14th ICCRTS

"C2 and Agility"

Title:
Towards Trust-based Cognitive Networks:
A Survey of Trust Management for Mobile Ad Hoc Networks

Topic:
2 - Networks and Networking

Name of Authors:
Jin-Hee Cho, Ph. D.
Army Research Laboratory – Computer and Information Sciences Directorate

Ananthram Swami, Ph. D.
Army Research Laboratory – Computer and Information Sciences Directorate

Point of Contact:
Jin-Hee Cho, Ph. D.
Computational & Information Sciences Directorate (CISD)
Communications and Network Systems Division
U.S. Army Research Laboratory (USARL)
2800 Powder Mill Rd, Adelphi, MD 20783
301-394-0492
jinhee.cho@us.army.mil

Towards Trust-based Cognitive Networks: A Survey of Trust Management for Mobile Ad Hoc Networks

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, or reconfigurability. In defining trust 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, mobility, node failure, propagation channel conditions) in a military MANET. We seek to combine notions of "social trust" derived from social networks with "quality-of-service (QoS) trust" derived from communication networks to obtain a composite trust metric. We will discuss the concept and properties of trust and derive some unique characteristics of trust in MANETs, drawing upon social notions of trust. We will give a survey of trust management schemes developed for MANETs and will discuss generally accepted classifications, potential attacks, and trust metrics in MANETs. Finally, we will suggest future research directions on trust management in MANETs based on the concept of social and cognitive networks.

1. Introduction

Security protocol designers for mobile ad hoc networks (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, high security threats or vulnerability, unreliable communication, and rapid changes in topologies or memberships due to user mobility or node failure. Security in a tactical network includes notions of communications security which is amenable to quantification and analysis, as well as the *perception* of security which is harder to quantify.

The concept of "Trust" originally derives from the social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity. Blaze *et al.* [9] first introduced the term "Trust Management" and identified it as a separate component of security services in networks. Trust management in MANETs is needed when participating nodes, without any previous interactions, must establish a network with an acceptable level of trust relationships among themselves. Typical examples include building initial trust bootstrapping, coalition operation without predefined trust, third-party certificate authentication when links are down, and in ensuring safety in battlefield situations [11]. In addition, trust management has diverse applicability in many decision making situations including intrusion detection [3, 4], authentication [14, 34, 42], access control [2, 28, 45], and isolation of misbehaving nodes for effective routing [6, 7, 8, 14, 16, 22, 30, 33, 34, 35, 39, 42, 46, 47].

Trust management, including trust establishment, trust update, and trust revocation, is much more challenging in a MANET than in traditional centralized environments. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to mobility induced changes in network topology. Resource constraints further confine the trust evaluation process to only local information, so that trust establishment would be based on incomplete and incorrect information. The dynamic nature and characteristics of MANETs result in uncertainty and incompleteness of the trust evidence that is continuously changing over time [11].

Despite a couple of surveys on trust [26, 37], a comprehensive survey of trust management in MANETs does not exist and is the main aim of this paper. The contributions of this paper are: (1) to give a clear definition of trust in the communication and networking field, (2) to extensively survey the existing trust management schemes developed for MANETs, and (3) to address novel trust metrics for MANETs based on the concepts of social and cognitive networks.

The rest of this paper is organized as follows. In Section 2, we introduce the concept of *trust* and provide a clear distinction between trust and trustworthiness, and also discuss the relationship between trust and risk. We also introduce the properties of trust as well as the main characteristics of trust in MANETs. Section 3 surveys generally accepted classifications of trust management schemes; attack models considered in current trust management schemes; trust metrics including the concepts of social trust and quality-of-service (QoS) trust; and a survey of existing trust management schemes for MANETs. Section 4 briefly describes future directions for developing trust management schemes in MANETs as well as our ongoing research based on the concepts of social networks and cognitive networks. Section 5 concludes this paper.

2. Concept and Properties of Trust

We review how trust is defined in different fields and how these trust concepts can be applied in modeling network trust. Further, we examine the relationship between trust and risk: how trust can be defined in order to realistically reflect the unique characteristics of MANETs.

2.1 What is Trust?

There are multiple definitions of trust, ranging from the *Merriam Webster dictionary* definition of "assured reliance on the character, strength, or truth of someone or something"; Gambetta's definition of *sociological trust* [13] as a subjective probability that the particular action that will be performed by an agent; definitions in *economics* based on the notion that humans are rational and seek to maximize their own utility functions [19]; definitions in psychology that involve reciprocity, loss and restoration [49]; definitions in organizational management as the willingness to take risk or be vulnerable [31], which need not be reciprocal, or mutual; to the modeling of trust in human-agent interactions.

The concept of trust is important to *communication and network* protocol designers where establishing trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. According to Eschenauer *et al*. [11], 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." Trust has also been defined as the degree of belief about the behavior of other entities (or agents) [10], often with an emphasis on context [26].

2.2Trust, Trustworthiness, and Risk

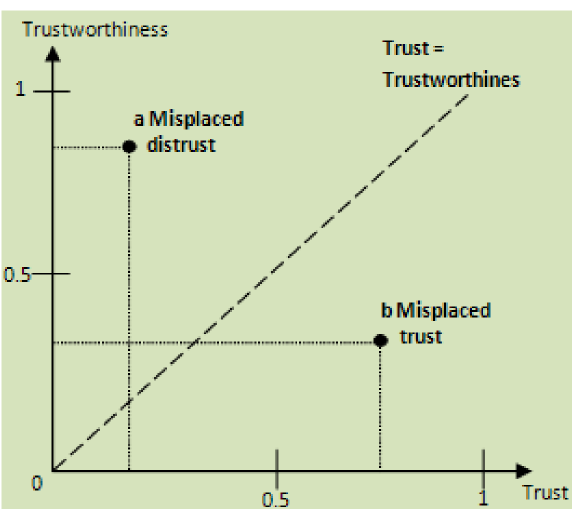

Figure 1: Trust Level [38].

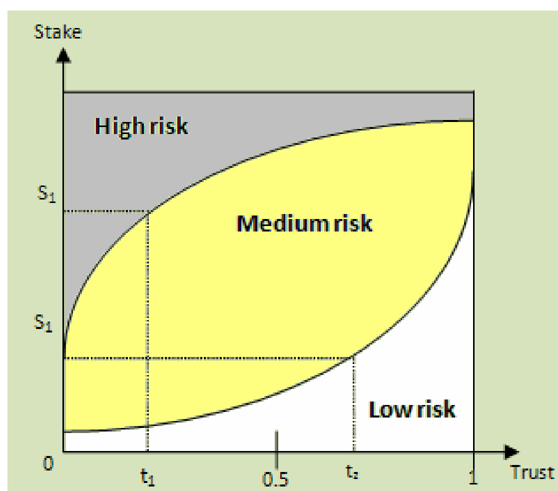

Figure 2: Risk and Trust [38].

In the literature, the terms *trust* and *trustworthiness* seem to be interchangeably used without clear distinction. Josang *et al*. [21] clarified the difference between trust and trustworthiness based on their definitions provided by Gambetta [13]. The level of trust is defined as the belief probability varying from 0 (complete distrust) to 1 (complete trust) [21]. In this sense, trustworthiness is a measure of the actual probability that the trustees will behave as expected.

Solhaug *et al.* [58] define *trustworthiness* as the objective probability that the trustee performs a particular action on which the interests of the trustor depend. Figure 1 [38] 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. In Figure 1, the diagonal dashed line is assumed to be marks of well-founded trust in which the subjective probability of trust (i.e., trust) is equivalent to the objective probability (i.e., 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 inconclusiveness about or a miscalculation of the involved risk. That is, the subjective aspect of trust brings incorrect risk estimation and wrong risk management accordingly. Figure 1 shows 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 well-founded trust, misplaced trust increases risk and thus the chance of deceit, as shown in the example marked with a and *b* in Figure 1. 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 the networks. One can also distinguish between two types of trust [21]: (1) a context independent *reliability trust* which measures the perceived reliability of 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 including utility and risk attitude. As an example, one may not trust an old rope for climbing from the 3rd floor of a building during a fire exercise (reliability trust) while trusting the rope in a real fire (decision trust).

The relationship between trust and risk has been studied in [21, 38]. Figure 2 shows an example of three different risk values: low, medium, and high. The risk value is low for all trust values when the stake is close to zero. If the stake is too high, risk is regarded as high regardless of the estimated trust value. The risk is generally low when the trust value is high. However, the risk value should be determined based on the value at stake as well as the risk probability; as shown in Figure 2 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) [21, 38]. 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 his or her acceptable risk level in terms of the calculated prospects. In general, trust is neither proportional nor inversely proportional to risk [21, 38].

2.3 Properties of Trust

Golbeck [15] discusses the three main properties of trust in the context of a social network perspective: *transitivity*, *asymmetry*, and *personalization*. *First*, trust is *not perfectly transitive* in a mathematical sense. That is, if *A* trusts *B*, and *B* trusts *C*, it does not guarantee that *A* trusts *C*. *Second*, trust is *not necessarily symmetric*, meaning not identical in both directions. A typical example of asymmetry of trust can be found in the relationships between supervisors and employees. *Third*, trust is inherently a *personal opinion*. Two people often evaluate trustworthiness about the same entity differently.

2.4 Characteristics of Trust in MANETs

Due to the unique characteristics of MANETs and the inherent unreliability of the wireless medium, the concept of trust in MANETs should be carefully defined. The main features of trust in MANETs are as follows [2, 10, 11, 23, 39]:

1. A decision method to determine trust against an entity should be *fully distributed* since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed.
2. Trust should be determined in a *highly customizable* manner without excessive computation and communication load, while also capturing the complexities of the trust relationship.
3. A trust decision framework for MANETs should not assume that all nodes are cooperative. In resource-restricted environments, *selfishness* is likely to be prevalent over cooperation, for example, in order to save battery life or computational power.
4. Trust is *dynamic*, not static.
5. Trust is subjective.
6. Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.
7. Trust is asymmetric and not necessarily reciprocal.
8. Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

3. Trust Management for MANETs

This section surveys existing trust management schemes developed for MANET environments. Before reviewing the literature, we would like to clarify some terminologies that have often been used interchangeably. In general, trust management is interchangeably used with reputation management [26]. However, there are important differences between trust and reputation. Trust is active while reputation is passive [24]. 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. 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 [1, 37]. As most of the literature agrees, reputation management is regarded as part of trust management based on widely accepted classifications explained below.

3.1 Classifications

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 [38]. Trust management includes trust establishment (i.e., collecting appropriate trust evidences, trust generation, trust distribution, trust discovery, and evaluation of trust evidence), trust update, and trust revocation [21, 40]. This section introduces popularly used classifications of trust management based on methodologies used for collecting information to evaluate trust.

Li *et al*. [22] classify trust management as *reputation-based framework* and *trust establishment framework*. A reputation-based framework uses direct observation and second-hand information distributed among a network to evaluate other nodes. A trust establishment framework evaluates neighboring nodes based on direct observations while trust relations between two nodes with no prior direct interactions are built through a combination of opinions from intermediate nodes.

Yonfang [45] suggests two different approaches to evaluate trust: *policy-based trust management* and *reputation-based trust management*. Policy-based approach 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. Such a policy-based trust management approach usually makes 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. On the other hand, reputation-based trust management utilizes numerical and computational mechanism to evaluate trust. Typically, trust is calculated by collecting, aggregating, and disseminating reputation among the entities.

According to Li and Singhal [26], trust management is classified as *evidence-based trust management* and *monitoring-based trust management*. Evidence-based trust management considers anything that proves the trust relationships among nodes including public key, address, identity, or any evidence that any node can generate for itself or other nodes through a challenge/response process. Monitoring-based trust management rates the trust level of each participating node based on direct information (e.g., observing neighboring nodes' benign or malign behaviors such as packet dropping or packet flooding) as well as indirect information (e.g., reputation ratings forwarded from other nodes such as recommendation).

Classifications of reputation management schemes may be found in [2] and [45].

3.2 Potential Attacks

Liu *et al*. [25] describe the characteristics of attacks in MANETs by both the nature of attack and the type of attacker. One classification of attacks is ***passive attack*** versus ***active attack***. Passive attack occurs when an unauthorized party gains access to an asset but does not modify its content. Passive attack can be either eavesdropping or 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. That is, in a more subtle way, the attacker gains intelligence by monitoring transmitted data content. Active attack occurs when an unauthorized party modifies a message, data stream, or file. Active attack usually takes 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*) (i.e., excessive resource consumptions in networks).

Attacks can be classified broadly as ***insider attack*** versus ***outsider attack*** [25]. If an entity is authorized to access system resources but employs them in a malicious way, it is classified as an *insider attack*. On the other hand, an *outsider attack* is initiated from unauthorized or illegitimate user from the system. They usually acquire access to an authorized account and try to perpetrate an inside attacker. 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 and malicious nodes. Specific examples of network layer attacks are as follows [10, 11, 12, 17, 18, 22, 25, 26, 39, 43]:

- ***Routing loop attack***: A malicious node may modify routing packets in such a way that the packets traverse a cycle, so that the packet does not reach the intended destination.
- ***Wormhole attack***: A group of cooperating malicious nodes can pretend to connect two distant points in the network with a low-latency communication link called wormhole link, causing disruptions in normal traffic load and flow.
- ***Black hole attack***: A malicious node, the so called black hole node, may respond always positively for route requests even without proper routing information. The black hole can drop all packets forwarded to it.
- ***Gray-hole attack***: A malicious node may selectively drop packets, as a special case of black hole attack. Variations include the *sinkhole attacker* that selectively routes packets.
- ***Denial-of-Service (DoS) attack***: A malicious node may block the normal use or management of communications facilities, for example, by causing excessive resource consumption.
- ***False information or false recommendation***: A malicious node may collude and provide false recommendations/information to isolate good nodes while keeping more malicious nodes. This attack also called a *black-mounting attack*.
- ***Incomplete information*****:** A malicious node may not cooperate in providing proper or complete information. Usually compromised nodes collude to perform this attack. Distinguishing malicious behaviors from normal behaviors is difficult in MANETs.
- ***Packet modification/insertion***: A malicious node may modify packets or insert malicious packets such as packets with incorrect routing information.
- ***Newcomer attack*****:** A malicious node may remove their bad reputation/distrust by registering as a new user. The malicious node simply leaves the system and joins again for trust revocation, flushing out previous bad history and starting to accumulate new trust.
- ***Sybil attack***: A malicious node can offer multiple identities to the network which can affect topology maintenance and fault tolerant schemes such as multi-path routing.
- ***Blackmailing***: A malicious node can blackmail another node by falsely claiming that another node is malicious or misbehaving. This can generate significant amount of traffic and ultimately disrupt the functionality of the entire network.
- ***Replay attacks***: A malicious node may replay earlier transmitted packets to the network. If the adversary replays route requests, old locations and routing information might make nodes unreachable.
- ***Selective misbehaving attack***: This attack is derived from the subjective characteristic of the trust management framework. A malicious node may selectively provide or deny proper services.
- ***On-off attack***: A malicious node may alternatively behave well and badly to stay undetected while disrupting services.
- ***Conflicting behavior attack***: A malicious node may behave differently to nodes in different groups to make the opinions from different good groups conflicting, and ultimately lead to non-trusted relationships.

3.3 Trust Metrics for MANETs

Even though many trust management schemes have been proposed, no work clearly addresses what should be measured to evaluate trust. Liu *et al.* [24] define trust in their model as reliability, timeliness, and integrity of message delivery to their intended next-hop. Also most trust-based protocols for secure routing calculate a trust value based on characteristics of well behaving nodes [6, 7, 8, 14, 16, 22, 30, 33, 34, 35, 39, 42, 46, 47]. Trust measurement can be application-dependent and will be different based on the design goals of the proposed network. In this work, we introduce two types of trust based on trust relationships that require measurements of different aspects of trust.

First, ***social trust*** refers to properties derived from social relationships. Examples of social networks are strong social relationships such as colleagues or relatives or loose social relationships such as school alumni or friends with common interests [44]. Social trust may include friendship, honesty, privacy, and social reputation/recommendation derived from direct or indirect interactions for "sociable" purpose. In MANETs, some metrics to measure these social trust properties can be frequency of communications, malign or benign behaviors (e.g., false accusation, impersonation), and quality of reputation.

Second, ***QoS trust*** represents competence, dependability, reliability, successful experience, and reputation/recommendation on task performance forwarded from direct or indirect interactions with others. In designing network protocols, many prior works measured the trust value of a node based on performance metrics such as the node's energy or computational power, lifetime, packet delivery rate, or evaluations using reputation or recommendation from other nodes about task performance. The term *QoS trust* is used in this work to define trust evaluation mainly in terms of task performance capability.

3.4 Existing Trust Management in MANETs

Trust management schemes have been developed for specific purposes such as secure routing, authentication, intrusion detection, and access control (authorization). Appendix A summarizes existing trust management schemes by scheme name, methodology, attacks targeted, performance metrics used, and other notable characteristics of the proposed schemes. In Appendix A, note that *methodology* explains how trust evidence is collected and *performance metrics* refers to the metrics used to evaluate the proposed trust management scheme. A narrative description of these schemes and an overview of some existing frameworks for trust evidence distribution and evaluation will be included in the journal version of this paper.

Trust Evidence Distribution and Evaluation

Some trust management schemes have been proposed in order to provide a general framework for trust evidence distribution or evaluation in MANETs. Jiang and Baras [20] proposed a trust distribution scheme called ABED (Ant-Based trust Evidence Distribution) based on the *swarm intelligence paradigm*, which is claimed to be highly distributed and adaptive to mobility. The swarm intelligence paradigm is widely used in dynamic optimization problems (e.g., traveling salesman problem, routing in communication networks) and is inspired from artificial ant colony techniques to solve combinatorial optimization problem. The key principle is called *stigmergy*, indirect communication through the environment. In ABED, nodes interact with each other through "agents" called ``ants'' that deposit information called "pheromones"; based on this the agents can identify an optimal path for accumulating trust evidence. However, no specific attacks were considered in [20]. Theodorakopoulos and Baras [40] proposed a trust evidence evaluation scheme for MANETs. The evaluation process is modeled as a path problem in a directed graph where nodes indicate entities and edges represent trust relations. The authors employ the theory of *Semirings* to show how two nodes can establish trust relationships without prior direct interactions. Their case study uses the GP web of trust to express an example trust model based on *Semirings* and shows that their proposed 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 as a continuous-valued variable. Even though no centralized trusted third party exists, their work makes use of a source node as a trusted infrastructure. Recently Buckerche and Ren [5] proposed a distributed reputation evaluation prototype called GRE (Generalized Reputation Evaluation) to effectively prevent malicious nodes from entering the trusted community. However, no specific attack model was addressed. Further, transitivity, asymmetry, and subjectivity characteristics of trust concept were not specifically explained in building their trust model.

4 Towards Trust-based Cognitive MANETs

In this section, we discuss a trust management scheme based on the concept of social and cognitive networks. In addition, we list several issues and questions that developers of MANET trust management schemes should keep in mind.

MANETs pose challenges in designing network security protocols due to their unique characteristics (e.g., resource constraints, vulnerability, unreliable transmission medium, and dynamics). Military MANETs must operate in hostile environments, deal with compromised nodes, support prioritized QoS performance, be able to participate in coalition operations without predefined trust relationships, and facilitate reconfigurability [36]. Thus, additional caution is required in designing security protocols for mission-driven group communication systems (GCSs) in military MANETs
We are particularly interested in evaluating the trust level of such a GCS by evaluating the trust value of a node in terms of its mission execution competence and sociability when a particular mission, X, is assigned. For example, we evaluate each node by asking "Can we trust this group member (node) to do mission X?" That is, our trust management protocol aims to dynamically reconfigure the trust threshold that determines the number of nodes qualified for performing the mission. We take into account the level of risk or difficulty upon failure while considering changing network conditions (i.e., bandwidth, node density, communication rate, degree of hostility) as well as the conditions of participating nodes in the network (i.e., energy, computational power, memory). As a result, the resulting protocols seek to prolong the system lifetime by identifying optimal design settings such as trust value threshold to determine trustable nodes to perform a mission, degree of trust transitivity chains, ratio of trust attributes (i.e., ratio of social trust versus QoS trust, explained in Section 3.3), conditional tolerance threshold of selfish behaviors, and length of trust chains based on efficient tradeoffs made between security and performance properties.

Unlike existing work on trust management in MANETs, our research proposes to embed intelligence in each node with cognitive functionality, adopting recent ideas about *cognitive networks* in wireless networks [41]. Thomas *et al*. [41] define a cognitive network first 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 level (e.g., facilitating cooperation among nodes) as a forward looking mechanism [41]. Cognitive networks are also often based on *cross-layer design* where they share internal information between layers rather than adhering to the traditional strict layered architecture [41].. We propose to use this concept of cognitive networks with cross-layer design for GCS operations in a MANET to introduce cognitive intelligence into each node to adapt to changing network behaviors, such as attacker behaviors, degree of hostility, node disconnection due to physical environment such as terrain, energy exhaustion on a node, or voluntary disconnection for energy savings. We also use social relationships in evaluating the trust metric among group members by employing the concept of *social networks*. Yu *et al*. [44] 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*. [44] used social networks to evaluate the overall trust value of a node. However, we use social networks to evaluate the *social trust* value of a node only in terms of the degree of personal or social trends, rather than the capability of executing a mission based on past collaborative interactions. We assume that a node's capability of completing a highly risky mission will be related to the node's QoS trust value as evaluated by *information networks* based on information sharing.

Developers of MANET trust management schemes should keep the following questions in mind:

- Does the trust metric used reflect the unique properties of trust in MANETs? (e.g., not necessarily perfect transitivity, asymmetry, subjectivity, non-binary value, decaying over time and increasing trust chain, dynamicity, context-dependency)
- What constituents does the trust metric have? Do the constituents change according to tasks given (e.g., high risk upon task failure), changing network environments (e.g., lack of bandwidth, hostile environment as attackers' strength increases, high communication load), or participating nodes' conditions (e.g., low energy, compromised status)?
- How does the trust metric contribute to improving scalability, reconfigurability, and reliability of the proposed network?
- Does the proposed network design achieve adaptability (i.e., learning based on the cognitive functionality of a node) to changing network conditions and environments of MANETs?
- Does the proposed trust metric provide adequate tradeoffs (e.g., altruism versus selfishness, trust level (or security) versus reliability, availability, or survivability, security versus performance)
- Does the proposed network design identify optimal settings under various network and environmental conditions?

5 Discussion

The goal of this paper was to provide MANET network protocol designers with multiple perspectives on the concept of trust, an understanding of the properties that should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the targeted system. By introducing the concept of social and cognitive networks, we suggested future research directions to develop trust management schemes with desirable attributes such as adaptation to environmental dynamics, scalability, reliability, and reconfigurability.

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 faces challenges from the severe resource constraints, the open nature of the wireless medium, the complex dependence between the communications network, the social network, and the application network, and hence the complex dependency of any trust metric to features, parameters, and interactions within and amongst these networks.

References

[1] Abdul-Rahman and S. Hailes, "Using Recommendations for Managing Trust in Distributed Systems," *Proc. IEEE Malaysia Int'l Conf. on Communication (MICC'97)*, Kuala Lumpur, Malaysia, Aug. 1997.

[2] 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 (IAW'05)*, 15-17 June, 2005, West Point, NY, pp. 317-324.

[3] 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.

[4] P. Albers, O. Camp, J.-M. Percher, B. Jouga, L. Mé, and 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 (WIS-2002)*, Apr. 2002, pp. 1-12.

[5] 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.

[6] 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*, Canary Islands, Spain, Jan. 2002, pp. 403-410.

[7] 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(MobiHOC),* Lausanne, CH, 9-11 June 2002, pp. 226-236.

[8] 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.

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

[10] 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.

[11] 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.

[12] Gahlin, "Secure Ad Hoc Networking," Master's Thesis, University of Umeå, March 2004.

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

[14] 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.

[15] 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.

[16] 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.

[17] K. Inkinen, "New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes," *Seminar on Internetworking*, Sjökulla, Finland, Spring 2004.

[18] 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.

[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] 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 (MDC)*, Tokyo, Japan, 23-24 March 2004, pp. 588-593.

[21] Josang and S. LoPresti, "Analyzing the Relationship between Risk and Trust," *Proc. 2nd Int'l Conf. Trust Management (iTrust'04), LNCS*, Springer-Verlag, 2004, pp. 135-145.

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

[23] 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. (VTC'07)*, 22-25 Apr. 2007, pp. 56-60.

[24] J. Liu and V. Issarny, "Enhanced Reputation Mechanism for Mobile Ad Hoc Networks," *Proc. 2nd Int'l Conf. of Trust Management (iTrust 2004)*, Oxford, UK, March 2004.

[25] 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.

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

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

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

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

[30] 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.

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

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

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

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

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

[36] T. Plesse, J. Lecomte, C. Adjih, M. Badel, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, 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.

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

[38] Solhaug, D. Elgesem, and K. Stolen, "Why Trust is not proportional to Risk?" *Proc. 2nd Int'l Conf. on Availability, Reliability, and Security (ARES'07)*, 10-13 April 2007, Vienna, Austria, pp. 11-18.

[39] 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 Journal on Selected Areas in Communications,* vol. 24, no. 2, Feb. 2006, pp. 305-317.

[40] Theodorakopoulos and J. S. Baras, “On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks,” *IEEE Journal on Selected Areas in Communications,* vol. 24, no. 2, Feb. 2006, pp. 318-328.

[41] 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.

[42] Weimerskirch and G. Thonet, “A Distributed Light-Weight Authentication Model for Ad-hoc Networks,” *Proc. 4th Int’l Conf. on Information Security and Cryptology (ICISC 2001),* 6-7 Dec. 2001.

[43] Yang, H. Luo, F. Ye, S. W. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[44] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman, “SybilGuard: Defending Against Sybil Attacks via Social Networks,” *IEEE/ACM Transactions on Networking,* vol. 16, no. 3, June 2008, pp. 576-589.

[45] 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.

[46] 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, pp. 1-10.

[47] 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.

[48] Merriam Webster Dictionary [Online]: http://www.merriam-webster.com/dictionary/trust%5B1%5D.

[49] Wikipedia [Online] http://en.wikipedia.org/wiki/Trust_(sociology)

Appendix A: The Survey on Existing Trust Management in MANETs based on Applicability.

Authors/Year	Methodology	Attacks targeted	Performance metrics	Other characteristics
SECURE ROUTING				
Buchegger *et al*.(2000) [6]	-Direct observation -Reputation	-Various malicious packet forwarding -DoS	No experimental results shown	-Extension of DSR -A hybrid scheme of selective altruism or Utilitarianism
Marti *et al*. (2000)[30]	-Reputation	-Black hole -False accusation	-Throughput -Overhead -Detection accuracy	-Redemption mechanism
Buchegger *et al.* (2002) [7]	-Reputation	-Forward defection (e.g., route diversion)	-Throughput -Goodput -Dropped packets -Overhead -Utility[1]	-Bayesian Model -Incentive mechanism -No punishment against misbehaving nodes
Paul *et al*. (2002) [33]	-Reputation	-Masquerading -Packet modification	No experimental results shown	-Extension of DSR
He *et al.* (2004) [16]	-Reputation	-Packet dropping -Selfish nodes	-Throughput -Overhead	-Incentive mechanism
Buchegger *et al.* (2004) [8]	-Reputation (reputation rating) -Direct observation (trust-rating)	-False information propagation	-mean detection time for misbehaving nodes -False alarm rate (false positives/false negatives)	-Bayesian Model -Redemption -Reputation reevaluation and fading
Ghosh *et al.*(2005) [14]	-Reputation -Direct observation	-Black hole -Gray hole -False accusation -DoS	-Overhead -Routes selected -Route errors	-Incentive mechanism -Trust is not transitive -Use of confidence level as a weight to compute trust value
Zouridaki *et al*. (2005) [46] Zouridaki *et al*. (2006) [47]	-Direct observation [46, 47] -Reputation by second-hand information [47]	-Packet dropping -Packet misrouting -Packet injection Added in [47] -False accusation -collusion of attackers -Replay	-Confidence level over trust value -Trustworthiness -Opinion values about other nodes	-Bayesian Model -Use of confidence level as a weight to compute trust value -Window scheme to flush out stale trust information
Pirzada *et al*. (2006) [35]	-Direct observation	-Packet modification -Black hole -Gray hole	-Packet loss -Packet forwarded -Throughput -Overhead -Latency -Path optimality -Detection probability	-Effort-return-based trust model
Sun *et al*. (2006) [39]	-Direct observation on packet dropping rate -Recommendation	-False recommendation -Newcomer attack -Sybil attack	-Trust level -Packet dropping ratio	-Entropy-based trust model -Probability-based trust model
Li *et al*. (2008) [22]	-Reputation -Direct observation	-Selective misbehaving -Bad mounting -On-off attack	-Ratio of trustworthiness over reputation for both good and bad nodes	-Modified Bayesian model -Use of confidence interval

1 Utility metric refers to the ratio of how many of the transmission of a node are originated or received by the node itself versus how many are just forwarded as an intermediate node on behalf of other nodes [7]. That is, this metric can be represented as A/(A+B) where A is the number of packets transmitted for a node itself and B is the number of packets transmitted for others.

Authors/Year	Methodology	Attacks targeted	Performance metrics	Other characteristics
		-Conflicting behavior		
AUTHENTICATION				
Weimerskirch *et al*. (2001) [42]	-Recommendation -References	-Packet modification -Breach of confidentiality -DoS	No experimental results shown	-Use of trust chains
Pirzada and McDonald (2004) [34]	-Direct observation	-Packet modification -Packet fabrication -Impersonation	No experimental results shown	-Extension of DSR -Extension of Marsh's trust model [29]
Ghosh *et al*. (2005) [14]	-Direct observation -Recommendation	-False certificate	-Rate for successfully detecting false certificates	-Extension of PGP
INTRUSION DETECTION				
Albers *et al*.(2002) [4]	-Direct observation for anomaly detection or misuse detection	-General misbehaving nodes	No experimental results shown	-Local Intrusion Detection System (LIDS)
Ahmed *et al*. (2006) [3]	-Direct observation	-Black hole -Packet dropping -Malicious flooding -Routing loop	-Overhead -False alarm rate	-Leverage IDS to evaluate trust level of other nodes
ACCESS CONTROL				
Luo *et al*. (2004) [28]	-Direct observation	-General misbehaving nodes	-Overhead -Delay and number of retries before ticket is received	-Localized group trust model based on threshold cryptography
Adams and Davis (2005) [2]	-Direct observation -Reputation	-General misbehaving nodes -No specific attacks addressed	No experimental results shown	-Bayesian Model for risk assessment -Trust is not transitive -Trust is a continuous value
Yunfang (2007) [45]	-Direct observation -Reputation -Policy proof	-General misbehaving nodes -No specific attacks addressed	No experimental results shown	-Trust is transitive
OTHERS				
Jiang and Baras (2004) [20]	-Direct observation	-General misbehaving nodes	-Number of hops and delay to obtain the certificate -Success rate obtaining the certificate	-Trust evidence distribution based on a swarm intelligence
Theodorakopoulos and Baras (2006) [40]	-Direct observation -Recommendation	-False accusation -Impersonation	-Confidence level -Opinions about other nodes	-Trust evaluation model based on *Seminrings* theory -Trust is transitive -Trust and confidence value is binary
Boukerche and Ren (2008) [5]	-Direct observation -Reputation	-General misbehaving nodes -No specific attacks addressed	-Query overhead -Security overhead -Percentage of packets -Number of nodes (or malicious nodes)	-Group-based trust model