REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 15-08-2012	**2. REPORT TYPE** Final report	**3. DATES COVERED** *(From - To)* 15 Nov 2009 - 14 August 2012

4. TITLE AND SUBTITLE
On Integrated Social and QoS Trust-Based Routing in Delay Tolerant Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-10-1-0156

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Chen, Ing-Ray (VT)
Bao, Fenye (VT)
Cho, Jin-Hee (ARL)

5d. PROJECT NUMBER
10PR02543-01

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
OFFICE OF SPONSORED PROGRAMS
1880 PRATT DRIVE, SUITE 2006
BLACKSBURG, VA 24060-3325

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
875 North Randolph Street
Arlington, VA 22203-1995

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSORING/MONITORING AGENCY REPORT NUMBER

12. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
We propose to combine the notion of social trust derived from social networks with that of quality-of-service (QoS) trust derived from communication networks to obtain a composite trust metric as a basis for evaluating trust of mobile nodes in mobile ad hoc network (MANET) environments. We develop a novel model-based approach to identify the best protocol setting under which peer-to-peer subjective trust as a result of executing our distributed trust management protocol is accurate with respect to ground truth status over a wide range of operational and environment conditions with high resiliency to malicious attacks and misbehaving nodes. Furthermore, using mission-oriented mobile groups as an application, we identify the best trust formation model under which the application performance in terms of the system reliability of mission-oriented mobile groups in MANET environments is maximized.

15. SUBJECT TERMS
trust management, mobile ad hoc networks, social networks, model-based evaluation, hierarchical modeling, Stochastic Petri Nets, reliability.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT** SAR	**18. NUMBER OF PAGES** 16	**19a. NAME OF RESPONSIBLE PERSON** Chen, Ing-Ray
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U			**19b. TELEPONE NUMBER** ***(Include area code)*** (703) 538-8376

SQTrust: Social and QoS Trust Management and Its Application to Mission-Oriented Mobile Groups

Ing-Ray Chen, Fenye Bao, and Jin-Hee Cho

20120816033

Abstract—We propose to combine the notion of *social trust* derived from social networks with that of *quality-of-service* (QoS) trust derived from communication networks to obtain a *composite* trust metric as a basis for evaluating trust of mobile nodes in mobile ad hoc network (MANET) environments. We develop a novel model-based approach to identify the best protocol setting under which peer-to-peer *subjective trust* as a result of executing our distributed trust management protocol is accurate with respect to ground truth status over a wide range of operational and environment conditions with high resiliency to malicious attacks and misbehaving nodes. Furthermore, using mission-oriented mobile groups as an application, we identify the best trust formation model under which the application performance in terms of the system reliability of mission-oriented mobile groups in MANET environments is maximized.

Index Terms— trust management, mobile ad hoc networks, social networks, model-based evaluation, hierarchical modeling, Stochastic Petri Nets, reliability.

1 Introduction

The concept of "trust" originally derives from the social sciences and is defined as the subjective degree of a belief about the behaviors of a particular entity [12]. Blaze et al. [7] 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 mobile ad hoc networks (MANETs) is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among them, for example, for coalition operation without predefined trust. Thus, the concept of trust is attractive to communication and network protocol designers where trust relationships among participating nodes are critical to building collaborative environments to achieve system optimization. Many researchers in the networking and communication field have defined trust differently such as "a set of relations in protocol running" [14], "a belief on reliability, dependability, or security" [24], "a belief about competence or honesty in a specific context" [3], and "reliability, timeliness, and integrity of message delivery" [25].

Trust management is often used with different purposes in diverse decision making situations such as secure routing [5], [16], [31], [34], [37], key management [9], [18], authentication [29], access control [1], and intrusion detection [2]. Further, general trust or reputation evaluation schemes have also been proposed with a variety of approaches such as semirings [35], graph/random theory [6], Markov chain [9], etc. Trust management has also received much research attention in peer-to-peer (P2P) networks (e.g., EigenTrust [23], PeerTrust [38]) for applications like file sharing, electronic commerce, etc. These protocols for P2P networks consider both direct observation and indirect recommendation in trust evaluation, which is similar to ours. However, these protocols obtain recommendations either from just acquaintance peers or from all peers. This hinders their applicability to MANETs because of rapidly changing topology and connectivity in MANET environments. In contrast, our protocol considers 1-hop neighbors as trust recommenders and identifies the best way of combining direct observation and indirect recommendation to achieve high accuracy. Moreover, our protocol does not require pre-trust information or the existence of a centralized trusted authority. The process of propagating and aggregating trust is essentially an information diffusion process [19]. Traditional information

- *Ing-Ray Chen and Fenye Bao are with the Department of Computer Science, Virginia Tech, 7054 Haycock Rd., Falls Church, VA 22043. E-mail: {irchen, baofenye}@vt.edu.*
- *Jin-Hee Cho is with Computational and Information Sciences Directorate, U.S. Army Research Laboratory, 2800 Powder Mill Rd. Adelphi, MD 20783. E-mail: jinhee.cho@us.army.mil.*

diffusion models assume that trust already exists to affect information diffusion, and do not consider false recommendation attacks performed by malicious entities. In this paper, we use the concept of information diffusion to build trust despite the presence of malicious nodes performing false recommendation attacks to break the trust system.

[10] provides a survey on trust management in MANETs. A mobile ad hoc group in MANET environments very frequently comprises human operators carrying communication devices. Thus, in addition to traditional *quality of service (QoS) trust* metrics including competence, cooperativeness, reliability, and task satisfaction, one must also consider *social trust* metrics including friendship, honesty, privacy, similarity, betweenness centrality and social ties [13] for trust management. Golbeck [17] suggested the use of social networks as a bridge to build trust relationships among entities. Yu *et al.* [39] used social networks to evaluate trust values in the presence of Sybil attacks. Standard QoS performance metrics such as control packet overhead, throughput, goodput, packet dropping rate and delay have been used to evaluate trust [16], [31], [37]. Dependability QoS metrics such as availability [18], convergence time to reach a steady state in trustworthiness for all participating nodes [6], percentage of malicious nodes [8], and fault tolerance based on reputation [26], [27] also have been employed. The use of a "trust level" to associate with a node has received attention recently, considering general attributes such as confidence [40], trust level [34], trustworthiness [26], and opinion [35].

Unlike prior work, we suggest using both social and QoS trust metrics to assess the trust level of a node in a mobile group consisting of entities exhibiting both social and performance and dependability behaviors. We note that prior works such as [13], [17], [41] also considered social trust metrics in communication networks. The contribution of our work relative to these prior works is that we not only identify the best way for each trust metric selected (either QoS or social) to take in direct experiences and recommendations information so that the assessment of the trust property is the most accurate against actual status, but also consider the trust formation issue of forming the overall trust out of individual social and QoS trust metrics to maximize application performance.

This paper has the following contributions: First, we develop a new trust management protocol (SQTrust) based on a composite social and QoS trust metric, with the goal to yield peer-to-peer *subjective trust evaluation*. Second, we propose a model-based evaluation technique for validating SQTrust based on the concept of *objective trust evaluation* which utilizes knowledge regarding the operational and environment conditions to yield idealistic trust values against which subjective trust values obtained from SQTrust are compared for validation. Our analysis methodology hinges on the use of a Stochastic Petri Net (SPN) mathematical model [36] for describing the "actual" dynamic behaviors of nodes in MANETs in the presence of well-behaved, uncooperative and malicious nodes. With this methodology, we demonstrate that SQTrust is capable of providing accurate trust assessment compared with global knowledge and actual node status. Finally, we apply SQTrust to a mission-oriented mobile group application considering the intrinsic relationship between trust and reliability for critical mission execution by a mobile group and identify the best trust protocol setting to maximize application performance.

We notice that in subjective logic [20], the term "subjective" represents the subjective perception about the world and individual opinions about the truth of propositions. We use the term "subjective" with a similar intention. However, in subjective logic, trust consists of three components (belief, disbelief, and uncertainty) while it is a single real value in our trust protocol. Subjective trust in this paper represents trust obtained by each node as a result of executing our proposed trust protocol. The term "subjective" is used to refer to the fact that a trustor node's trust towards a trustee node is subjective based on local knowledge (including both direct observations and indirection recommendations). Objective trust represents ground truth status of a trustee node derivable from the output of the SPN model which faithfully describes actual status of nodes in the system.

The rest of the paper is organized as follows. Section 2 describes the system model and assumptions. Section 3 explains SQTrust executed by each node to perform peer-to-peer subjective trust evaluation. Section 4 develops a performance model to describe dynamic behaviors of nodes in MANETs in the presence of misbehaving nodes with the objective to validate subjective trust evaluation with objective trust evaluation. Section 5 presents quantitative results obtained with physical interpretations given. Section 5 also examines the effect of trust management on the reliability of mission-oriented mobile groups with an application scenario involving a commander node dynamically selecting a number of nodes it trusts most for mission execution to demonstrate the applicability of SQTrust. Section 6 presents simulation results for simulation validation. Finally, Section 7 summarizes the paper and outlines future research areas.

2 System Model

A. Operational Profile

We follow the notion of "*operational profiles*" in software reliability engineering [28] as input to specify the anticipated operational and environment conditions. Specifically, a system's *operational profile* provides knowledge regarding (a) environment hostility, i.e., how often nodes are compromised; (b) node mobility, i.e., how often nodes meet and how they interact with each other; (c) node behavior, i.e., how nodes will behave based on node status including good behaviors by good nodes and bad behaviors by bad nodes; (d) environment resources, i.e., the initial energy each node has and how fast energy is consumed by good or bad nodes; and (e) system failure definitions including both operational and security failure conditions. Later in Section 5, we will exemplify the input operational profile for a mobile group application in MANET environments. An operating profile does not represent a controlled setting. For example, hostility and node behavior as part of the operational profile merely specify per-node compromise rate and energy consumption/cooperativeness behavior but do not tell us which nodes are compromised and/or uncooperative over time. In response to operational or environment changes (e.g., change of hostility), the system using the results obtained in the paper can adaptively adjust trust settings to optimize application performance.

B. Problem Definition and Desirable Output

SQTrust is distributed in nature and is run by each mobile node to subjectively yet informatively assess the trust levels of other mobile nodes. Further, SQTrust is resilient against misbehaving nodes. Given the operational profile as input covering a wide range of operational and environment conditions, we aim to solve two problems:

- Discover and apply the best trust aggregation protocol setting of SQTrust to make "subjective trust" accurate compared with "objective trust" despite the presence of misbehaving nodes. The desirable output is to achieve high accuracy in peer-to-peer subjective trust evaluation with high resiliency to malicious attacks.
- Discover and apply the best trust formation to maximize application performance. For the mission-oriented mobile group application, the desirable output is to maximize the system reliability given a system failure definition.

C. Node Behavior

Node behavior is part of the operational profile. While our model-based analysis technique is generally applicable to any node behavior specification, for illustration we consider the following node behavior specification in this paper:

- Every node shall conserve its resources (e.g., energy) as long as it does not jeopardize the global welfare (i.e., successful mission execution). Thus, when a node senses that it is surrounded by many uncooperative 1-hop neighbors, it will tend to become cooperative to ensure successful mission execution. On the other hand, a node with many cooperative 1-hop neighbors around will tend to become uncooperative to conserve its resources, knowing that this will not jeopardize the global welfare.
- Every node has a different level of energy, speed and vulnerability reflecting node heterogeneity. The energy consumption rate of a node depends on its status. If a node is uncooperative, the speed of energy consumption is slowed down since an uncooperative node will not follow protocol execution. If a node becomes compromised, the speed of energy consumption increases since a compromised node will perform attacks which consume energy. A node's vulnerability is reflected by a compromised rate, e.g., a capture by attackers after which the node is compromised.
- A compromised node may perform slandering attacks, (e.g., good-mouthing bad nodes and bad-mouthing good nodes), identity attacks (e.g., Sybil) or Denial-of-Service (DoS) attacks (e.g., consuming resources unnecessarily by disseminating bogus packets). We assume that a compromised node will always perform attacks on good nodes and does not discriminate good nodes when performing attacks.

D. Mission-Oriented Mobile Groups

As an application of SQTrust, we apply it to mission-oriented mobile groups. A mission-oriented mobile group consists of a number of mobile nodes cooperating to complete a mission, with one or more being the commander nodes of the group. Upon a membership change due to join or leave, rekeying can be performed based on a distributed key agreement protocol such as the Group Diffie-Hellman (GDH) protocol [33]. For mission-critical applications, it is frequently required that nodes on a mission must have a minimum degree of trust for the mission to have a reasonable chance of success. On one hand, a mission may require a sufficient number of nodes to collaborate. On the other hand, the trust relationship may fade away between nodes both temporarily and spatially. SQTrust equips each node with the ability to subjectively assess the trust levels of other nodes and select highly trustworthy nodes for collaboration to maximize the probability of successful mission execution.

3 Design of SQTrust

In this section, we first describe our SQTrust protocol to be executed by every node at runtime. Then we discuss its application to reliability assessment of a mission-oriented mobile group in MANET environments.

A. Trust Composition

A node with a very low trust value is of little value to the system and depending on the application requirement may be evicted to prevent it from performing attacks to damage the system functionality. A node's trust value is assessed based on evidences such as direct observations as well as indirect recommendations. Our trust model is evidence-based. Thus we do not consider dispositional belief or cognitive characteristics of an entity in deriving trust. The trust assessment of one node toward another node is updated periodically.

Our trust metric consists of two trust types: *social trust* and *QoS trust*. Social trust is evaluated through interaction experiences in social networks to account for social relationships. Note that this work concerns mobile devices carried by human users as part of a social network. Among the many social trust metrics such as friendship, honesty, privacy, similarity, betweenness centrality, and social ties [13], we select social ties (measured by ***intimacy***) and honesty (measured by ***healthiness***) to measure the social trust level of a node as these social properties are considered critical for trustworthy mission execution in group settings. *QoS trust* is evaluated through the communication and information networks by the *capability* of a node to complete a mission assigned. Among the many QoS metrics such as competence, cooperation, reliability, and task performance, we select competence (measured by ***energy***) and protocol compliance (measured by ***cooperativeness*** in protocol execution) to measure the QoS trust level of a node since competence and cooperation are considered the most critical QoS trust properties for mission execution in group settings. Quantitatively, let a node's trust level toward another node be a real number in the range of [0, 1], with 1 indicating complete trust, 0.5 ignorance, and 0 complete distrust. Let a node's trust level toward another node's particular trust component also be in the range of [0, 1] with the same physical meaning.

The rationale of selecting these social and QoS trust metrics is given as follows. The intimacy component (for measuring social ties) has a lot to do with if two nodes have a lot of direct or indirect interaction experiences with each other, for example, for packet routing and forwarding. The healthiness component (for measuring honesty) is essentially a belief of whether a node is malicious or not. We relate it to the probability that a node is not compromised. The energy component refers to the residual energy of a node, and for a MANET environment, energy is directly related to the survivability capability of a node to be able to execute a task completely, particularly when the current and future missions may require a long mission execution time. Finally, the cooperativeness component of a node is related to whether the node is cooperative in routing and forwarding packets. For mobile groups, we relate it to the trust to a node being able to faithfully follow the prescribed protocol such as relaying and responding to group communication packets.

Other than the healthiness trust component, we assert that a node can have fairly accurate trust assessments toward its 1-hop neighbors utilizing monitoring, overhearing and snooping techniques. For example, a node can monitor interaction experiences with a target node within radio range, and can overhear the transmission power and packet forwarding activities performed by the target node over a trust evaluation window Δt to assess the target node's energy and cooperativeness status. For a target node more than 1-hop away, a node will refer to a set of recommenders for its trust toward the remote target node.

B. Design against Slandering Attacks

SQtrust is resilient to good-mouthing and bad-mouthing attacks by two recommender selection criteria: (a) *threshold-based filtering* by which only trustworthy recommenders with trust higher than a minimum trust threshold are qualified as recommenders; and (b) *relevance-based trust* by which only recommenders with high trust in trust component *X* are qualified as recommenders to provide recommendations about a trustee's trust component *X*.

C. SQTrust Protocol Description

The trust value of node *j* as evaluated by node *i* at time *t*, denoted as $T_{i,j}(t)$, is in the range of [0, 1] and is computed by node *i* as a weighted average of intimacy, healthiness, energy, and cooperativeness trust components. The assessment is done periodically in every Δt interval. Specifically node *i* will compute $T_{i,j}(t)$ by:

$$T_{i,j}(t) = \sum_{X} w^X \times T_{i,j}^X(t) \qquad (1)$$

where $T_{i,j}^X(t)$ is the trust belief of node *i* toward node *j* in trust component *X*=intimacy, healthiness, energy or cooperativeness and w^X is the weight associated with *X*. Below we use the notation $w_1 \colon w_2 \colon w_3 \colon w_4$ for $w^{intimacy} \colon w^{healthiness} \colon w^{energy} \colon w^{cooperativeness}$ for notational convenience.

Node *i* evaluates node *j* at time *t* by direct observations and indirect recommendations. Direct observations are direct evidences collected by node *i* toward node *j* over the time interval $[t - d\Delta t, t]$ when node *i* and node *j* are 1-hop neighbors at time *t*. Here Δt is the trust update interval and *d* is a design parameter specifying the extent to which recent interaction experiences would contribute to intimacy. We can go back as far as *t*=0, that is, d=$t/\Delta t$, if all interaction experiences are considered equally important. Indirect recommendations, on the other hand, are indirect evidences given to node i by a subset of 1-hop neighbors selected based on *threshold-based filtering* and *relevance-based trust* selection criteria. Specifically, node i will compute $T^{X}_{i,j}(t)$ where X is a trust component in Equation 1 by:

$$T^{X}_{i,j}(t) = \beta_1\, T^{direct,\ X}_{i,j}(t) + \beta_2\, T^{indirect,\ X}_{i,j}(t) \qquad (2)$$

In Equation 2, β_1 is a parameter to weigh node i's own information toward node j at time t, i.e., "direct observations" or "self-information" and β_2 is a parameter to weigh indirect information from recommenders, i.e., "information from others," with $\beta_1 + \beta_2 = 1$. When $\beta_1 > \beta_2$ it reflects a node's higher confidence on its own direct observations than indirect information obtained from third parties.

The direct trust part, $T^{direct,\ X}_{i,j}(t)$, in Equation 2 is evaluated by node i at time t depending on if node i is a 1-hop neighbor of node j at time t. If yes, node i uses its direct observations toward node j during $[t - d\Delta t, t]$ to update $T^{direct,\ X}_{i,j}(t)$ where Δt is the periodic trust evaluation interval. Otherwise, it uses its old direct trust assessment at time $t - \Delta t$ multiplied by $e^{-\lambda_d \Delta t}$ (for exponential trust decay over time) to update $T^{direct,\ X}_{i,j}(t)$. Specifically, node i will compute $T^{direct,\ X}_{i,j}(t)$ by:

$$T^{direct,\ X}_{i,j}(t) = \begin{cases} T^{1-hop,\ X}_{i,j}(t) & \text{if } i \text{ is a neighbor to } j \text{ at } t \\ e^{-\lambda_d \Delta t} \times T^{direct,X}_{i,j}(t - \Delta t) & \text{otherwise} \end{cases} \qquad (3)$$

To account for trust decay over time, we adopt an exponential time decay factor, $e^{-\lambda_d \Delta t}$, to satisfy the desirable property that trust decay must be invariable to the trust update frequency [21]. Depending on the trust evaluation interval Δt, we can fine tune the value of λ_d to test the effect of trust decay over time. The notation $T^{1-hop,\ X}_{i,j}(t)$ here refers to the new "direct" trust assessment at time t. Below we describe specific detection mechanisms by which node i collects direct observations to assess $T^{1-hop,\ X}_{i,j}(t)$ for the case in which i and j are 1-hop neighbors at time t.

- $T^{1-hop,\ intimacy}_{i,j}(t)$: This refers to the new assessment of node i's direct interaction experience toward node j. It is computed by node i by the ratio of the amount of time nodes i and j are 1-hop neighbors directly interacting with each other during $[t - d\Delta t, t]$.
- $T^{1-hop,\ healthiness}_{i,j}(t)$: This refers to the belief of node i that node j is healthy based on node i's direct observations during $[t - d\Delta t, t]$. Node i estimates $T^{1-hop,\ healthiness}_{i,j}(t)$ by the ratio of the number of suspicious interaction experiences observed during $[t - d\Delta t, t]$ to a system "healthiness" threshold to reduce false positives. Node i uses a set of anomaly detection rules including the interval rule (for detecting node j's sending bogus messages), the retransmission rule (for detecting node j's dropping messages), the integrity rule (for detecting node j's modifying messages), the repetition/jamming rule (for detecting node j's performing DOS attacks), and the delay rule (for detecting node j's delaying message transmission) as in [32] to keep a count of suspicious experiences of node j during $[t - d\Delta t, t]$. If the count exceeds the "healthiness" threshold, node i considers node j as totally unhealthy, i.e., $T^{1-hop,\ healthiness}_{i,j}(t)$=0. Otherwise it is equal to 1 minus the ratio. We model the deficiencies in anomaly detection (e.g., imperfection of rules) by a false negative probability (P^{H}_{fn}) of misidentifying an unhealthy node as a healthy node, and a false positive probability (P^{H}_{fp}) of misidentifying a healthy node as an unhealthy node.
- $T^{1-hop,\ energy}_{i,j}(t)$: This refers to the belief of node i that node j's energy is adequate and hence is competent providing proper services at time t. Node i overhears node j's packet transmission activities during $[t - d\Delta t, t]$ utilizing an energy consumption model [15] to first compute the amount of energy consumed by node j during $[t - d\Delta t, t]$ and then deduce the residual energy left in node j at time t by extrapolation.
- $T^{1-hop,\ cooperativeness}_{i,j}(t)$: This provides the belief of node i that node j is protocol compliant based on direct observations during $[t - d\Delta t, t]$. Node i estimates $T^{1-hop,\ cooperativeness}_{ij}(t)$ by the ratio of the number of cooperative interaction experiences to the total number of protocol interaction experiences. Note that both counts are related to protocol execution except that the former count is for positive experiences when node j, as observed by node i, cooperatively follows the prescribed protocol execution.

The indirect trust part, $T^{indirect,\ X}_{i,j}(t)$ in Equation 2 is evaluated by node i at time t by taking in recommendations from a subset of 1-hop neighbors selected following the threshold-based filtering and relevance-based trust selection criteria. Specifically, node i will compute $T^{indirect,\ X}_{i,j}(t)$ by:

$$T^{indirect,\ X}_{i,j}(t) = \begin{cases} \dfrac{\sum_{m \epsilon V}\left(T^{X}_{i,m}(t) \times T^{X}_{m,j}(t)\right)}{n_r} & \text{if } n_r > 0 \\ e^{-\lambda_d \Delta t} \times T^{indirect,X}_{i,j}(t - \Delta t) & \text{if } n_r = 0 \end{cases} \qquad (4)$$

In Equation 4, m is a recommender and V is a set of

n_r recommenders chosen by node i from its 1-hop neighbors which satisfy the *threshold-based filtering* and *relevance-based trust* selection criteria. That is, these are the recommenders for which node i's $T^X_{i,m}(t)$ in trust component X is higher than a minimum threshold denoted by T^X_t. Here we note that when a recommender node, say, node m, provides its recommendation to node i for evaluating node j in trust component X, node i's trust in node m is also taken into consideration in the calculation as reflected in the product term on the right hand side of Equation 4. This accounts for trust decay over space. If n_r=0 then $T^{indirect,\ X}_{i,j}(t) = e^{-\lambda_d \Delta t} \times T^{indirect,\ X}_{i,j}(t - \Delta t)$ to account for trust decay over time.

Lastly, depending on the mobile application, nodes in a mobile group may join or leave the mobile group. For a non-member, say, node j, the trust level $T_{i,j}(t)$ is the same as its trust level at the last trust evaluation instant $t - \Delta t$ discounted by time decay, that is, $T_{i,j}(t) = e^{-\lambda_d \Delta t} \times T_{i,j}(t - \Delta t)$.

An interesting metric is the average "subjective" trust of node j in trust component X at time t, $T^{sub,X}_j(t)$, as evaluated by all active member nodes in the system. It can be calculated by a weighted average of trust component X from all active member nodes except node j, i.e.,

$$T^{sub,X}_j(t) = \frac{\sum_{all\ i \neq j}(T^X_{i,j}(t)\ )}{\sum_{all\ i \neq j} 1} \tag{5}$$

Another interesting metric is the overall average "subjective" trust level of node j, denoted by $T^{sub}_j(t)$, as evaluated by all active nodes. Once we obtain $T_{i,j}(t)$ from Equation 1, $T^{sub}_j(t)$ can be computed by:

$$T^{sub}_j(t) = \frac{\sum_{all\ i \neq j} T_{i,j}(t)}{\sum_{all\ i \neq j} 1} \tag{6}$$

In this paper, we compare $T^{sub}_j(t)$ with the "objective" trust of node j, denoted by $T^{obj}_j(t)$, calculated based on actual, global information to see how much deviation subjective trust evaluation is from objective trust evaluation. Specifically, let $T^{obj,X}_j(t)$ denote the "objective" trust of node j in trust component X at time t, which we can obtain by a mathematical model (see Section 4 below). Then, following Equation 1, $T^{obj}_j(t)$ is calculated by:

$$T^{obj}_j(t) = \sum_X w^X \times T^{obj,X}_j(t) \tag{7}$$

By means of a novel mathematical model (discussed later in Section 4) describing node behaviors in a MANET, we can calculate the objective trust levels of all nodes in the system based on actual status of nodes. This serves as the basis for validating SQTrust.

D. Mission-Oriented Mobile Group Applications

We consider mission-oriented mobile groups as an application of SQTrust. In military battlefield situations, very frequently a commander (a special node in a MANET) will need to assemble and dynamically manage a mobile task group to achieve a critical mission assigned despite failure, disconnection or compromise of member nodes. A commander node, say node i, can use $T_{i,j}(t)$ based on its own local view towards node j as an indicator to judge if node j satisfies the mission-specific trust requirements for successful mission execution. More importantly, the commander node could obtain the mission success probability (as a reliability metric) when given knowledge regarding the mission failure definition, member failure definition and mission time.

Let $R(t)$ be the mission reliability given that the mission time is t. Then, the mission success probability, denoted by $P_{mission}$, is simply $R(TR)$ when the commander is given TR as the mission time, i.e.,

$$P_{mission} = R(TR) \tag{8}$$

The mission failure definition is application dependent. Assume that the commander node is fault-free because of high integrity and high security protection. Also assume that the mission fails if at least *n-k+1* out of n members (trustees) fail. Let $R_j(t)$ be member j's reliability at time t. Then,

$$R(t) = \sum_{|J|>k} \left(\prod_{j \in J} R_j(t) \prod_{j \notin J} (1 - R_j(t)) \right) \tag{9}$$

The member failure definition, on the other hand, hinges on trustworthiness of each individual member. Suppose there are two trust thresholds: M_1 is a trust threshold above which a member is considered completely trustworthy for successful mission completion and M_2 is a drop dead trust level below which a member is completely not trustworthy. Below we give a possible definition of member failure based on dual trust thresholds, M_1 and M_2, defined above. Specifically, if at any time t, node j's trust level is above M_1 then node j is completely trustworthy, so its *instantaneous trustworthiness*, denoted by $X_j(t)$, is 1. If node j's trust level is below M_2 then node j is completely untrustworthy, so $X_j(t)$ is 0. If node j's trust level is in between M_1 and M_2 then node j's instantaneous trustworthiness is calculated as the ratio of its trust level to M_1. The commander node, node i, computes member j's reliability $R_j(t)$ based on node j's instantaneous trustworthiness over [*0*, *t*]. If at any time $t' \leq t$, $X_j(t') = 0$, then the trust level of node j is not acceptable, so $R_j(t)$ is 0; otherwise, $R_j(t)$ is the average trustworthiness of node j over [*0*, *t*]. Summarizing above, node i computes member j's reliability $R_j(t)$ by:

$$R_j(t) = \begin{cases} 0, if\ X_j(t') = 0 \text{ for any } t' \leq t \\ E[X_j(t')], t' \leq t, \quad \text{otherwise} \end{cases}$$

$$\text{with } X_j(t') = \begin{cases} 1, \quad if\ T_{i,j}(t') \geq M_1 \\ 0, \quad if\ T_{i,j}(t') < M_2 \\ T_{i,j}(t')/M_1, \quad \text{otherwise} \end{cases} \qquad (10)$$

Here $X_j(t')$ is the instantaneous trustworthiness of node j at time t' and $E[X_j(t')]$ is the expected value of $X_j(t')$, $0 \leq t' \leq t$, over $[0, t]$. One can see that the knowledge of $T_{i,j}(t)$ is very desirable for the command node to compute $P_{mission}$ given knowledge regarding the mission execution time, member failure definition, and mission failure definition.

4 Performance Model

Our analysis methodology is model-based and hinges on the use of a SPN mathematical model to probabilistically estimate node status over time, given an anticipated operational profile as input. The SPN outputs provide ground truth node status and can serve as the basis for "objective" trust evaluation. Our goal is to compare "subjective" trust obtained through protocol execution with "objective" trust obtained through the SPN outputs to provide a sound theoretical basis for validating the algorithm design for SQTrust.

A. *Node SPN for Modeling Node Behavior*

Figure 1 shows the "node" SPN model developed for describing the lifetime behavior of a mobile node in the presence of other uncooperative and malicious nodes in a mobile group following the input operational profile. The system SPN model consists of *N* node SPN models where *N* is the number of nodes in the system. We utilize the node SPN model to obtain a single node's information (e.g., intimacy, healthiness, energy, and cooperativeness) and to derive its trust relationships with other nodes in the system. It also captures location information of a node as a function of time. We consider a square-shaped operational area consisting of *M*×*M* regions each with the width and height equal to radio radius *R*. The node mobility model is specified as part of the operational profile.

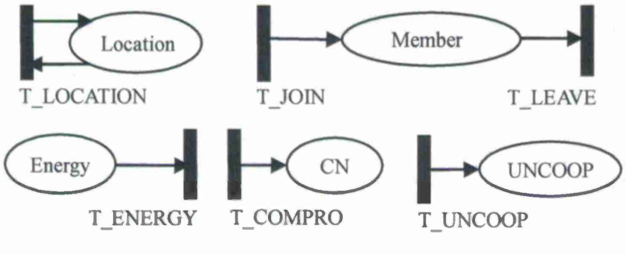


Figure 1: Node SPN Model.

The reason of using node SPN models is to yield a probability model (a semi-Markov chain [30], [36]) to model the stochastic behavior of nodes in the system, given the system's anticipated operational profile as input. The theoretical analysis yields *objective trust* based on ground truth of node status, against which *subjective trust* as a result of executing our proposed trust protocol is compared. This provides the theoretical foundation that subjective trust (from protocol execution) is accurate compared with ground truth. The underlying semi-Markov chain [30], [36] has a state representation comprising "places" in the SPN model. A node's status is indicated by a 5-component state representation (*Location*, *Member*, *Energy*, *CN*, *UNCOOP*) with "*Location*" (an integer) indicating the current region the node resides, "*Member*" (a boolean variable) indicating if the node is a member, "*Energy*" (an integer) indicating the current energy level, "*CN*" (a boolean variable) indicating if the node is compromised, and "UNCOOP" (a boolean variable) indicating if the node is cooperative. For example, place *Location* is a state component whose value is indicated by the number of "tokens" in place *Location*. A state transition happens in the semi-Markov chain when a move event occurs with the event occurrence time interval following a probabilistic time distribution such as exponential, Weibull, Pareto, and hyper-exponential distributions. This is modeled by a "transition" with the corresponding firing time in the SPN model. For example, when the node moves across a regional boundary after its residence time in the previous region elapses, transition T_LOCATION will be triggered, thus resulting in a location change. This is reflected by flushing all the tokens in place *Location* and replacing by a number of tokens corresponding to the id of the new region it moves into. After the move, the value of "*Location*" will be the id of the new region it moves into. Thus the three primary entities, i.e., places, tokens, and transitions, allow the node SPN model to be constructed to describe a node's lifetime behavior dynamically as time evolves. Below we explain how we construct the node SPN model.

Location: Transition T_LOCATION is triggered when the node moves to another region from its current location with the rate calculated as S_{init}/R (i.e., the node's mobility rate) based on an initial speed (S_{init}) and wireless radio range (*R*). Depending on the location a node moves into, the number of tokens in place *Location* is adjusted. Initially for simplicity nodes are randomly distributed over the operational area based on uniform distribution. Suppose that nodes move randomly. Then a node randomly moves to one of four locations in four directions (i.e., north, west, south, and east) in accordance with its mobility rate. To avoid end-effects, movement is wrapped around (i.e., a torus is assumed). The underlying semi-Markov model of the node SPN model when solved utilizing solution techniques such as SOR, Gauss

Seidel, or Uniformization [36] gives the probability that a node is at a particular location at time *t*, e.g., the probability that node *i* is located in region *j* at time *t*. This information along with the location information of other nodes at time *t* provides global information if two nodes are 1-hop neighbors at time *t*.

Intimacy: Intimacy trust is an aggregation of *direct* interaction experience ($T_{i,j}^{direct,\ intimacy}(t)$) and *indirect* interaction experience ($T_{i,j}^{indirect,\ intimacy}(t)$). Out of these two, only new *direct* interaction experience ($T_{i,j}^{direct,\ intimacy}(t)$ via $T_{i,j}^{1\text{-}hop,\ intimacy}(t)$) is calculated based on if two nodes are 1-hop neighbors interacting with each other via packet forwarding and routing. Since the node SPN model gives us the probability that a node is in a particular location at time *t*, we can objectively compute direct interaction experience $T_{i,j}^{1-hop,\ intimacy}(t)$ (see Equation 3) based on the probability of nodes *i* and *j* are in the same location at time *t* from the output of the two SPN models associated with nodes *i* and *j*.

Energy: Place *Energy* represents the current energy level of a node. An initial energy level of each node is assigned differently to reflect node heterogeneity. We randomly generate a number between 12 to 24 hours based on uniform distribution, representing a node's initial energy level E_{init}. Then we put a number of tokens in place *Energy* corresponding to this initial energy level. A token is taken out when transition T_ENERGY fires. The transition rate of T_ENERGY is adjusted on the fly based on a node's state: it is lower when a node becomes uncooperative to save energy and is higher when the node becomes compromised so that it performs attacks more and consumes energy more. Therefore, depending on the node's status, its energy consumption is dynamically changed.

Healthiness: A node is compromised when transition T_COMPRO fires. The rate to transition T_COMPRO is λ_{com} as the node compromising rate (or the capture rate) reflecting the hostility of the application. If the node is compromised, a token goes to *CN*, meaning that the node is already compromised and may perform good-mouthing and bad-mouthing attacks as a recommender by good-mouthing a bad node with a high trust recommendation and bad-mouthing a good node with a low trust recommendation.

Cooperativeness: Place *UNCOOP* represents whether a node is cooperative or not. If a node becomes uncooperative, a token goes to *UNCOOP* by triggering T_UNCOOP. We model a node's uncooperativeness behavior following the 'node behavior' model discussed in Section 2. Specifically, the rate to transition T_UNCOOP is modeled as a function of its remaining energy, the mission difficulty, and the neighborhood uncooperativeness degree as follows:

$$rate(T\_UNCOOP) = \frac{f_e(E_{remain}) f_m(M_{difficulty}) f_s(S_{degree})}{T_{gc}} \qquad (11)$$

where E_{remain} represents the node's current energy level as given in *mark(Energy)*, $M_{difficulty}$ is the difficulty level of the given mission, S_{degree} is the degree of uncooperativeness computed based on the ratio of uncooperative nodes to cooperative nodes among 1-hop neighbors and T_{gc} is the group communication interval over which a node may decide to become uncooperative in protocol execution and drop packets. The form $f(x) = \alpha x^{-\varepsilon}$ follows the demand-pricing relationship in Economics [4] to model the effect of its argument *x* on the uncooperative behavior, including:

- $f_e(E_{remain})$: If a node has a lower level of energy, it is less likely to be cooperative. This is to consider a node's individual utility in resource-constrained environments.
- $f_m(M_{difficulty})$: If a node is assigned to a more difficult mission, it is more likely to be cooperative to ensure successful mission execution.
- $f_s(S_{degree})$: If a node's 1-hop neighbors are not very cooperative, the node is more likely to be cooperative to complete a given mission successfully.

A compromised node is necessarily uncooperative as it won't follow the protocol execution rules. So if place CN contains a token, place UNCOOP will also contain a token.

B. *Objective Trust Evaluation*

With the node behaviors modeled by a probability model (a semi-Markov chain) described above, the objective trust evaluation of node *j* in trust component *X*, i.e., $T_j^{obj,X}(t)$, can be obtained based on exact global knowledge about node *j* as modeled by its node SPN model that has met the convergence condition with the location information supplied. To calculate each of these objective trust probabilities of node *j*, one would assign a reward of r_s with state *s* of the underlying semi-Markov chain of the SPN model to obtain the probability weighed average reward as:

$$T_j^{obj,X}(t) = \textstyle\sum_{s\epsilon S}(r_s * P_s(t)) \qquad (12)$$

for *X* = healthiness, energy or cooperativeness, and as:

$$T_j^{obj,X}(t) = \frac{\int_{t-d\Delta t}^{t} \sum_{s\epsilon S}(r_s * P_s(t\prime))dt\prime}{d\Delta t} \qquad (13)$$

for *X* = intimacy. Here *S* indicates the set of states in the underlying semi-Markov chain of our SPN model, r_s is the reward to be assigned to state *s*, and $P_s(t)$ is the probability that the system is in state *s* at time *t*, which can be obtained by solving the underlying semi-Markov model of our SPN model utilizing solution techniques such as SOR, Gauss Seidel, or Uniformization [36]. Table 1 summarizes specific reward assignments used to calculate $T_j^{obj,X}(t)$ for

X=intimacy, healthiness, energy, or cooperativeness. In Table 1, E_T is the energy threshold below which the energy trust toward a node goes to 0. Once $T_j^{obj,X}(t)$ is obtained, we compute the average objective trust value of node j, $T_j^{obj}(t)$, based on Equation 7.

Here we note that in Table 1 we assign a binary trust value of 0 or 1 to a state in which it is clear in this particular state the trust value is either 0 or 1. Since the system evolves over time and there is a probability that it may stay at any state at time t with all state probabilities sum to 1, the expected value of a trust property (intimacy, healthiness, energy or cooperativeness) at time t based on a state-probability-weighted trust calculation is a real number between 0 and 1.

C. *Subjective Trust Evaluation*

Unlike objective trust evaluation, subjective trust evaluation is based on Equations 1-4 following the trust protocol execution. In particular, in Equation 3, a node must assess $T_{i,j}^{1-hop,\ X}(t)$ of its 1-hop neighbors using the detection mechanisms for trust component X described in Section 3. Because the assessment is direct, assuming that the detection mechanisms are effective, $T_{ij}^{1-hop,X}(t)$ computed by node i will be close to actual status of node j at time t, which can be obtained from the SPN model output. We assert that all detection mechanisms (discussed in Section 3) are effective and accurate, except for the anomaly detection mechanisms for detecting unhealthiness because of imperfection in anomaly detection, causing $T_{i,j}^{1-hop,\ healthiness}(t)$ to deviate from the actual healthiness status of node j. The imperfection is accounted for by considering the false alarm probabilities of anomaly detection mechanisms employed, i.e., a false negative probability (P_{fn}^H) and a false positive probability (P_{fp}^H), given as input to the system. Both P_{fn}^H and P_{fp}^H can be obtained from the provider of specific anomaly detection mechanisms, e.g., [32]. Both must be sufficiently low (e.g., less than 5%) for the anomaly detection mechanisms to be considered as a valid design.

With these key observations, we leverage SPN outputs reflecting actual status of nodes to predict $T_{i,j}^{1-hop,\ X}(t)$ which would be obtained by node i at runtime. Table 2 gives specific reward assignments used to compute $T_{i,j}^{1-hop,\ X}(t)$. Here we note that when computing $T_{i,j}^{1-hop,\ healthiness}(t)$ in order to account for the imperfection of the anomaly detection mechanisms employed for detecting unhealthiness, instead of assigning a reward of 1 if node j is not compromised, i.e., *mark(j's CN)* = 0, we assign a reward of *1-*P_{fp}^H to account for the false positive probability. Also instead of assigning a reward of 0 if node j is compromised, i.e., *mark(j's CN)* = 1, we assign a reward of P_{fn}^H to account for the false negative probability. All other reward assignments for X=intimacy, energy, and cooperativeness simply yield the actual status of node j in trust component X at time t.

Table 1: Reward Assignments for Objective Trust Evaluation.

Component trust probability toward node j	r_s: reward assignment to state s
$T_j^{obj,intimacy}(t)$	$1\ if\ mark(j's\ \ location)$ *is within a 5-region neighbor area at time t; 0 otherwise*
$T_j^{obj,healthiness}(t)$	$1\ if\ (mark(j's\ CN) = 0)$; 0 *otherwise*
$T_j^{obj,energy}(t)$	$1\ if\ (mark(j's\ Energy) > E_T)$; 0 *otherwise*
$T_j^{obj,cooperativeness}(t)$	$1\ if\ (mark(j's\ UNCOOP) = 0)$; 0 *otherwise*

Table 2: Reward Assignments for Subjective Trust Evaluation.

Component trust probability of node i toward node j	r_s: reward assignment to state s
$T_{i,j}^{1-hop,intimacy}(t)$	1 *if i and j are 1-hop neighbors within last* $d\Delta t$; 0 *otherwise*
$T_{i,j}^{1-hop,healthiness}(t)$	1-P_{fp}^H *if (mark(j's CN)* = 0); P_{fn}^H *otherwise*
$T_{i,j}^{1-hop,energy}(t)$	$1\ if\ (mark(j's\ Energy) > E_T)$; 0 *otherwise*
$T_{i,j}^{1-hop,cooperativeness}(t)$	$1\ if\ (mark(j's\ UNCOOP) = 0)$; 0 *otherwise*

When node i obtains $T_{i,j}^{1-hop,\ X}(t)$, it computes $T_{i,j}^{direct,\ X}(t)$ from Equation 3. Then node i computes $T_{i,j}^{indirect,\ X}(t)$ based on Equation 4, as well as $T_{i,j}^{X}(t)$ and $T_{i,j}(t)$ from Equations 2 and 1, respectively. Finally, the overall average subjective trust values of node j, $T_j^{sub,X}(t)$ and $T_j^{sub}(t)$, can be obtained through Equations 5 and 6, respectively. We compare $T_j^{sub}(t)$ with objective trust $T_j^{obj}(t)$ for validating SQTrust design.

5 Evaluation Results

A. *Operational Profile as Input*

Table 3: Operational Profile for a Mobile Group Application.

Parameter	Value	Parameter	Value
# of regions	6x6	R	250m
area	1250mx1250m	E_{init}	[12, 24] hrs
S_{init}	(0, 2] m/sec.	ε	1.2
$1/\lambda_{com}$	18 hrs	α	0.8
T_{gc}	120 sec.	P_{fn}^H, P_{fp}^H	0.5%

Table 3 lists the parameter set and their default values specifying the operational profile given as input for testing SQTrust for a mobile group application in MANET environments. We populate a MANET with 150 nodes moving randomly with speed S_{init} in the range of (0, 2] m/s in a 6×6 operational region in a 1250mx1250m area, with each region covering R=250m radio radius. The environment being considered is assumed hostile and insecure with the average

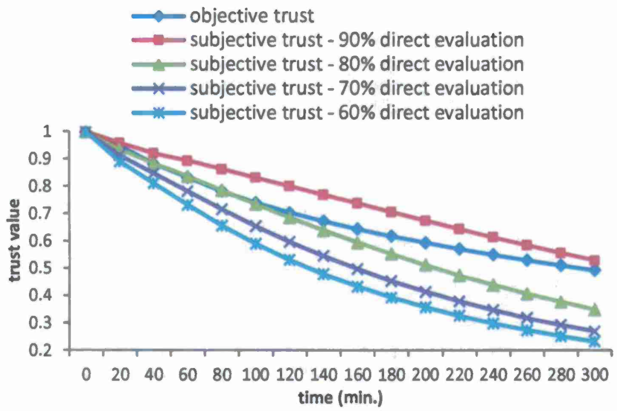


Figure 2: Overall Trust Evaluation: Subjective Trust is Most Accurate When using 85% Direct Trust Evaluation *($\beta 1$:$\beta 2$=0.85:0.15).*

compromising rate λ_{com} set to once per 18 hours. Each node's energy is in the range of [12, 24] hours. Further each node observes the node behavior model as specified in Section 2.C and Section 4.A with ε=1.2, α=0.8 and T_{gc}=120 sec. Initially all nodes are not compromised. When a node turns malicious, it performs good-mouthing and bad-mouthing attacks, i.e., it will provide the most positive recommendation (that is, 1) toward a bad node to facilitate collusion, and conversely the most negative recommendation (that is, 0) toward a good node to ruin the reputation of the good node. The initial trust level is set to 1 for healthiness, energy and cooperativeness because all nodes are considered trustworthy initially. The initial trust level of intimacy is set to the probability that a node is found to be in a 5-region neighbor area relative to 6x6 regions in accordance with the intimacy definition.

Given this operational profile as input to the mobile group application, we aim to identify the best setting of β_1: β_2 (with higher β_1 meaning more direct observations or self-information being used for subjective trust evaluation) under which subjective trust is closest to objective trust. We also aim to identify the best setting of $w_1 : w_2 : w_3 : w_4$ (the weight ratio for the 4 trust components considered), and M_1 and M_2 (the minimum trust level and drop-dead trust level) under which the application performance is maximized. For trust protocol execution, we set the decay coefficient $\lambda_d = 0.001$, and the trust evaluation interval $\Delta t = 20$ min, resulting in $e^{-\lambda_d \Delta t} = 0.98$ to model small trust decay over time. Also the minimum recommender threshold T_t^X is set to 0.6, the trust evaluation window size d is set to 2, and the minimum energy trust threshold E_T is set to 0.

B. Identifying SQTrust Protocol Settings for Accurate Peer-to-Peer Subjective Trust Evaluation

Figure 2 shows the node's overall trust values obtained from subjective trust evaluation vs. objective trust evaluation, i.e., $T_j^{sub}(t)$ vs. $T_j^{obj}(t)$, for the equal-weight ratio case as a function of time, with β_1: β_2 varying from 0.6: 0.4 (60% direct evaluation: 40% indirect evaluation) to 0.9: 0.1 (90% direct evaluation: 10% indirect evaluation). The 10% increment in β_1 allows us to identify the best β_1: β_2 ratio under which subjective trust is closest to objective trust. We see that subjective trust evaluation results are closer and closer to objective trust evaluation results as we use more conservative direct observations or self-information for subjective trust evaluation. However, there is a cutoff point (at about 85%) after which subjective trust evaluation overshoots. This implies that using too much direct observations for subjective trust evaluation could overestimate trust because there is little chance for a node to use indirect observations from trustworthy recommenders. Our analysis allows such a cutoff point to be determined given design considerations regarding trust decay over time ($e^{-\lambda_d \Delta t} = 0.98$ for direct trust decay in our case study).

C. Identifying Best Trust Formation Setting to Maximize Application Performance

We consider a mission-oriented mobile group application scenario in which a commander node, say node i, dynamically selects n nodes (n=5 in the case study) which it trusts most out of active mobile group members for mission execution. We consider dynamic team membership such that after each trust evaluation window Δt the commander will reselect its most trusted nodes composing the team for mission executions based on its peer-to-peer subjective evaluation values $T_{i,j}(t)$ toward nodes j's as calculated from Equation 1. The rationale behind dynamic membership is that the commander may exercise its best judgment to select n most trusted nodes to increase the probability of successful mission execution. Assume that all n nodes selected at time t are critical for mission execution during [t, t+Δt] so that if any one node selected fails, the mission fails. We can then apply Equations 8 and 9 to compute $P_{mission}$ over an interval [t, t+Δt]. Since all time intervals are connected in a series structure, $P_{mission}$ over the overall mission period [0, TR] can be computed by the product of individual $P_{mission}$'s over intervals [0, Δt], [Δt, $2\Delta t$], ..., [TR-Δt, TR].

Figure 3 shows the mission success probability $P_{mission}$ as a function of mission completion deadline TR. To examine the effect of $w_1 : w_2 : w_3 : w_4$ (the weight ratio for the 4 trust components considered in this paper), we consider 5 test cases: (a) *equal-weight*, (b) *social trust only*, (c) *QoS trust only*, (d) *more social trust*, and (e) *more QoS trust* as listed in Table 4 with (M_1, M_2) set to (0.85, 0.55) to isolate its effect.

For all test cases we see that as TR increases, the mission success probability decreases because a longer mission execution time increases the probability of low-trust nodes (whose population increases over time because of cooperativeness or healthiness trust decay) becoming members of the team for mission execution. For comparison, the mission success probability $P_{mission}$ based on objective trust evaluation results is also shown, representing the ideal case in which node i has global knowledge of status of all other nodes in the system and therefore it always picks n truly most trustworthy nodes in every Δt interval for mission execution. For each case, we also show the optimal β_1: β_2 ratio (with higher β_1 meaning more direct observations or self-information being used for subjective trust evaluation) at which $P_{mission}$ obtained based on subjective trust evaluation results is virtually identical to $P_{mission}$ obtained based on objective trust evaluations.

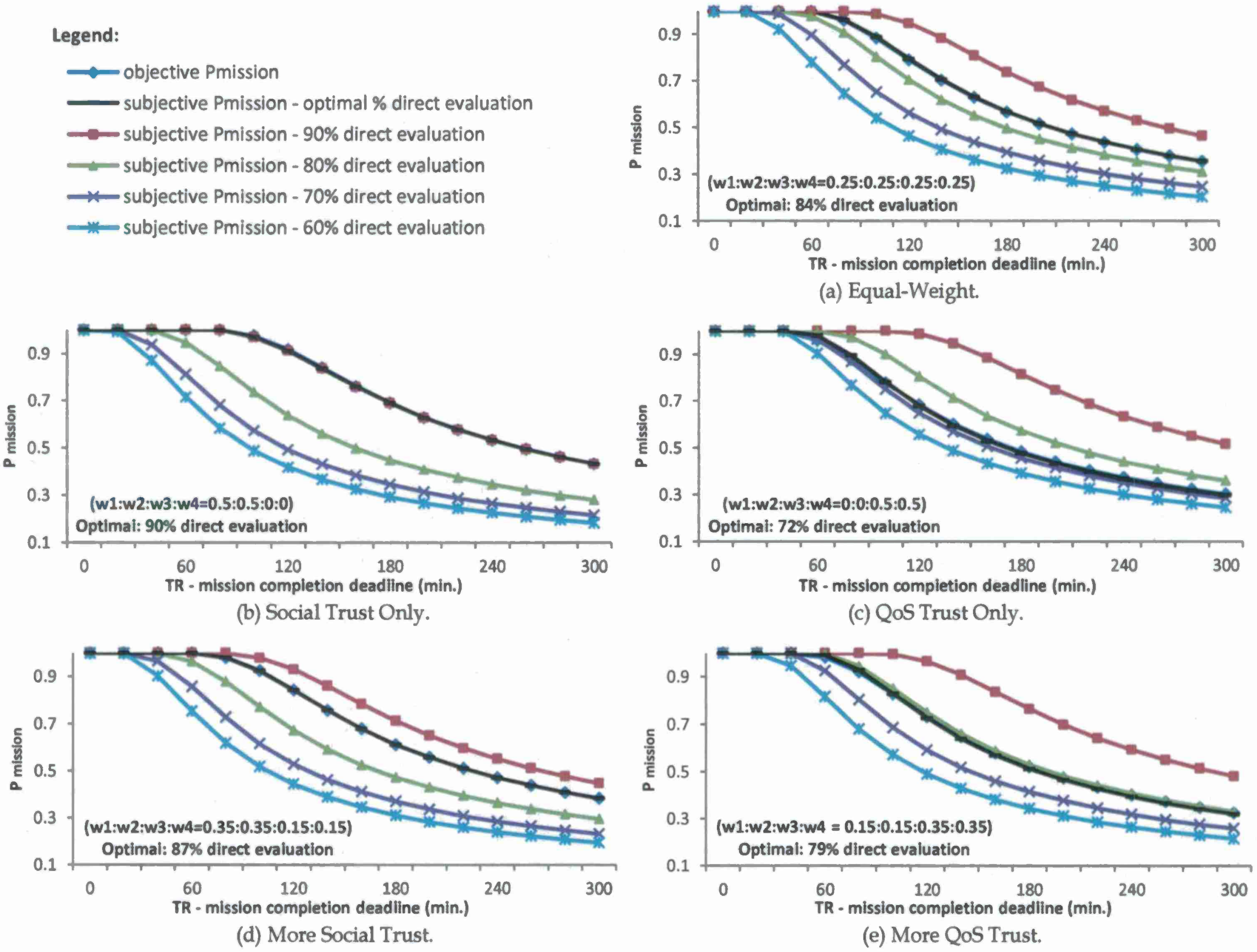
Table 4: Weight Ratio for Trust Components.

Test case	Weight ratio
Equal-weight	$w_1: w_2: w_3: w_4 = 0.25: 0.25: 0.25: 0.25$
Social trust only	$w_1: w_2: w_3: w_4 = 0.5: 0.5: 0: 0$
QoS trust only	$w_1: w_2: w_3: w_4 = 0: 0: 0.5: 0.5$
More social trust	$w_1: w_2: w_3: w_4 = 0.35: 0.35: 0.15: 0.15$
More QoS trust	$w_1: w_2: w_3: w_4 = 0.15: 0.15: 0.35: 0.35$

We observe that as more social trust is being used for subjective trust evaluation, the optimal β_1: β_2 ratio increases, suggesting that social trust evaluation is very subjective in nature and a node would rather trust its own interaction experiences more than recommendations provided from other peers, especially in the presence of malicious nodes that can perform good-mouthing and bad-mouthing attacks. Also again we observe that while using more conservative direct observations or self-information for subjective trust evaluation in general helps in bringing subjective $P_{mission}$ closer to objective $P_{mission}$, there is a cutoff point after which subjective trust evaluation overshoots.

Figure 3 demonstrates the effectiveness of SQTrust. When given an operational profile characterized by a set of model parameter values defined in Table 3, the analysis methodology developed in this paper helps identify the best weight of direct observations vs. indirect recommendations (i.e., β_1: β_2) to be used for subjective trust evaluation, so that SQTrust can be fine-tuned to yield results virtually identical to those by objective trust evaluation based on actual knowledge of node status.

In Figure 4 we compare $P_{mission}$ vs. TR for the mission group under various $w_1: w_2: w_3: w_4$ ratios, with each operating at its best β_1:β_2 ratio identified so that



(a) Equal-Weight.

(b) Social Trust Only.

(c) QoS Trust Only.

(d) More Social Trust.

(e) More QoS Trust.

Figure 3: Mission Success Probability: Subjective vs. Objective Evaluation.

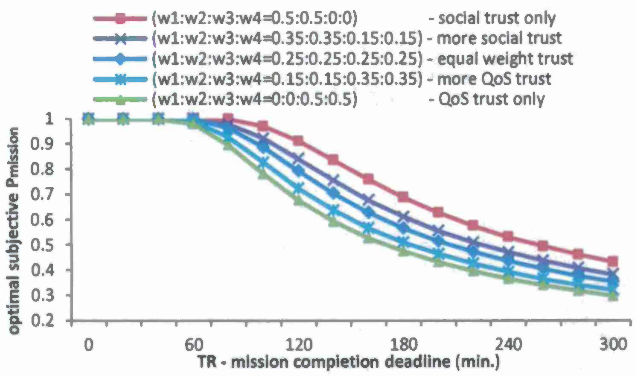


Figure 4: Effect of $w_1{:}w_2{:}w_3{:}w_4$ on Mission Success Probability: Using More Social Trust Increases Mission Success Probability.

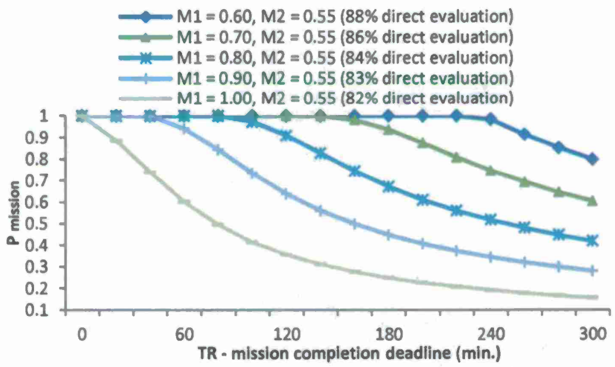


Figure 5: Effect of M1 on Mission Success Probability: Using Higher M1 (Minimum Trust Level) Decreases Mission Success Probability.

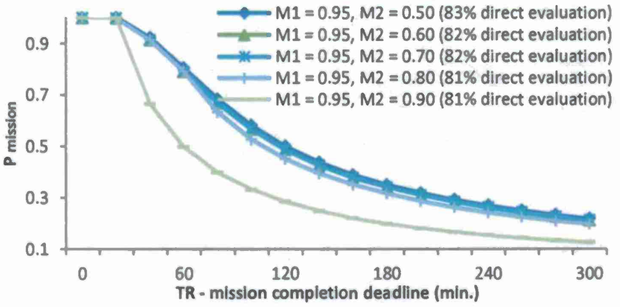


Figure 6: Effect of M_2 on Mission Success Probability: Using Higher M2 (Drop Dead Trust Level) Decreases Mission Success Probability.

in each test case subjective $P_{mission}$ is virtually the same as objective $P_{mission}$. We see that "social trust only" produces the highest system reliability, while "QoS trust only" has the lowest system reliability among all, suggesting that in this case study social trust metrics used (intimacy and healthiness) are able to yield higher trust values than those of QoS trust metrics used (energy and cooperativeness). Certainly, this result should not be construed as universal. When given an operational profiles input, the model-based analysis methodology developed in this paper helps identify the best $w_1{:}w_2{:}w_3{:}w_4$ weight ratio to maximize the system reliability.

Lastly we analyze the effect of mission trust thresholds M_1 (the minimum trust level required for successful mission completion) and M_2 (the drop dead trust level). Figures 5 and 6 show $P_{mission}$ vs. TR for the system operating under best $\beta_1{:}\beta_2$ settings in the equal-weight case for each (M_1, M_2) combination. Recall that M_1 and M_2 are the high and low trust thresholds to determine if a node is trustworthy for mission execution. From Figure 5, we see that as M_1 increases, the system reliability decreases because there is a smaller chance for a node to satisfy the high threshold for it to be completely trustworthy for mission execution. Similarly from Figure 6, we see that as M_2 increases, the system reliability decreases because there is a higher chance for a node to be completely untrustworthy for mission execution. We also observe that the reliability is more sensitive to M_1 than M_2. A system designer can set proper M_1 and M_2 values based on the mission context such as the degree of difficulty and mission completion deadline, utilizing the model-based methodology developed in the paper to analyze the effect of M_1 and M_2 so as to improve the system reliability.

6 SIMULATION VALIDATION

We validate SQTrust and its application to mobile group reliability assessment through extensive simulation using ns-3 [22]. The simulated MANET environment is setup as described in Table 3. The network consists of 150 nodes following the random waypoint mobility model in a 1500 m × 1500 m operational area, with the speed in the range of (0, 2] m/s and pause time of zero. The initial node energy is in the range of [40, 80] joules, corresponding to [12, 24] hours of operational time in normal status. A node may be compromised with a per-node capture rate of λ_{com}. As time progresses, a node may become uncooperative, the rate of which is implemented according to Equation 12. When a node becomes uncooperative, it would not follow protocol execution and will drop packets to save energy. A compromised node will also drop packets. In addition, it will perform bogus message attacks, as well as good-mouthing and bad-mouthing attacks. All nodes execute SQTrust as described in Section 3 to perform subjective trust evaluation.

We collect simulation data to validate analytical results reported earlier. Due to space limitation, we only report two figures. Figure 7 shows the simulation results for the overall subjective trust obtained under the equal-weight case, corresponding to Figure 2 obtained earlier from theoretical analysis. As in Figure 2, we simulate 7 cases with β_1: β_2 varying from 0.6: 0.4 to 0.9: 0.1. For each case, we collect observations from sufficient simulation runs with disjoint random number streams to achieve ±5% accuracy level with 95% confidence. The simulation results in Figure 7 are remarkably similar to the analytical results shown in

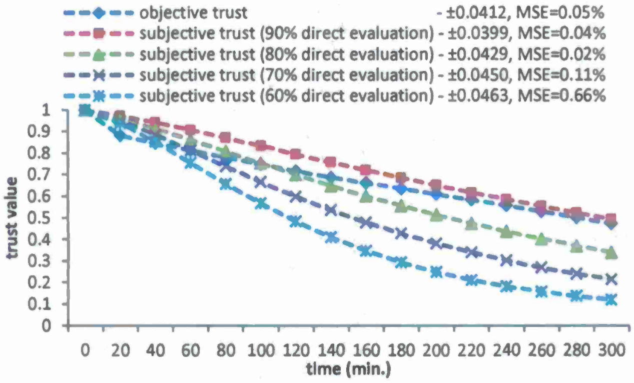


Figure 7: Simulation Results of Overall Trust Corresponding to Figure 2.

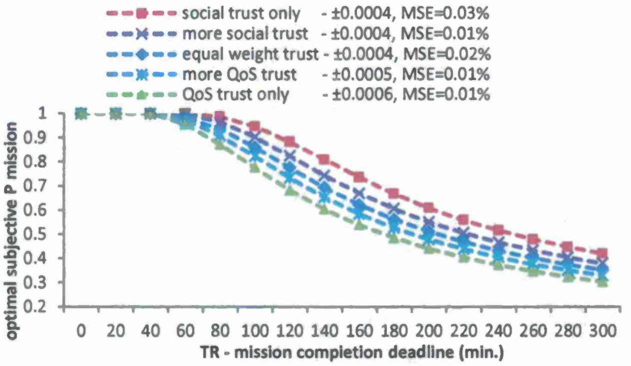


Figure 8: Simulation Results of Reliability Assessment Corresponding to Figmure 4.

Figure 2, with the average mean square error (MSE) between the simulation results vs. the analytical results less than 5%.

Figure 8 shows the simulation results for the effect of $w_1 : w_2 : w_3 : w_4$ on mission success probability $P_{mission}$, corresponding to Figure 4 obtained earlier from analytical calculations. As in Figure 4, we simulate 5 cases for the w_1: w_2: w_3: w_4 weight ratio (see Table 4). We observe that Figure 8 is virtually identical to Figure 4 in shape exhibiting the same trend that using more social trust would yield higher system reliability. The MSE is remarkably small (less than 0.03%) for all cases. We conclude that our analytical results reported in Figures 2-6 are accurate and valid.

7 Conclusion

In this paper, we proposed and analyzed a trust management protocol called SQTrust that incorporates both social and QoS trust metrics for subjective trust evaluation of mobile nodes in MANETs. The most salient feature of SQTrust is that it is distributed and dynamic, only requiring each node to periodically estimate its degree of social and QoS trust toward its peers local or distance away. We developed a novel model-based methodology based on SPN techniques for describing the behavior of a mobile group consisting of well-behaved, malicious and uncooperative nodes given the anticipated system operational profile as input. By using a probability model describing node behavior in a MANET based on an anticipated operational profile given as input, we allow the *objective* trust values of nodes to be calculated based on actual status of nodes as time progresses, which serves as the basis for validating SQTrust. The analytical results validated by simulation results demonstrate that SQTrust is able to provide accurate subjective trust evaluation results compared with objective trust evaluation results, thus supporting its resiliency property to bad-mouthing and good-mouthing attacks by malicious nodes. We also demonstrated the effect of SQTrust on the reliability of mission-oriented mobile groups with simulation validation. Using mission-oriented mobile groups as an application, we demonstrated that one can identify the best trust formation to maximize the application performance in terms of the system reliability.

In the future we plan to investigate the notion of adaptive trust management by which the trust formation formula for forming trust out of social and QoS components is dynamically adjusted in response to changing environment conditions such as dynamically evolving hostility or evolving mission requirements to optimize application performance.

Acknowledgement

This work was supported in part by the Office of Naval Research under Grant N00014-10-1-0156.

References

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

[2] E. Ahmed, et al., "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks." *Asia Pacific Information Technology Security Conf.*, Gold Coast, Australia, May 2006.

[3] E. Aivaloglou, S. Gritxalis, and C. Skianis, "Trust Establishment in Ad Hoc and Sensor Networks," *1st Int'l Workshop on Critical Information Infrastructure Security*, Samos, Greece, vol. 4347, Aug. 2006, pp. 179-192.

[4] M. Aldebert, M. Ivaldi, and C. Roucolle, "Telecommunications Demand and Pricing Structure: an Economic Analysis," *Telecommunication Systems*, vol. 25, no. 1-2, Jan. 2004, pp. 89-115.

[5] 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, June 2007, pp. 64-69.

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

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

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

[9] B.J. Chang and S.L. Kuo, "Markov Chain Trust Model for Trust Value Analysis and Key Management in Distributed Multicast MANETs," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, 2009, pp. 1846-1863.

[10] J.H. Cho, A. Swami and I.R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, DOI 10.1109/SURV.2011.092110.00088, Oct. 2010.

[11] J.H. Cho and I.R. Chen, "Effect of Intrusion Detection on Reliability of Mission-Oriented Mobile Group Systems in Mobile Ad Hoc Networks," *IEEE Transactions on Reliability*, vol. 59, no. 1, 2010, pp. 231-241.

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

[13] E.M. Daly and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, May 2009, pp. 606-621.

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

[15] L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," *Mobile Networks and Applications*, 2001, vol. 6, pp. 239-249.

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

[17] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," *Securecomm*, Baltimore, MD, Aug. 2006, pp. 1-7.

[18] G.C. Hadjichristofi, W.J. Adams, and N.J. Davis, "A Framework for Key Management in a Mobile Ad Hoc Network," *Int'l Conf. on Information Technology*, Tiejun Huang, China, April 2005, vol. 2, pp. 568-573.

[19] C. Hui, M. Goldberg, M. Magdon-Ismail, and W. Wallace, "Simulating the diffusion of information: An agent-based modeling approach," *International Journal of Agent Technologies and Systems*, 2010, vol. 2, no. 3, pp. 31-46.

[20] A. Josang, "Artificial Reasoning with Subjective Logic," *2nd Australian Workshop on Commonsense Reasoning*, Perth, Australian, Dec. 1997, pp. 1-17.

[21] A. Josang and R. Ismail, "The Beta Reputation System," *15th Conference on Electronic Commerce*, Bled, Slovenia, June 17-19, 2002, pp. 1-14.

[22] *The ns-3 Network Simulator*, http://www.nsnam.org, Nov. 2011.

[23] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," *12th international conference on World Wide Web*, May 20-24, 2003, Budapest, Hungary, pp. 640-651.

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

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

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

[27] 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.

[28] J.D. Musa, "Operational Profiles in Software-Reliability Engineering," *IEEE Software*, vol. 10, no. 2, March 1993, pp. 14-32.

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

[30] R.A. Sahner, K.S. Trivedi and A. Puliafito, *Performance and Reliability Analysis of Computer Systems*, Kluwer Academic Publishers, 1996.

[31] 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*, Dec. 2006. Surathkal, India, pp. 62-67.

[32] A. daSilva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," *ACM 1st International Workshop on Quality of Service and Security in Wireless and Mobile Networks*, Montreal, Quebec, Canada, 2005.

[33] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication," *Proc. 3rd ACM Conf. on Computer and Communications Security*, Jan. 1996, pp. 31-37.

[34] 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, 2006, pp. 305-317.

[35] G. 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.

[36] K.S. Trivedi, *Stochastic Petri Net Package*, version 6, Duke University, 1999.

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

[38] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," *IEEE Transactions on Knowledge and Data Engineering*, 2004, vol 16, no. 7, pp. 843-857.

[39] 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.

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

[41] L. Capra, and M. Musolesi, "Autonomic Trust Prediction for Pervasive Systems," in International Conference on Advanced Information Networking and Applications, April 2006, pp. 1-5.