

Authors, Year, Ref. no	Purpose	Methodology	Attacks considered	Performance metrics	Trust property	Trust management model
Marti (2000) [67]	Secure routing	Direct observation Reputation	Black hole False accusation	Throughput Overhead Detection accuracy	Dynamicity	Watchdog and Pathrater Trust revocation introducing redemption Underlying routing protocol: DSR
Buchegger & Boudec (2002) [68]	Secure routing	Direct observation Reputation	Various malicious packet forwarding DoS	N/A	Weighted transitivity Dynamicity	An extension of DSR using a hybrid scheme of selective altruism and utilitarianism
Buchegger & Boudec (2002)[69]	Secure routing	Direct observation Reputation	Forward defection (e.g., route diversion)	Throughput Goodput Dropped packets Overhead Utility[a]	Weighted transitivity Dynamicity	CONFIDANT Bayesian Model Incentive mechanism No punishment against misbehaving nodes An extension of DSR
Paul & Westhoff (2002)[70]	Secure routing	Direct observation Reputation	Masquerading Packet modification	N/A	N/A	Contextaware Inference Mechanism An extension of DSR
Michiardi & Molva (2002) [71]	Secure routing	Direct observation Reputation	Selfish nodes False information propagation DoS attack	N/A	Dynamicity Subjectivity	Extension of [67] Functional trust concept introduced to combine subjective direct observation plus indirect information.
He *et al.* (2004)[72]	Secure routing	Direct observation Reputation	Packet dropping Selfish nodes Impersonation False information propagation	Throughput Overhead	Weighted transitivity	Secure and Objective Reputation-based Incentive (SORI) based on DSR Incentive mechanism
Nekkanti & Lee (2004)[73]	Secure routing	N/A	General outside attackers	Average endtoend delay Packet delivery ratio	Trust value ranges from 0 to 10 as an integer	Trust-based adaptive AODV
Li *et al.* (2004) [74]	Secure routing	Direct observation Recommendation	General malicious nodes	N/A	Dynamicity Asymmetry Weighted transitivity[b]	An extension of AODV using subjective logic

[a]"Utility" metric refers to the ratio of the number of transmissions originated at the node itself to the number forwarded as an intermediate node on behalf of other nodes [69]. This metric can be represented as A/(A+B) where A is the number of packets transmitted by a node for itself and B is the number of packets transmitted for others.

[b]"Weighted transitivity" means that trust is transitive only with a weight reflecting decaying of trust depending on confidence level, credibility, reliability, time, reputation, distance, etc.

[11] S. Ruhomaa, L. Kutvonen, and E. Koutrouli, "Reputation Management Survey," *2nd Int'l Conf. on Availability, Reliability, and Security*, 10-13 Apr. 2007, Vienna, Austria, pp. 103-111.

[12] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications," *IEEE Commun. Surveys and Tutorials*, vol. 3, no. 4, pp. 2-16, 2000.

[13] J. H. Cho and A. Swami, "Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks," *14th Int'l Command and Control Research and Technology Symposium*, Washington D.C. 15-17 June 2009.

[14] Merriam Webster's Dictionary [Online]: http://www.merriamwebster.com/dictionary/trust%5B1%5D.

[15] D. Gambetta, "Can We Trust Trust?" *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, Oxford, 1990, pp. 213-237.

[16] N. Luhmann, *Trust and Power*, Wiley, 1979.

[17] W. J. Adams, N. J. Davis, "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration," *Proc. 6th Annual IEEE SMC Information Assurance Workshop*, 15-17 June, 2005, West Point, NY, pp. 317-324.

[18] T. Harford, "The Economics of Trust," [Online]: http://www.forbes.com/2006/09/22/trust-economy-markets-tech_cx_th_06trust_0925harford.html

[19] H. S. James, "The Trust Paradox: A Survey of Economic Inquiries into the Nature of Trust and Trustworthiness," *Journal of Economic Behavior and Organization*, vol. 47, no. 3, 2002.

[20] A. B. MacKenzie and S. B. Wicker, "Game Theory and the Design of Self-Configuring, Adaptive Wireless Networks," *IEEE Commun. Mag.*, vol. 39, no. 11, pp. 126-131, Nov. 2001.

[21] R. Axelrod, "The Evolution of Cooperation," *Science*, vol. 211, no. 4489, pp. 1390-1396, March 1981.

[22] M. Srivatsa, S. Balfe, K. G. Paterson, and P. Rohatgi, "Trust Management for Secure Information Flows," *Proc. 15th ACM Conf. on Computer and Communications Security*, Alexandria, VA, Oct. 2008, pp. 175-188.

[23] Stanford Encyclopedia of Philosophy, Feb. 20, 2006 [Online]: http://plato.stanford.edu/entries/trust/

[24] B. Lahno, "Olli Lagerspetz: Trust. The Tacit Demand," *Ethical Theory and Moral Practice*, vol. 2, no. 4, pp. 433-435, Dec. 1999, Published Springer Netherlands.

[25] Wikipedia-Trust in Social Science, 16 Sept. 2009 [Online]: http://en.wikipedia.org/wiki/Trust_(sociology)

[26] M. Deutsch, *The Resolution of Conflict: Constructive and Destructive Processes*, Carl Hovland Memorial Lectures Series, New Haven and London: Yale University Press, 1973.

[27] R. Hardin, "The Street-Level Epistemology of Trust," *Politics and Society*, vol. 21, no. 4, 1993, pp. 505-529.

[28] J. B. Rotter, "Interpersonal Trust, Trustworthiness, and Gullibility," *American Psychologist*, vol. 35, no. 1, Jan. 1980, pp. 1-7.

[29] D. McKnight and N. Chevany, "The Meanings of Trust," Carlson School of Management, University of Minnesota, Technical Report TR 94-04, 1996.

[30] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "An Integrative

TABLE II

Authors, Year, Ref. no	Purpose	Methodology	Attacks considered	Performance metrics	Trust property	Trust management model
Pisinou *et al.* (2004) [75]	Secure routing	Direct observation	Black hole Route injection Selfish nodes	Route overhead Algorithm running time Number of routes selected Rout errors sent	Transitivity Dynamicity	An extension of AODV called Trust-embedded AODV
Buchegger & Boudec (2004) [76]	Secure routing	Direct observation Reputation	False information propagation	Mean detection time for misbehaving nodes False alarm	Dynamicity	Bayesian Model Trust revocation introducing redemption
Ghosh (2005) [77]	Secure routing	Reputation Direct observation	Black hole Gray hole False accusation DoS	Overhead Routes selected Route errors	Weighted transitivity	Trust-embedded AODV (TAODV) Incentive mechanism
Wang *et al.* (2005) [78]	Secure routing	Direct observation Reputation	False accusation False information	Detection rate False alarm	N/A	Specification-based approach as an extension of AODV
Zouridaki *et al.* (2005) [79] (2006) [80]	Secure routing	Direct observation [79][80] Reputation by secondhand information [80]	Packet dropping Packet misrouting Packet injection Added in [2006] False accusation propagation Malicious node colluding Replay Duplicate packet forwarding	Confidence level over trust value Trustworthiness Opinion values about other nodes	Weighted transitivity Dynamicity	*Herms* Bayesian Model Trust revocation introducing Window scheme to flush out stale trust information
Pirzada *et al.* (2006) [81]	Secure routing	Direct observation	Packet modification Black hole Gray hole	Packet loss Packet forwarded Throughput Overhead Latency Path optimality Detection probability	Dynamicity	Trust-based reactive routing protocols (DSR, AODV, TORA) Effortreturnbased trust model
Sun *et al.* (2006) [46]	Secure routing	Direct observation on packet dropping rate Recommendation	False recommendation Newcomer attack Sybil attack	Trust level Packet dropping ratio	Trust is a continuous value Subjectivity Asymmetry Weighted transitivity	Information theory-based modeling: Entropy-based trust model and Probability-based trust model

Model of Organizational Trust: Past, Present, and Future," *Academy of Management Review*, vol. 31, no. 2, 2007, pp. 344-354.

[31] J. D. Lee and K. A. See, "Trust in Automation: Designing for Appropriate Reliance," *Human Factors*, vol. 46, no. 1, Spring 2004, pp. 50-80.

[32] R. Parasuraman, "Humans and Automation: Use, Misuse, Disuse, Abuse," *Human Factors*, vol. 39, no. 2, 1997, pp. 230-253.

[33] S. Staab (Editor), "The Pudding of Trust," *IEEE Intelligent Systems*, vol. 19, no. 5, pp. 74-88, 2004.

[34] L. Capra, "Toward a Human Trust Model for Mobile Ad-hoc Networks," *Proc. 2nd UK-UbiNet Workshop*, 5-7 May 2004, Cambridge University, Cambridge, UK.

[35] H. Li and M. Singhal, "Trust Management in Distributed Systems,"*Computers*, vol. 40, no.2, Feb. 2007, pp. 45-53.

[36] E. Aivaloglou, S. Gritxalis, and C. Skianis, "Trust Establishment in Ad Hoc and Sensor Networks," *Proc. 1st Int'l Workshop on Critical Information Infrastructure Security, Lecture Notes in Computer Science*,vol. 4347, pp. 179-192, Samos, Greece, 31 Aug. – 1 Sep. 2006, Springer.

[37] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," *Securecomm and Workshops-Security and Privacy for Emerging Areas in Communications Networks*, Baltimore, MD, 28 Aug. – 1 Sep. 2006, pp. 1-7.

[38] J. Golbeck and J. Hendler, "Inferring Trust Relationships in Web-based Social Networks," *ACM Transactions in Internet Technology*, Nov. 2006, vol. 6, no. 4, pp. 497-529.

[39] J. Golbeck (Ed.), *Computing with Social Trust*, Human-Computer Interaction Series, Springer, 2009.

[40] H. C. Wong, K. P. Sycara, "Adding Security and Trust to Multiagent Systems," *Applied Artificial Intelligence*, vol. 14, no. 9, pp. 927-941, Oct. 2000.

[41] A. Josang and S. LoPresti, "Analyzing the Relationship between Risk and Trust," *Proc. 2nd Int'l Conf. Trust Management*, LNCS, Springer-Verlag, 2004, pp. 135-145.

[42] B. Solhaug, D. Elgesem, and K. Stolen, "Why Trust is not proportional to Risk?" *Proc. 2nd Int'l Conf. on Availability, Reliability, and Security*, 10-13 Apr. 2007, Vienna, Austria, pp. 11-18.

[43] W. E. Walker, P. Harremoes, J. Rotmans, J. P. van der Sluijs, M. B. A. van Asselt, P. Janssen, and M.P. Krayer von Krauss, "Defining Uncertainty: A Conceptual Basis for Uncertainty Management in Model-based Decision Support," *Integrated Assessment*, vol. 4, no. 1, March 2003, pp. 5-17.

[44] W. J. Adams, G. C. Hadjichristofi and N. J. Davis, "Calculating a Node's Reputation in a Mobile Ad Hoc Network," *Proc. 24th IEEE Int'l Performance Computing and Communications Conference*, Phoenix, AX, 7-9 April 2005, pp. 303-307.

[45] A. Abdul-Rahman and S. Hailes, "Using Recommendations for Managing Trust in Distributed Systems," *Proc. IEEE Malaysia Int'l Conf. on Communication*, Kuala Lumpur, Malaysia, Aug. 1997.

[46] Y. L. 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, Feb. 2006, pp. 305-317.

[47] C. R. Davis, "A Localized Trust Management Scheme for Ad Hoc Networks," *Proc. 3rd Int'l Conf. on Networking*, March 2004, pp. 671-675.

[48] R. W. Thomas, L. A. DaSilva, and A.B. MacKenzie, "Cognitive Networks," *Proc. 1st IEEE Int'l Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 8-11 Nov. 2005, pp. 352-360.

TABLE III

Authors, Year, Ref. no	Purpose	Methodology	Attacks considered	Performance metrics	Trust property	Trust management model
Abusalah *et al.* (2006) [81]	Secure routing	Direct observation on forwarding packets Recommendation Evidences	Packet dropping	Routing overhead Route discovery time	N/A	TARP (trustaware routing protocol)
Sen *et al.* (2006) [83]	Secure routing	Direct observation Evidences	False accusation Packet dropping Tampering	Packet dropping rate Reputation level	Dynamicity	Group trust value is used based on reputations for neighboring nodes
Soltanali *et al.* (2007) [84]	Secure routing	Reputation only based on direct and indirect observation	Selfish nodes	Throughput Detection percentage	Dynamicity Weighted transitivity Subjectivity	An extension of DSR with the components of monitor, reputation manager, opinion manager, routing and forwarding manager
Balakrishnnan *et al.* (2007) [85]	Secure routing	Direct observation Recommendation	Packet dropping DoS (flooding) Routing information modification False accusation False recommendation	Packet delivery ratio Latency	Contextdependency Weighted transitivity Trust is a continuous value	Fellowship model using DSR
Li *et al.* (2008) [52]	Secure routing	Reputation Direct observation	Selective misbehaving Bad mouthing Onoff attack Conflicting behavior	Ratio of trustworthiness over reputation for both good and bad nodes	Weighted transitivity	Objective Trust Management Framework (OTMF) Modified Bayesian model
Mundinger & Boudec (2008) [86]	Secure routing	Direct observation Recommendation	False accusation /recommendation Freeriding	The incorrect reputation threshold point that does not affect the system performance	N/A	A general framework to evaluate robustness of reputation systems by analyzing them using deviation test.
Moe *et al.* (2008) [87]	Secure routing	Direct observation Recommendation	Selective packet dropping by selfish nodes DoS	Trustworthiness of a node	Dynamicity	Trustbased Secure Routing (TSR) An extension of DSR Incentive mechanism
Reidt *et al.* (2009) [88]	Secure routing	N/A (assume that information can be derived through observation or other mechanisms)	N/A	Communication cost Probability to reach Trust Authority (TA) nodes	N/A	A group of TA nodes are selected based on their reliability, energy level, and connectedness with the network.

[49] Z. Liu, A. W. Joy, and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," *Proc. 10th IEEE Int'l Workshop on Future Trends of Distributed Computing Systems*, Sushou, China, 26-28 May 2004, pp. 80-85.

[50] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, Feb. 2006.

[51] R. Li, J. Li, P. Liu, H. H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," *Proc. IEEE 65th Vehicular Technology Conf.*, 22-25 Apr. 2007, pp. 56-60.

[52] J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[53] F. Yunfang, "Adaptive Trust Management in MANETs," *Proc. 2007 Int'l Conf. on Computational Intelligence and Security*, Harbin, China, 15-19 Dec. 2007, pp. 804-808.

[54] P. G. Argyroudis and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks," *IEEE Commun. Surveys and Tutorials*, vol. 7, no. 3, pp. 2-21, 2005.

[55] D. Djenouri, L. Khelladi and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," *IEEE Commun. Surveys and Tutorials*, vol. 7, no. 4, pp. 2-28, 2005.

[56] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," *Wireless Network Security-Signals and Communication Technology*, Part II, 2007, pp. 103-135, Springer U.S.

[57] P. Kruus, D. Sterne, R. Gopaul, M. Heyman, B. Rivera, P. Budulas, B. Luu, T. Johnson, N. Ivanic, and G. Lawler, "In-Band Wormholes and Countermeasures in OLSR Networks," *Securecomm and Workshops 2006*, Baltimore, MD, 28 Aug. – 1 Sept. 2006, pp. 1-11.

[58] R. Maheshwari and S. R. Jie Gao Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," *Proc. 26th IEEE Int'l Conf. on Computer Communications*, Anchorage, AK, 6-12 May 2007, pp. 107-115.

[59] D. Sterne, G. Lawler, R. Gopaul, B. Rivera, K. Marcus, and P. Kruus, "Countering False Accusations and Collusion in the Detection of In-Band Wormholes," *Proc. 23rd Annual Computer Security Applications Conf.*, Miami Beach, FL, Dec. 2007, pp. 243-256.

[60] Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security and Privacy*, vol. 2, no. 3, May 2004, pp. 28-39.

[61] C. Kardof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proc. 1st IEEE Int'l Workshop on Sensor Network Protocols and Applications*, Anchorage, AK, USA, 11 May 2003, pp. 113-117.

[62] P. L. Campbell, "The Denial-of-Service Dance," *IEEE Security and Privacy*, vol. 3, no. 6, pp. 34-40, Nov./Dec. 2005.

[63] G. C. Hadjichristofi, W. J. Adams, and N. J. Davis, "A Framework for Key Management in a Mobile Ad Hoc Network," *Proc. Int'l Conf. on*

TABLE IV

Authors, Year, Ref. no	Purpose	Methodology	Attacks considered	Performance metrics	Trust property	Trust management model
Adnane *et al.* (2009) [90]	Secure routing	Direct & indirect information Evidences (PKI)	Fake identity General malicious nodes	N/A	N/A	Extension of OLSR No specific trust metric shown
Ayachi *et al.* (2009) [89]	Secure routing	Direct information	Message replication/ forgery/modification	N/A	N/A	Extension of AODV No specific trust metric shown
Weimerskirch *et al.* (2001) [91]	Authentication	Recommendation References	Packet modification Breach of confidentiality DoS	N/A	Weighted transitivity	Distributed Trust Model
Verma *et al.* (2001) [92]	Authentication	Direct observation Indirect information	General inside and outside attackers	N/A	Transitivity	An extension of DSR and ZRP
Pirzada & McDonald (2004) [93]	Authentication	Direct observation	Packet modification Packet fabrication Impersonation	N/A	Weighted transitivity Dynamicity	An extension of DSR An extension of Marsh's trust model [125]
Davis (2004) [47]	Authentication	Evidence-based (i.e., certificates)	False accusation	N/A	N/A	Certificate issuance, storage, validation, and revocation are considered
Ngai & Lyu (2004) [94]	Authentication	Direct observation Recommendation	False certificate	Successful, failure, and unreachable rate for detecting false certificates	Trust is a continuous value Asymmetry	Distributed trust-based authentication
Albers *et al.* (2002) [95]	Intrusion Detection	Direct observation for anomaly detection or misuse detection Policybased	General misbehaving nodes	N/A	Symmetry	Local Intrusion Detection System (LIDS)
Ahmed *et al.* (2006) [96]	Intrusion Detection	Direct observation	Black hole Packet dropping Malicious flooding Routing loop	Overhead False alarm rate	N/A	Leverage IDS to evaluate trust level of other nodes
Gray *et al.* (2002) [97]	Access control	Policy-based (local and global policies)	Loss of authorization	Trust level per session	Context-dependency Weighted transitivity Trust is a continuous value	Trustbased admission control
Luo *et al.* (2004) [98]	Access control	Direct observation	General misbehaving nodes	Overhead Delay and number of retries before ticket is received	Dynamicity	URSA(Ubiquitous and RobuSt Access control) Localized group trust model based on threshold cryptography

Information Technology: Coding and Computing, Tiejun Huang, China, 4-6 April 2005, vol. 2, pp. 568-573.

[64] Z. Yan, P. Zhang, and T. Virtanen, "Trust Evaluation Based Security Solutions in Ad Hoc Networks," *Proc. 7th Nordic Workshop on Security IT Systems*, Gjovik, Norway, 15-17 Oct. 2003.

[65] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation Systems," *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[66] N. Bhalaji and A. Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET," *Journal of Software*, vol. 4, no. 6, Aug. 2009, pp. 536-543.

[67] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. 6th Annual ACM/IEEE Mobile Computing and Networking*, Boston, MA, Aug. 2000, pp.255-265.

[68] S. Buchegger and J. –Y. Le Boudec, "Node Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," *Proc. IEEE 10th Euromicro Workshop on Parallel, Distributed, and Network-based Processing*, pp. 403-410, Canary Islands, Spain, Jan. 2002.

[69] S. Buchegger and J. –Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes- Fairness In Dynamic Ad-hoc NeTworks," *Proc. 3rd IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing*, Lausanne, CH, 9-11 June 2002, pp. 226-236.

[70] K. Paul and D. Westhoff, "Context-Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks," *Proc. IEEE Globecom Conf.*, Taipeh, Taiwan, 2002.

[71] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *The 6th IFIP Conf. on Security Communications, and Multimedia*, Porotoz, Slovenia, 2002.

[72] Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-Hoc Networks," *Proc. IEEE Wireless Communications and Networking Conf.*, vol. 2, pp. 825-830, March 2004.

[73] R. K. Nekkanti and C. Lee, "Trust-based Adaptive On Demand Ad Hoc Routing Protocol," *Proc. 42th Annual ACM Southeast Regional Conf.*, Huntsville, Alabama, 2004, pp. 88-93.

[74] X. Li, M. R. Lyu and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," *Proc. 2004 IEEE Aerospace Conf.*, Bug Sky, Montana, 6-13 Mar. 2004, vol. 2, pp. 1286-1295.

[75] N. Pisinou, T. Ghosh and K. Makki, "Collaborative Trust-based Routing in Multi-hop Ad Hoc Networks," *Proc. 3rd Int'l IFIP-TC06*

TABLE V

Authors, Year, Ref. no	Purpose	Methodology	Attacks considered	Performance metrics	Trust property	Trust management model
Adams & Davis (2005) [17]	Access control	Direct observation Reputation	General misbehaving nodes	N/A	Conditional transitivity[1] Trust is a continuous value	Bayesian Model for risk assessment
Yunfang (2007) [53]	Access control	Direct observation Reputation Policybased	General misbehaving nodes	N/A	Weighted transitivity	Integrated (policy-based plus reputation-based) adaptive trust management
Virendra *et al.* (2005) [99]	Key Management	Direct/indirect observation	False key generation Compromise of other nodes' keys	N/A	Weighted transitivity Subjectivity Dynamicity Trust is a continuous value	Physical-Logical Trust Domains (PLTDs)
Hadjichristofi *et al.* (2005) [63]	Key Management	Direct observation Reputation	Stacking attack General malicious nodes	% of available nodes with capability of service provision Average shortest path % of isolated nodes Success ratio to obtain system service	Trust ranges from 1 to 100 Dynamicity	A modified hierarchical trust PKI model
Adams *et al.* (2005) [17]	Key Management Nonrepudiation	Direct observation Reputation	Selfish nodes Blackmailing Stacking attack	Trust value	Contextdependency Trust is a continuous number Subjectivity Dynamicity	Interpersonal trust model Redemption Simple weighted model
Li *et al.* (2006) [100]	Key Management	Direct observation	Fake certificate Tampering	Average overhead of the repository in each node	Transitivity	Localized Public-Key Management (LPM) Combining certificate chain and communication path based on PGP
Chang & Kuo (2009) [101]	Key Management	Direct observation	On-Off attack Conflicting behavior attack Newcomer attack Fake ID attack Cheating attack Collusion attack	Trust value Packet delivery ratio	Trust value is a discrete value	Markov chain trust model
Yan *et al.* (2003) [64]	Trust evaluation	Direct observation Reputation Recommendation	Black hole DoS	Planned metric: security level	Subjectivity Weighted transitivity	Personal Trusted Bubble (PTB)

Networking Conf., Lecture Notes in Computer Science, Athens, Greece, 9-14 May 2004, vol. 3042, pp. 1446-1451.

[76] S. Buchegger and J.Y.L. Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," *Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems*, 15 Nov. 2004.

[77] T. Ghosh, N. Pissinou, and K. Makki, "Towards Designing a Trust Routing Solution in Mobile Ad Hoc Networks," *Mobile Networks and Applications*, vol. 10, pp. 985-995, 2005.

[78] B. Wang, S. Soltani, J. Shapiro, and P. Tab, "Local Detection of Selfish Routing Behavior in Ad Hoc Networks," *Proc. 8th Int'l Symposium on Parallel Architectures, Algorithms and Networks* , 7-9 Dec. 2005, pp. 392-399.

[79] C. Zouridaki, B. L. Mark, M. Hejmo and R. K. Thomas, "Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs," *Proc. 3rd ACM Workshop on Security for Ad Hoc and Sensor Networks*, Alexandria, VA, Nov. 7, 2005.

[80] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "Robust Cooperative Trust Establishment for MANETs," *Proc. 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, VA, 30 Oct. 2006, pp. 23-34.

[81] A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad Hoc Networks," *Proc. 27th Australasian Computer Science Conf.*, vol. 26, pp. 47-54, 2004.

[82] L. Abusalah, A. Khokhar, and M. Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," *IEEE Commun. Surveys and Tutorials*, vol. 19, no. 4, pp.78-93, 2008.

[83] J. Sen, P. Chowdhury, and I. Sengupta, "A Distributed Trust Mechanism for Mobile Ad Hoc Networks," *Int'l Symposium on Ad Hoc and Ubiquitous Computing*, 20-23 Dec. 2006. Surathkal, India, pp. 62-67.

[84] S. Soltanali, S. Pirahesh, S. Niksefat, and M. Sabaei, "An Efficient Scheme to Motivate Cooperation in Mobile Ad Hoc Networks," *Int'l Conf. on Networking and Services*, Athens, Greece, 19-25 June 2007, pp. 98-103.

[85] V. Balakrishnnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and Recommendations in Mobile Ad Hoc Networks," *Int'l Conf. on Networking and Services*, Athens, Greece, 19-25 June 2007, pp. 64-69.

[86] J. Mundinger and J. Le Boudec, "Analysis of a Reputation System for Mobile Ad Hoc Networks with Liars," *Performance Evaluation*, vol. 65, no. 3-4, pp. 212-226, Mar. 2008.

[87] M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "TSR: Trust-based Secure MANET Routing using HMMs," *Proc. 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Vancouver, British Columbia, Canada, 27-28 Oct. 2008, pp. 83-90.

[88] S. Reidt, S. D. Wolthusen, and S. Balfe, "Robust and Efficient Communication Overlays for Trust Authority Computations," *Proc. 2009 IEEE Sarnoff Symposium*, March 2009.

TABLE VI

Authors, Year, Ref. no	Purpose	Methodology	Attacks considered	Performance metrics	Trust property	Trust management model
Jiang & Baras (2004) [103]	Trust evidence distribution	Evidence-based (certificates) Direct observation	General misbehaving nodes	Number of hops and delay to obtain the certificate Success rate obtaining the certificate		Ant-Based adaptive trust Evidence Distribution (ABED) based on a *swarm intelligence paradigm*
Baras & Jiang (2004) [104]	Trust computation	Local direct observation Evidencebased (certificates) Recommendation (i.e., voting)	General misbehaving nodes	Probability of having at least one secure path between trusted pairs percentage of trusted nodes in the network Time taken to converge to a steady state in trustworthiness of all nodes	Dynamicity	Distributed trust computation model using graph theory and random theory
Theodorakopoulos & Baras (2006) [50]	Trust evaluation	Direct observation Recommendation	False accusation Impersonation	Confidence level Opinions about other nodes	Transitivity Trust and confidence value is binary	Trust evaluation model based on *Semirings* theory
Boukerche & Ren (2008) [105]	Reputation evaluation	Direct observation Reputation	General misbehaving nodes	Query overhead Security overhead Percentage of packets Number of nodes Percentage of malicious nodes	Weighted transitivity	Generalized Reputation Evaluation (GRE) Prototype Groupbased trust model
Moloney & Weber (2005) [106]	General security level identification	Direct/indirect observation Recommendation	General misbehaving nodes	N/A	Context-dependency	Context-aware security system for MANETs
Cho *et al*. (2009) [107]	Battlefield trust establishment under no prior interactions	Direct/indirect observation Recommendation	General misbehaving nodes	Trust level	Dynamicity Weighted transitivity Context-dependency Asymmetry Subjectivity	Quantitative modeling technique used called hierarchical Stochastic petri nets

[89] M. A. Ayachi, C. Bidan, T. Abbes, and A. Bouhoula, "Misbehavior Detection Using Implicit Trust Relations in the AODV Routing Protocol," *2009 Int'l Conf. on Computational Science and Engineering*, Vancouver, Canada, vol. 2, 29-31 Aug. 2009, pp. 802-808.

[90] A. Adnane, C. Bidan, R. T. de Sousa, "Trust-based Countermeasures for Securing OLSR Protocol," *2009 Int'l Conf. on Computational Science and Engineering*, Vancouver, Canada, vol. 2, 28-31 Aug. 2009, pp. 745-752.

[91] A. Weimerskirch and G. Thonet, "A Distributed Light-Weight Authentication Model for Ad-hoc Networks," *Proc. of 4th Int'l Conf. on Information Security and Cryptology*, 6-7 Dec. 2001.

[92] R. R. S. Verma, D. O'Mahony and H. Tewari, "NTM – Progressive Trust Negotiation in Ad Hoc Networks," *Proc. 1st Joint IEI/IEE Symposium on Telecommunications Systems Research*, Dublin, Ireland, 27 Nov. 2001.

[93] A. A. Pirzada, C. McDonald, and A. Datta, "Performance Comparison of Trust-based Reactive Routing Protocols," *IEEE Trans. Mobile Comput.*, vol. 5, no. 6, June 2006, pp. 695-710.

[94] E. C. H. Ngai and M. R. Lyu, "Trust and Clustering-based Authentication Services in Mobile Ad Hoc Networks," *Proc. 24th Int'l Conf. on Distributed Computing Systems Workshops*, 23-24 March 2004, pp. 582-587.

[95] P. Albers, O. Camp, J.-M. Percher, B. Jouga, L. Me, R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches", *Proc. 1st Int'l Workshop on Wireless Information Systems*, Apr. 2002, pp. 1-12.

[96] E. Ahmed, K. Samad and W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks." *AusCERT Asia Pacific Information Technology Security Conf.*, Gold Coast, Australia, 21-26 May 2006.

[97] E. Gray, P. O'Connell, C. Jensen, a. Weber, J.-M. Seigneur, and C. Yong, "Towards a Framework for Assessing Trust-based Admission Control in Collaborative Ad Hoc Applications," *Technical Report*, TCD-CS-2002-66, Trinity College Dublin, 2002.

[98] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 6, Dec. 2004, pp. 1049-1063.

[99] M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks," *Proc. Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems*, 18-21 April 2005, pp. 65-70.

[100] R. Li, J. Li, P. Liu, and H. H. Chen, "On Demand Public Key Management for Mobile Ad Hoc Networks," *Wiley's Wireless Communications and Mobile Computing*, May 2006, vol. 6, no. 3, pp. 295-306.

[101] B. J. Chang and S. L. Kuo, "Markov Chain Trust Model for Trust Value Analysis and Key Management in Distributed Multicast MANETs," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, May 2009, pp. 1846-1863.

[102] A. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure and P. Spilling, "A Survey of Key Management in Ad Hoc Networks," *IEEE Commun. Surveys and Tutorials*, vol. 8, no. 3, pp. 48-66, 2006.

[103] T. Jiang and J. S. Baras, "Ant-based Adaptive Trust Evidence Distribution in MANET," *Proc. 2nd Int'l Conf. on Mobile Distributed Computing Systems Workshops*, Tokyo, Japan, 23-24 March 2004, pp.588-593.

[104] J. S. Baras and T. Jiang, "Cooperative Games, Phase Transition on Graphs and Distributed Trust in MANETs," *Proc. 43th IEEE Conf. on Decision and Control*, Atlantis, Bahamas, 14-17 Dec. 2004, vol. 1, pp. 93-98.

[105] A. Boukerche and Y. Ren, "A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks," *Proc. Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, Vancouver, British Columbia, Canada, pp. 88-95, 2008.

[106] M. Moloney and S. Weber, "A Context-aware Trust-based Security System for Ad Hoc Networks," *Proc. 1st Int'l Conf. on Security and Privacy for Emerging Areas in Communication Networks-Workshop*, 5-9 Sept. 2005, pp. 153-160.

[107] J. H. Cho, A. Swami and I.R. Chen, "Modeling and Analysis of Trust Management for Cognitive Mission-driven Group Communication Systems in Mobile Ad Hoc Networks," *2009 Int'l Conf. on Computational Science and Engineering*, vol. 2, Vancouver, Canada, 29-31 Aug. 2009, pp. 641-650.

[108] Q. Mahmoud (Editor), "Cognitive Networks: Towards Self-Aware Networks," Wiley, Sept. 2007.

[109] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, June 2008, pp. 576-589.

[110] M. Maheswaran, H. C. Tang, and A. Ghunaim, "Toward a Gravity-based Trust Model for Social Networking Systems," *Proc. 27th Int'l Conf. on Distributed Computing Systems Workshops*, 22-29 June 2007, pp. 24-31.

[111] R. Kohlas, J. Jonczy, and R. Haenni, "A Trust Evaluation Method Based on Logic and Probability Theory," *Trust Management II: IFIP Int'l Federation for Information Processing*, vol. 263, 2008, Springer Boston.

[112] G. Yin, D. Shi, H. Wang, and M. Guo, "RepCom: Towards Reputation Composition over Peer-to-Peer Communities," *2009 Int'l Conf. on Computational Science and Engineering*, vol. 2, Vancouver, Canada, 29-31 Aug. 2009, pp. 765-771.

[113] L. Boursas and W. Hommel, "Multidimensional Dynamic Trust Management for Federated Services," *2009 Int'l Conf. on Computational Science and Engineering*, vol. 2, Vancouver, Canada, 29-31 Aug. 2009, pp.684-689.

[114] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of Trust and Distrust," *Proc. 13th Int'l Conf. on World Wide Web*, New York, NY, 19-21 May 2004, pp. 403–412.

[115] Y. Wang and M. P. Singh, "Trust Representation and Aggregation in a Distributed Agent System," *Proc. 21st National Conf. on Artificial Intelligence (AAAI)*, 2006, Boston, MA, pp. 1425–1430.

[116] Y. Wang and M. P. Singh, "Formal Trust Model for Multiagent Systems," *Proc. 20th Int'l Joint Conf. on Artificial Intelligence*, Jan. 2007, pp. 1551–1556.

[117] X. Hong, D. Huang, M. Gerla, and Z. Cao, "SAT: Building New Trust Architecture for Vehicular Networks," *ACM SIGCOMM 3rd Int'l Workshop on Mobility in the Evolving Internet Architecture*, Seattle, WA, 22 Aug. 2008.

[118] U. S. Army Research Laboratory, Program Announcement for Network Science CTA, [Online]: http://www.arl.army.mil/www/DownloadedInternetPages/CurrentPages/CTA/Documents/NSCTAFINAL23JAN09.pdf, 23 Jan. 2009.

[119] D. Agrawal, H. Chivers, J. Clark, C. Jutla, and J. McDermid, "A Proposal for Trust Management in Coalition Environments," *26th Army Science Conf.*, 14 Dec. 2008.

[120] M. Blaze, S. Kannan, I. Lee, O. Sokolsky, J.M. Smith, A.D. Keromytis, and W. Lee, "Dynamic Trust Management," *Computer*, vol. 42, no. 2, Feb. 2009, pp. 44-52.

[121] M. Tavakolifard , "Situation-aware Trust Management," *Proc. 2009 ACM Conf. on Recommender Systems*, New York, USA, Oct. 2009, pp. 413-416.

[122] M. Tavakolifard, P. Herrmann, and S. J. Knapskog, "Inferring Trust based on Similarity with TILLIT," *Proc. 3rd IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2009)*, *IFIP Advances in Information and Communication Technology: Trust Management III*, vol. 300, Springer Boston, West Lafayette, USA, June 2009, pp. 138-148.

[123] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," *Proc. 12th Int'l Conf. on World Wide Web*, New York, NY, 20-23 May 2003, pp. 640–651.

[124] H. Zhang, A. Goel, R. Govindan, K. Mason, and B. Van Roy, "Making Eigenvector-based Reputation Systems Robust to Collusion," *Proc. 3rd Int'l Workshop on Algorithms and Models for the Web-Graph*, LNCS, vol. 3243, Oct. 2004, pp. 92-104.

[125] S. Marsh, "Formalizing Trust as a Computational Concept," Ph. D. Dissertation, *Department of Mathematics and Computer Science*: University of Stirling, 1994.

Jin-Hee Cho received her BA from Ewha Womans University, and MA from Washington University in St. Louis, MO in 1997, and 1999 respectively. She also received her MS, and PhD in Computer Science from Virginia Tech in 2004, and 2008 respectively. She received an IREAN fellowship through the NSF IGERT program during her Ph.D. study and a postdoctoral research fellowship through the Army Research Laboratory/Oak Ridge Associated Universities postdoctoral fellowship program from January 2009 to June 2010. After then, she joined ARL, Adelphi, MD as a computer scientist in the Network Science Division, Computational and Information Sciences Directorate. Her research interests include wireless mobile networks, mobile ad hoc networks, sensor networks, secure group communications, group key management, network security, intrusion detection, performance analysis, trust management, social/cognitive networks, and network economic modeling. She is a member of the IEEE and ACM.

Ananthram Swami received the B.Tech. degree from the Indian Institute of Technology (IIT), Bombay; the M.S. degree from Rice University, Houston, TX, and the Ph.D. degree from the University of Southern California(USC), Los Angeles, all in electrical engineering.

He has held positions with Unocal Corporation, USC, CS-3 and Malgudi Systems. He was a Statistical Consultant to the California Lottery, developed HOSAT, a MATLAB-based toolbox for non-Gaussian signal processing, and has held visiting faculty positions at INP, Toulouse, France. He is the ST for Network Science at the U.S. Army Research Laboratory. His work is in the broad areas of signal processing, wireless communications, sensor and mobile ad hoc networks. He is co-editor of the book Wireless Sensor Networks: Signal Processing and Communications Perspectives (New York: Wiley, 2007).

Dr. Swami is a member of the IEEE Signal Processing Society's (SPS) Technical Committee on Sensor Array and Multichannel systems and serves on the Senior Editorial Board of the IEEE Journal on Selected Topics in Signal Processing. He was a tutorial speaker on Networking Cognitive Radios for Dynamic Spectrum Access at IEEE ICC 2010, co-chair of IEEE SPAWC'10, and has served on the IEEE SPS BoG.

Ing-Ray Chen received the BS degree from the National Taiwan University, Taipei, Taiwan, and the MS and PhD degrees in computer science from the University of Houston. He is a professor in the Department of Computer Science at Virginia Tech. His research interests include mobile computing, wireless networks, security, fault tolerance, multimedia, trust management, real-time intelligent systems, and performance analysis. Dr. Chen currently serves as an editor for The Computer Journal, Wireless Personal Communications, Wireless Communications and Mobile Computing, Security and Communication Networks, and International Journal on Artificial Intelligence Tools. He is a member of the IEEE and ACM.