REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
15-08-2010	Quarterly technical report	16 May 2010 - 15 August 2010

4. TITLE AND SUBTITLE
SQTrust: Social and QoS Trust Management for Mission-Oriented Mobile Groups

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 notions of social trust derived from social networks with 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 demonstrate the effectiveness of the composite social and QoS trust management protocol (henceforward referred to as SQTrust) for mission-oriented mobile groups in MANETs for critical mission executions. SQTrust is distributed in nature and will be run by each mobile node to subjectively yet informatively assess the trust levels of other mobile nodes nearby or distance away based on direct observations towards its neighbors, and indirect observations obtained from recommenders. We take a model-based approach to analyze both objective and subjective trust as the basis for fine-tuning and validating SQTrust so that subjective trust evaluation is close to objective trust evaluation. We demonstrate resiliency of SQTrust against malicious attacks and identify the best direct vs. indirect evaluation ratio as well as the best social trust vs. QoS trust weight ratio under which the reliability of mission-oriented mobile groups in MANET environments is maximized.

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

16. SECURITY CLASSIFICATION OF:	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
			Chen, Ing-Ray

INSTRUCTIONS FOR COMPLETING SF 298

a. REPORT	b. ABSTRACT	c. THIS PAGE	SAR	6	19b. TELEPONE NUMBER (*Include area code*)
U	U	U			(703) 538-8376

STANDARD FORM 298 Back (Rev. 8/98)

SQTrust: Social and QoS Trust Management for Mission-Oriented Mobile Groups

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

Abstract— We propose to combine the notions of *social trust* derived from social networks with *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 demonstrate the effectiveness of the composite social and QoS trust management protocol (henceforward referred to as SQTrust) for mission-oriented mobile groups in MANETs for critical mission executions. SQTrust is distributed in nature and will be run by each mobile node to subjectively yet informatively assess the trust levels of other mobile nodes nearby or distance away based on direct observations towards its neighbors, and indirect observations obtained from recommenders. We take a model-based approach to analyze both *objective* and *subjective* trust as the basis for fine-tuning and validating SQTrust so that subjective trust evaluation is close to objective trust evaluation. We demonstrate resiliency of SQTrust against malicious attacks and identify the best direct vs. indirect evaluation ratio as well as the best social trust vs. QoS trust weight ratio under which the reliability of mission-oriented mobile groups in MANET environments is maximized.

Index Terms— trust management, group communication systems, 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 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 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" [16], "a belief on reliability, dependability, or security" [19], "a belief about competence or honesty in a specific context" [3], and "reliability, timeliness, and integrity of message delivery" [20].

There is yet consensus about what should be measured to evaluate trust management systems. Golbeck [15] introduced the concept of *social trust* by suggesting the use of social networks as a bridge to build trust relationships among entities. Yu *et al.* [28] used social networks to evaluate trust values in the presence of Sybil attacks. Standard performance metrics such as control packet overhead, throughput, goodput, packet dropping rate and delay have been used to evaluate trust [14], [24], [27]. Dependability metrics such as availability [17], 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 thresholds [21] 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 [29], trust level [25], trustworthiness [21], and opinion [26].

Trust management is often used with different purposes in diverse decision making situations such as secure routing [5], [14], [24], [25], [27], [29], key management [9], [17], authentication [23], 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 [26], graph/random theory [6], Markov chain [9], etc. For more details on trust management in MA-

- *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, Powder Mill Rd. Adelphi, MD 20783. E-mail: jinhee.cho@us.army.mil.*

NETs, the interested readers are referred to our very recent survey paper [10].

In this work, we concern the trust level of a node as perceived by another node. However, instead of considering just one particular trust attribute, we consider multiple trust attributes drawing from *social trust* and *QoS trust* to form a composite social and QoS trust metric. More specifically our proposed social and QoS trust management protocol (henceforth called SQTrust) is capable of incorporating *social trust* metrics including friendship, honesty, privacy, similarity, betweenness centrality, and social ties [13], as well as *QoS trust* metrics including competence, cooperation, reliability, and task satisfaction, for trust management of mobile groups in MANET environments. Further, we take a model-based approach and develop a mathematical model based on Stochastic Petri net (SPN) techniques to define a mission-oriented mobile group consisting of a large number of mobile nodes designed to achieve missions in the presence of malicious, erroneous, partly trusted and uncertain information. The SPN provides a global view of the system and can serve as the basis for *objective trust evaluation* based on global knowledge of actual node status against which subjective trust evaluation can be compared and validated.

This paper has the following contributions: First, we develop a new trust management protocol (SQTrust) based on composite social and QoS trust, 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 full global knowledge 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 SPN mathematical model for describing the "actual" dynamic behaviors of nodes in MANETs in the presence of behaved, selfish and malicious nodes, as well as an intrusion detection system (IDS) for detecting and removing malicious nodes. The SPN model allows us to analytically determine objective trust, leveraging on the global knowledge on actual node status which evolves dynamically. With this methodology, we demonstrate that SQTrust is capable of providing valid trust evaluation results close to those obtained from objective trust evaluation based on global knowledge and actual node status. Finally, we analyze the effect of SQTrust on the reliability of a mission-oriented mobile group considering the intrinsic relationship between trust and reliability for critical mission executions by the mobile group.

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 dynamically. Section 4 develops a performance model to describe dynamic behaviors of nodes in MANETs in the presence of behaved, selfish and malicious nodes and IDS with the objective to validate subjective trust evaluation with objective trust evaluation. Section 5 presents quantitative results obtained with physical interpretations given. Section 6 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 the most for mission execution to demonstrate the applicability of SQTrust. Finally, Section 7 summarizes the paper and outlines future research areas.

2 System Model

There is no centralized trusted authority. Nodes communicate through multi-hops. Every node may have a different level of energy and speed reflecting node heterogeneity. Some nodes may behave selfishly in order to save their own energy particularly when they have low energy. Further, nodes can be compromised. The energy level of a node is related with the speed at which the node may be compromised. That is, a node is more likely to be compromised when it has low energy and vice versa since a node with high energy may be more capable of defending itself against attackers by performing energy-consuming defense mechanisms. To deal with inside attackers, the system employs a distributed intrusion detection system (IDS) such as one described in [11] for detecting compromised nodes. As soon as a compromised node is detected by IDS, the node is evicted from the system and the trust value of the node drops to the lowest level. The distributed IDS is characterized by false positive and false negative probabilities for which less than 1% is deemed acceptable. The energy level of each node is adjusted depending on its status. For example, if a node becomes selfish, the speed of energy consumption is slowed down and vice versa. If a node becomes compromised but not detected by IDS, the speed of energy consumption would grow since the node may have a chance to perform attacks which may consume more energy.

Our system model also considers redemption possibilities for selfish nodes. That is, upon learning status of neighbor nodes through periodic trust evaluation, a selfish node can go back to normal or continue being selfish depending on their own energy level. For a mobile group, when a node is not a member, it will not consume energy as much as when it is a member. Upon every membership change due to join or leave or eviction, individual rekeying (meaning the rekey operation is done immediately) will be performed based on a distributed key agreement protocol such as the Group Diffie-Hellman (GDH) protocol. We assume that a node's trust value is assessed based on direct and indirect information incorporating direct observations and recommendations. The trust assess-

ment of one node toward another node is updated periodically.

Trust Metric Model – A node's trust value is assessed based on direct observations as well as indirect recommendations. We do not consider dispositional belief or cognitive characteristics of an entity in deriving trust. Our trust metric consists of two trust types: *social trust* and *QoS trust*. Social trust is evaluated through social networks to account for social relationships. 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 are considered to represent the important aspects of social trust in MANETs [10]. *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 cooperation (measured by ***unselfishness*** for packet delivery) to measure the QoS trust level of a node. 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. To allow the system designer to assign weights to different trust components, we use a weight ratio between these four trust components as $w_1 : w_2 : w_3 : w_4$ to reflect their desirable degrees in mission execution, denoting the effect of intimacy: healthiness: energy: unselfishness on the overall trust. One goal of this paper is to identify the effects of these weights, when given a mission-oriented mobile group characterized by a set of design parameter values reflecting the unique characteristics of MANET environments.

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 are close to each other and have a lot of interaction experiences with each other, for example, for packet routing and forwarding. In MANET environments due to node mobility and grouping, intimacy is invariably related to the probability of two nodes being physically close to each other engaging in packet routing and forwarding activities. 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. A compromised node may perform fake information dissemination (e.g., good-mouthing for bad nodes and bad-mouthing attacks against good nodes), identity attacks (e.g., Sybil, masquerading) or Denial-of-Service (DoS) attacks (e.g., consuming resources unnecessarily by disseminating bogus packets). With the presence of IDS which detects and announces malicious nodes in the system, each node can use this information to help with the assessment of healthiness of another node. We assume that a malicious node will always perform attacks on good nodes and does not discriminate good nodes when performing attacks. The energy component refers to the residual energy of a node, and for a MANET environment, energy is directly related to the ability of a node to be able to execute a task competently. Finally the unselfishness (cooperation) 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 probability of a node being able to faithfully relay and respond to group communication packets.

Referral Trust vs. Functional Trust – We differentiate referral trust from functional trust [18]. When a recommender node, say, node m, provides its recommendation to node i for evaluating node j, node i's referral trust on node m is multiplied with node m's functional trust on node j to yield node m's recommending trust value toward node j to account for trust decay in time and space. 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 intimacy, energy and unselfishness 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.

Attack Models – A malicious node may perform good-mouthing and bad-mouthing attacks. Further it may perform whitewashing attacks, e.g., reporting false information about itself to improve its trust status. SQTrust is based on monitoring, snooping and overhearing for direct observations, and referral trust for indirect observations. It does not take information passed to it from a neighbor node as part of its trust evaluation process toward the neighbor node, so it is resilient to whitewashing attacks. It is resilient to good-mouthing and bad-mouthing attacks by weighting indirect recommendations by the recommender's referral trust. Thus if a bad node (while performing a good-mouthing attack) provides a good recommendation about a bad node, the good recommendation will be discounted by the recommender's bad referral trust. This is further assured by choosing only 1-hop neighbors as recommenders in SQTrust because a node can have fairly accurate trust assessments toward its one-hop neighbors in intimacy, energy and unselfishness status. Our approach of showing resiliency against good-mouthing and bad-mouthing attacks by malicious nodes is model-based, that is,

through a mathematical model (introduced in Section 4) we show quantitatively that subjective trust evaluation results obtained from SQTrust are close to objective evaluation results obtained from actual knowledge.

Mission Reliability Model - SQTrust aims to increase the probability of successful mission execution. For mission-critical applications, it is also 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 the 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 in the system and thus upon a mission assignment allows the node to select highly trustable nodes for collaboration to maximize the probability of successful mission execution.

3 Design of SQTrust

SQTrust is designed to be executed by every node at runtime. The trust value of node j as evaluated by node i at time t, denoted as $T_{i,j}(t)$, is computed by node i as a weighted average of intimacy, healthiness, energy, and unselfishness trust components. Specifically node i will compute $T_{i,j}(t)$ by:

$$T_{i,j}(t) = w_1\, T_{i,j}^{intimacy}(t) + w_2\, T_{i,j}^{healthy}(t) + w_3\, T_{i,j}^{energy}(t) + w_4\, T_{i,j}^{unselfish}(t) \quad (1)$$

where $T_{i,j}^{intimacy}(t)$, $T_{i,j}^{healthy}(t)$, $T_{i,j}^{energy}(t)$ and $T_{i,j}^{unselfish}(t)$ are the trust beliefs of node i toward node j in intimacy, healthiness, energy and unselfishness trust components, respectively, and $w_1 : w_2 : w_3 : w_4$ is the weight ratio for weighing intimacy: healthiness: energy: unselfishness with $w_1 + w_2 + w_3 + w_4 = 1$. While we do not know exactly where a node is at time t, we might have knowledge about the probability of its location given the mobility pattern of the mobile node especially for group operations. Let the probability that node j being located in area q be $P_j^{loc=q}(t)$. Let the probability that node i and node j are k-hop apart at time t be $P_{i,j}^{k-hop}(t)$ given by:

$$P_{i,j}^{k-hop}(t) = \sum_{(p,q)\in U} \left(P_i^{loc=p}(t)\, P_j^{loc=q}(t) \right) \quad (2)$$

where U is a set covering all (p, q) pairs with the distance between p and q being k-hops. We propose to use a simple mathematical model based on SPN techniques to yield these probabilities. Now $T_{i,j}^{intimacy}(t)$, $T_{i,j}^{healthy}(t)$, $T_{i,j}^{energy}(t)$ and $T_{i,j}^{unselfish}(t)$ in Equation 1 can be calculated by the weighted average of $T_{i,j}^{k-hop,intimacy}(t)$, $T_{i,j}^{k-hop,healthy}(t)$, $T_{i,j}^{k-hop,energy}(t)$, and $T_{i,j}^{k-hop,unselfish}(t)$ respectively, conditioning on nodes i and j are being k-hop apart, for example, by:

$$T_{i,j}^{unselfish}(t) = \sum_{all\ k \le k_{max}} \left(P_{i,j}^{k-hop}(t)\, T_{i,j}^{k-hop,\ unselfish}(t) \right) \quad (3)$$

where k_{max} is the maximum number of hops that can possibly separate any two nodes as bounded by the physical operational area. These conditional terms, i.e., $T_{i,j}^{k-hop,intimacy}(t)$, $T_{i,j}^{k-hop,healthy}(t)$, $T_{i,j}^{k-hop,energy}(t)$, and $T_{i,j}^{k-hop,unselfish}(t)$ in turn can be computed by a weighted average of direct observations of node i itself toward node j (when k=1) or self-information (when k>1) versus indirect information obtained from recommenders. As an example, $T_{i,j}^{k-hop,unselfish}(t)$ can be computed by:

$$T_{i,j}^{k-hop,unselfish}(t) = \beta_1\, T_{i,j}^{k-hop,\ direct,\ unselfish}(t) + \beta_2\, T_{i,j}^{k-hop,\ indirect,\ unselfish}(t) \quad (4)$$

In Equation 4, β_1 is a weight parameter to weigh node i's own information toward node j's unselfish assessment at time t, i.e., "direct observations" (when k=1) or "self-information" (when k>1) and β_2 is a weight parameter to weigh indirect information from recommenders, i.e., "information from others," with $\beta_1 + \beta_2 = 1$.

$T_{i,j}^{k-hop,\ direct,\ unselfish}(t)$ in Equation 4 is defined as:

$$T_{i,j}^{k-hop,\ direct,\ unselfish}(t) = \begin{cases} T_{i,j}^{1-hop,\ direct,\ unselfish}(t) & \text{if } k = 1 \\ T_{i,j}^{k-hop,\ unselfish}(t - \Delta t) & \text{if } k > 1 \end{cases} \quad (5)$$

In Equation 5, if node i is within one-hop of node j, i.e., k=1, it can use its own direct observations obtained through monitoring, overhearing and snooping to assess node j. We will explain how to late $T_{i,j}^{1-hop,\ direct,\ unselfish}(t)$ in Section 4. If k>1, node i will use its belief in node j in unselfishness as evaluated at t-Δt, corresponding to the belief of node i toward node j based on past interaction experiences prior to time t, as the basis of direct observations for node i to further evaluate node j at time t. Essentially, this self information is just the trust component probability of node j as evaluated by node i at t-Δt where

Δt is the trust evaluation window.

$T_{i,j}^{k-hop,\ indirect,\ unselfish}(t)$ in Equation 4 is defined as:

$$T_{i,j}^{k-hop,\ indirect,\ unselfish}(t) = \frac{\sum_{m \epsilon V} \left(T_{i,m}^{(i,m)-hop,\ unselfish}(t) \times T_{m,j}^{(m,j)-hop,\ unselfish}(t) \right)}{n_r} \quad (6)$$

In Equation 6, m is a recommender and the notation (i, m)-hop refers to the number of hops separating node i from node m, such that (i, m)-hop + (m, j)-hop = (i, j)-hop = k, and V is a set including the ids of n_r recommender nodes chosen by node i for evaluating node j. These recommender nodes may be just 1-hop away from node i or up to k hops away from node i but they form the set for which node i trusts the most. In practice, V may cover just 1-hop neighbors of node i since node i may trust its one-hop neighbors the most. When a recommender node, say, node m, provides its recommendation to node i for evaluating node j (functional trust), node i's trust on node m (referral trust) is also taken into consideration in the calculation as reflected in the product term on the right hand side of Equation 6. This models the decay of trust as the trust space increases.

An interesting metric is the average "subjective" unselfish trust probability of node j at time t, $T_j^{unselfish}(t)$, as evaluated by all active nodes in the system. It can be calculated by a weighted average of unselfishness trust beliefs from all nodes, i.e.,

$$T_j^{unselfish}(t) = \frac{\sum_{all\ i} (T_{i,j}^{unselfish}(t))}{\sum_{all\ i} 1} \quad (7)$$

We can follow the same formulation to compute the average subjective trust probabilities of the other three trust components, i.e., $T_j^{intimacy}(t)$, $T_j^{healthy}(t)$, and $T_j^{energy}(t)$. Another metric of interest is the overall average trust level of node j, denoted by $T_j^{SQTrust}(t)$, as evaluated by all active nodes. Following Equation 1, $T_j^{SQTrust}(t)$ can be calculated by:

$$T_j^{SQTrust}(t) = w_1 T_j^{intimacy}(t) + w_2 T_j^{healthy}(t) + w_3 T_j^{energy}(t) + w_4 T_j^{unselfish}(t) \quad (8)$$

Alternatively once we obtain $T_{i,j}(t)$ from Equation 1, $T_j^{SQTrust}(t)$ can be computed by:

$$T_j^{SQTrust}(t) = \frac{\sum_{all\ i} T_{i,j}(t)}{\sum_{all\ i} 1} \quad (9)$$

In this paper, we compare $T_j^{SQTrust}(t)$ with the "objective" trust of a node which is calculated based on actual, global information of each node to see how much subjective trust evaluation is from objective trust evaluation. Such objective trust calculations can be obtained by a mathematical model (see Section 4 below) that describes the global behavior exactly so we may ideally calculate the objective trust levels of nodes in the system based on the global knowledge. This serves as the basis for validating SQTrust.

Trust Management vs. Reliability Assessment – We can use $T_j^{SQTrust}(t)$ as an indicator to know if node j satisfies the minimum trust threshold set for a mission execution. More importantly, we could obtain the mission success probability (as a reliability metric) if the application provides some knowledge regarding the "minimum trust level" and "drop dead trust level" for successful mission execution and the amount of time taken for mission completion if a particular node, along with other trusted nodes, is assigned with the mission execution. We consider a mission application for which there are two trust thresholds: M_1 is a minimum trust level required for successful mission completion and M_2 is a drop dead trust level for the system to fail. TR is the deadline for completion for this mission. Suppose we have knowledge regarding the time to complete the mission, i.e., $g(t)$ is the probability density function of the mission execution time (e.g., a uniform distribution from 0 to TR). Note that TR, M_1, and M_2 can be determined based on system requirements. Let $R(t)$ be the system reliability at time t. Then the mission success probability, denoted by $P_{mission}$, is simply the expected system reliability conditioning on the mission execution time, i.e.,

$$P_{mission} = \int_0^{TR} R(t) * g(t) dt \quad (10)$$

where $R(t)$ is zero if $t > TR$. For the special case in which a system failure occurs when node j fails, $R(t)$ is equal to $R_j(t)$, which can be calculated by:

$$R_j(t) = \begin{cases} 0, if\ X_j(t') = 0 \text{ for any } t' \le t \\ E[X_j(t')], t' \le t, \quad \text{otherwise} \end{cases} \quad (11)$$

$$\text{where } X_j(t') = \begin{cases} 1, & if\ T_j^{SQTrust}(t') \ge M_1 \\ 0, & if\ T_j^{SQTrust}(t') < M_2 \\ T_j^{SQTrust}(t')/M_1, & \text{otherwise} \end{cases}$$

Here $X_j(t'), t' \leq t$, is the instantaneous trust degree of nodes j at time t'. One can see that the knowledge of $T_j^{SQTrust}(t)$ is very desirable for computing $P_{mission}$ once we are given knowledge regarding mission execution time distribution, definition of system failure based on trust (e.g., a condition is when a majority of nodes have trust fall below M_2) and the trust requirements for successful mission execution.

4 Performance Model

Our analysis methodology is model-based and hinges on the use of a Stochastic Petri net (SPN) mathematical model for describing "actual" dynamic behaviors of nodes in MANETs in the presence of behaved, selfish and malicious nodes, as well as IDS for detecting malicious nodes. The SPN outputs can provide a global view of the system and can serve as the basis for "objective" trust evaluation. Our goal is to compare "subjective" trust versus "objective" trust obtained through SQTrust to provide a sound theoretical basis for guiding the algorithm design for SQTrust. Once the subjective trust is proven close to the objective trust, we make use of the resulting SPN model outputs to compute the mission success probability ($P_{mission}$ in Equation 10) when given knowledge regarding the mission execution time distribution, the definition of system failure based on trust, and the trust requirements for successful mission execution for mission critical applications.

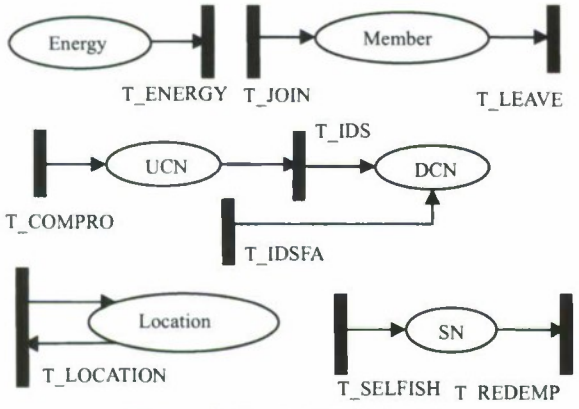


Figure 1: Node SPN Model.

Analytical Modeling based on SPN – We develop a node SPN model as shown in Figure 1 for describing the behavior of a mobile node in the system. The node SPN model describes a single node's lifetime in the presence of other selfish and malicious nodes, as well as IDS for detecting inside attackers. It is used to obtain a single node's information (e.g., intimacy, healthiness, energy, and unselfishness) and to derive the trust relationship with other nodes in the system. It also captures location information of a node as a function of time.

Below we explain how we construct the node SPN model for describing a node's lifetime in terms of its location, energy level, membership, degree of healthiness (e.g., whether or not a node is compromised or/and detected by IDS), and degree of selfishness.

Location: Transition T_LOCATION is triggered when the node moves to a randomly selected area out of four different directions from its current location with the rate calculated as S_{init}/R based on an initial speed (S_{init}) and wireless radio range (R). Depending on the randomly selected location, the number of tokens in place *Location* is adjusted. Without loss of generality, we consider a square-shaped operational region consisting of $M \times M$ sub-grid areas each with the width and height equal to R. Initially for simplicity nodes are randomly distributed over the operational area based on uniform distribution. 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 node SPN model produces the probability that a node is at a particular location at time t, for example, the probability that node i is located in area j at time t. This information along with the location information of other nodes at time t provides the information to a node about its k-hop neighbors at time t, which is important for measuring trust among peers.

Intimacy: A node is intimate to another node when they have a lot of interaction experiences. In MANET environments because of node mobility, two nodes interact with each other when they are physically close by each other particularly in packet routing and forwarding. Thus intimacy can be modeled by the time-averaged probability that two nodes are physically close by each other within radio range over $[t\text{-}d\Delta t, t]$, thus modeling past but recent interaction experiences. Since the node SPN model for a node gives us the probability that the node is in a particular location at time t, we can easily compute this time-averaged probability that two nodes are physically close by each other over $[t\text{-}d\Delta t, t]$ from the two node SPN models associated with the two nodes. Here 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.

Energy: Place *Energy* represents the current energy level of a node. An initial energy level of each node is assigned according to node heterogeneity information. 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 into place *Energy* a number of tokens 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 selfish to save energy or when a node changes its membership from a member to a non-member, 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 transition rate to transition T_COMPRO is modeled as $1/T_{comp}$ with the interval $T_{comp} = (mark(Energy) + 1)/\lambda_{com}$ where λ_{com} is the node compromising rate initially given, and $mark(Energy)$ indicates the level of current energy. In practice, λ_{com} can be derived from first-order approximation of historical attack data. We model the behavior of node compromise such that if the node has low energy, it is more likely to become compromised, and vice versa. If the node is compromised, a token goes to *UCN*, meaning that the node is being compromised but not yet detected by IDS. While the node is not detected by IDS, it has a chance to 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. If a compromised node is being detected by IDS, a token is taken out from *UCN* into *DCN* and the node is evicted immediately through individual rekeying. We model a mobile group equipped with IDS being characterized by false alarm probabilities. A false negative probability (P_{fn}^{IDS}) of IDS is considered in T_IDS which has the rate of $\left(1 - P_{fn}^{IDS}\right)/T_{IDS}$ and a false positive probability (P_{fp}^{IDS}) of IDS is considered in T_IDSFA which has the rate of P_{fp}^{IDS}/T_{IDS}, where T_{IDS} is the IDS executing interval.

Unselfishness: Place *SN* represents whether a node is selfish or not. If a node becomes selfish while forwarding a packet, a token goes to *SN* by triggering T_SELFISH. We consider a mobile group in which a node's selfish behavior is a function of its remaining energy, the mission difficulty and the neighborhood selfishness degree. Specifically, the transition rate to T_SELFISH - is given by:

$$rate(T\_SELFISH) = \frac{f(E_{remain})f(M_{difficulty})f(S_{degree})}{T_{gc}} \quad (12)$$

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 selfishness computed based on the ratio of selfish nodes to unselfish nodes among 1-hop neighbors and T_{gc} is the group communication interval over which a node may decide to become selfish and drop packets. The form $f(x) = \alpha x^{-\epsilon}$ follows the demand-pricing relationship in Economics [4] to model the effect of its argument x on the selfishness behavior, including:

- $f(E_{remain})$: If a node has a higher level of energy, it is less likely to be selfish. This is to consider a node's individual welfare.
- $f(M_{difficulty})$: If a node is assigned to a mission with a high degree of difficulty, it is less likely to be selfish. This is to take global welfare into consideration for achieving a given mission successfully.
- $f(S_{degree})$: If a node has a higher level of selfishness among its 1-hop neighbors, it is less likely to be selfish. This is because a node will contribute to serving to achieve the mission if there are not many healthy nodes around it.

Similarly a selfish node may become unselfish again through transition T_REDEMP. The redemption rate is modeled in a similar way as:

$$rate(T\_REDEMP) = \frac{f(E_{consumed})f(M_{easiness})f(H_{degree})}{\Delta t} \quad (13)$$

where $E_{consumed}$ is the amount of energy consumed as given by $E_{init} - mark(Energy)$, $M_{easiness}$ is the degree of mission easiness, H_{degree} is the degree of unselfishness among 1-hop neighbors and Δt is the trust evaluation window over which a selfish node may decide to become unselfish again. The form $f(x) = \alpha x^{-\epsilon}$ implies the following physical meanings:

- $f(E_{consumed})$: If a node has a higher level of energy already consumed, it is less likely to be redeemed. This means that when a node has low energy, it wants to further save its energy considering its own individual benefit.
- $f(M_{easiness})$: If a node is assigned with an easier mission, it is less likely to be redeemed. An easier mission may not burden the node's neighboring nodes, and thus a selfish node may want to stay being selfish.
- $f(H_{degree})$: If a node has a higher level of unselfishness among its 1-hop neighbors, it is less likely to be redeemed. When a node believes that there are other unselfish nodes to service a given mission, it may stay being selfish to save its energy.

The overall system SPN model consists of a large number of node SPN models, one for each node in the system. To reduce computational complexity, we only run one node SPN model at a time. We develop a novel iterative technique to solve the system SPN model. In the first round of iteration, since there is no

information available about other nodes, each area is assumed to have an equal number of nodes and all nodes are assumed to be healthy, unselfish, and uncompromised. In the second round of iteration, based on the information collected (e.g., numbers of healthy, selfish, or undetected compromised nodes as 1-hop neighbors) from the first round of node SPN models and also the location information, each node knows how many nodes are 1-hop neighbors that can directly communicate with it and their conditions whether they are selfish or compromised, as well as how many n-hop neighbors it has at time t. It then adjusts its conditions of 1-hop neighbors at time t with the outputs obtained from the j^{th} round of iteration as inputs to the $(j+1)^{th}$ round of iteration. This process continues until a specified convergence condition is met. We use the Mean Percentage Difference (MPD) to measure the difference between critical design parameter values, including a node's actual energy level, unselfish probability, and undetected compromised probability at time t in two consecutive iterations. The iteration stops when the MPD is below a threshold (1%) for all nodes in the system. The node SPN models for node i after convergence will produce model outputs allowing *objective* trust evaluation of $T_j^{intimacy}(t)$, $T_j^{healthy}(t)$, $T_j^{energy}(t)$ and $T_j^{unselfish}(t)$.

Objective Trust Evaluation - With the node behaviors modeled by the overall system SPN model described above, the objective trust evaluation of node j, i.e., $T_j^{intimacy}(t)$, $T_j^{healthy}(t)$, $T_j^{energy}(t)$ and $T_j^{unselfish}(t)$ 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 $T_j^X(t) = \sum_{s\in S}(r_s * P_s(t))$ for X = healthiness, energy or unselfishness, and as $T_j^X(t) = \frac{\int_{t-d\Delta t}^{t}\sum_{s\in S}(r_s * P_s(t))dt}{d\Delta t}$ for X = intimacy. Here S indicates the set of states in the underlying semi-Markov chain, $P_s(t)$ is the probability that the system is in state s at time t, and r_s is the reward to be assigned to state s. Table 1 summarizes specific reward assignments used to calculate $T_j^{intimacy}(t)$, $T_j^{healthy}(t)$, $T_j^{energy}(t)$ and $T_j^{unselfish}(t)$ as $T_j^X(t)$.

In Table 1, E_T is the energy threshold below which the trust toward a node in energy goes to the worst trust level. Once objective trust values of node j, i.e., $T_j^{intimacy}(t)$, $T_j^{healthy}(t)$, $T_j^{energy}(t)$ and $T_j^{unselfish}(t)$, are obtained, we can calculate the overall average objective trust value of node j, $T_j^{SQTrust}(t)$, based on Equation 8.

Table 1: Reward Assignments for Objective Trust Evaluation.

Component trust probability toward node j	r_s: reward assignment to state s
$T_j^{intimacy}(t)$	1 *if* $mark(j's\ location)$ *is in a particular area at time* t; 0 *otherwise*
$T_j^{healthy}(t)$	1 *if* $(mark(j's\ DCN) = 0$ & $mark(j's\ UCN) = 0)$; 0 *otherwise*
$T_j^{energy}(t)$	1 *if* $(mark(j's\ Energy) > E_T)$; 0 *otherwise*
$T_j^{unselfish}(t)$	1 *if* $(mark(j's\ SN) = 0$ & $mark(j's\ member) > 0)$; 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
$T_{i,j}^{1-hop,direct,intimacy}(t)$	1 *if* i *and* j *are in the same area within last* $d\Delta t$; 0 *otherwise*
$T_{i,j}^{1-hop,direct,healthy}(t)$	1 *if* $(mark(j's\ DCN) = 0)$; 0 *otherwise*
$T_{i,j}^{1-hop,direct,energy}(t)$	1 *if* $(mark(j's\ Energy) > E_T)$; 0 *otherwise*
$T_{i,j}^{1-hop,direct,unselfish}(t)$	1 *if* $(mark(j's\ SN) = 0$ & $mark(j's\ member) > 0)$; 0 *otherwise*

Subjective Trust Evaluation - Unlike objective trust evaluation, subjective trust evaluation is based on Equations 1-7. The only knowledge a node has about other nodes at time t is the intimacy, energy and unselfishness behaviors of its 1-hop neighbors (but not healthiness which is most likely concealed by a compromised node) through monitoring, overhearing and snooping techniques. For the healthiness trust component, node i knows node j is compromised only when IDS announces the eviction message to the mobile group, i.e., when node j's *DCN* (in Figure 1) becomes nonempty. Thus, we can also easily pute $T_{i,j}^{1-hop,\ direct,\ intimacy}(t)$, $T_{i,j}^{1-hop,\ direct,\ healthy}(t)$, $T_{i,j}^{1-hop,\ direct,\ energy}(t)$ and $T_{i,j}^{1-hop,\ direct,\ unselfish}(t)$ from the SPN model through reward assignments. Table 2 summarizes specific reward assignments used to obtain these subjective trust beliefs. Note that here the probability weighted average reward will need to be calculated from the outputs of the node SPN models for nodes i and j as the trust evaluation is subjective.

In Table 2, Δt is the trust evaluation window. The subjective trust component probabilities at k hops, i.e., $T_{i,j}^{k-hop,intimacy}(t)$, $T_{i,j}^{k-hop,healthy}(t)$, $T_{i,j}^{k-hop,energy}(t)$, and $T_{i,j}^{k-hop,unselfish}(t)$, can then be obtained through Equation 4 which is applied recursively through Equ-

ations 5 and 6. Then the subjective trust evaluation of node j, i.e., $T_j^{intimacy}(t)$, $T_j^{healthy}(t)$, $T_j^{energy}(t)$ and $T_j^{unselfish}(t)$ can be calculated through Equation 7, and, subsequently, the overall average subjective trust value of node j, $T_j^{SQTrust}(t)$, can be obtained through Equation 8. This last quantity is to be compared with that obtained through objective trust evaluation discussed above as the basis for validating the design of SQTrust. It should be noted that a node that is detected compromised by IDS will be evicted and the eviction decision will be made known to all nodes by the mobile group. Therefore, there is no need for node i to do peer-to-peer subjective trust evaluation toward node j based on $T_{i,j}(t)$ after learning that node j has been evicted at time t.

5 Evaluation Results

In this section, we show numerical data resulting from subjective trust evaluation based on SQTrust and compare the results obtained from objective trust evaluation.

Table 3: Default Parameter Values Used.

Parameter	Value	Parameter	Value
$M \times M$	6×6	R	250m
α	1	M_1:M_2	0.85:0.55
ε	1.2	n	5
β_1:β_2	Variable	d	2
w_1, w_2, w_3, w_4	0.25	$P_{fn}^{IDS}, P_{fp}^{IDS}$	0.5%
TR	Variable	$1/\lambda_{com}$	8400s
S_{init}	(0, 2] m/s	Δt	1200s
T_{gc}	120s	E_{init}	[12, 24] hrs
T_{IDS}	600s	E_T	0 hrs
$g(t)$	*uniform distribution* over [0, TR]		

Table 3 lists the default parameter values used. We populate a MANET with 150 nodes moving randomly in 6×6 operational areas, with each area covering 250m radio radius. We use all 1-hop neighbors as the recommenders for indirect trust evaluation. The environment being considered is assumed hostile and insecure with the compromising rate set to once per 140 minutes. When a node turns malicious, it performs good-mouthing and bad-mouthing attacks, i.e., it will provide the highest trust recommendation toward a bad node to facilitate collusion, and conversely the lowest trust recommendation toward a good node to ruin the reputation of the good node. When a malicious node is detected by the IDS, the trust level of the malicious node drops to zero, thereby nullifying its good-mouthing and bad-mouthing attacks. The initial trust level is set to 1 for healthiness, energy and unselfishness because all nodes are considered trustworthy initially. The initial trust level of intimacy is set to the probability that another node is found in the same location in accordance with the intimacy definition.

We vary the values of important parameters such as β_1: β_2 (with higher β_1 meaning more direct observations or self-information being used for subjective trust evaluation), w_1:w_2:w_3:w_4 (the weight ratio for the 4 trust components considered), M_1 and M_2 (the minimum trust level and drop-dead trust level), and TR (the mission completion deadline) to test the sensitivity of the results with respect to these design parameters.

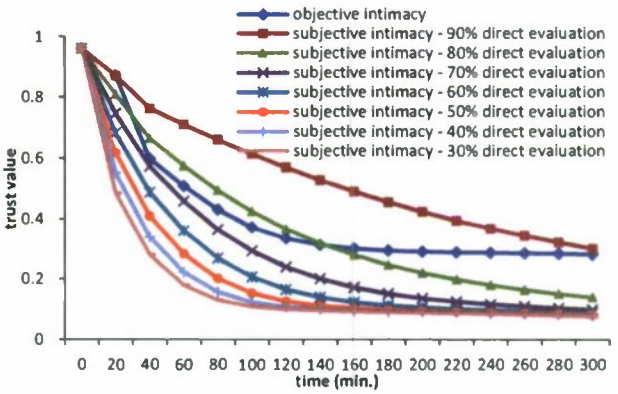


Figure 2: Intimacy Evaluation.

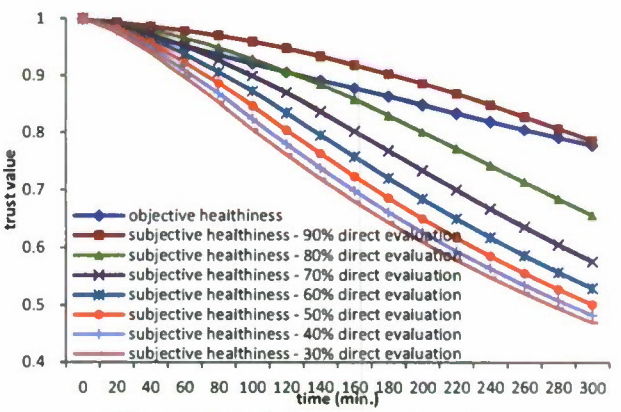


Figure 3: Healthiness Evaluation.

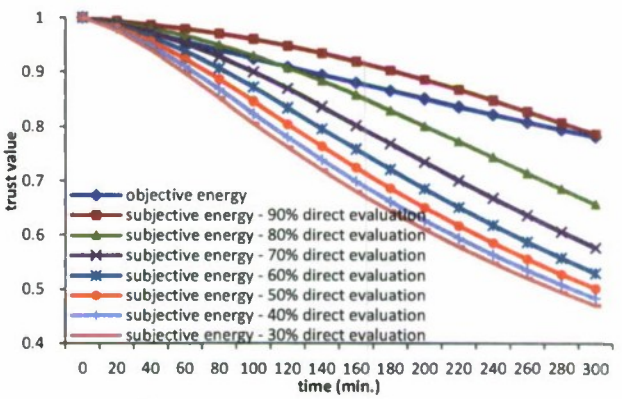


Figure 4: Energy Evaluation.

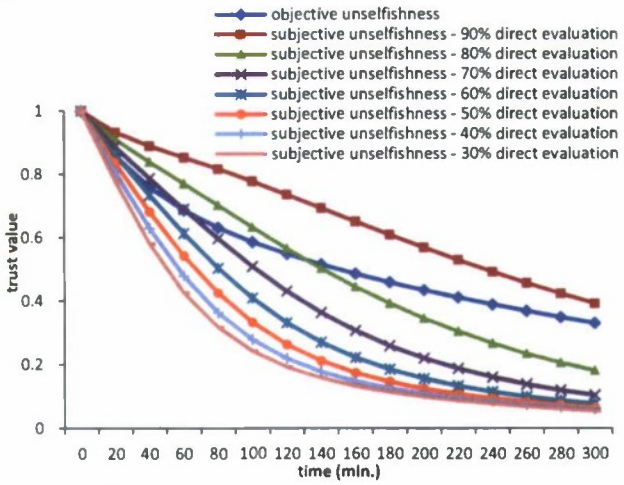


Figure 5: Unselfishness Evaluation.

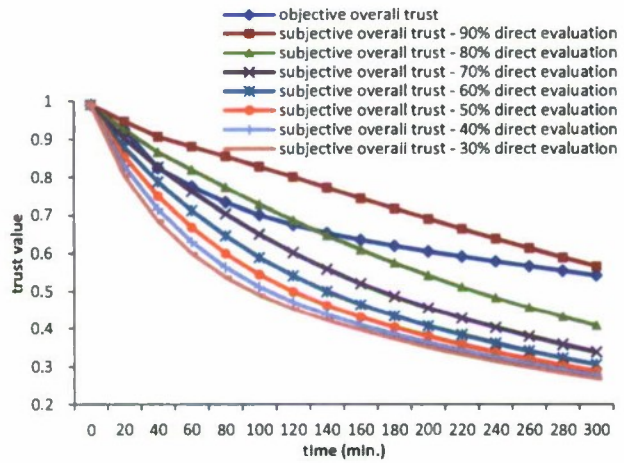


Figure 6: Overall Trust Evaluation.

To reveal which trust component might have a more dominant effect, we show individual trust component values, i.e., $T_j^{intimacy}(t)$, $T_j^{healthy}(t)$, $T_j^{energy}(t)$ and $T_j^{unselfish}(t)$ for a node randomly picked. Other nodes exhibit similar trends and thus only one set of results is shown here. Figures 2-5 show the node's trust values as a function of mission execution time for intimacy, healthiness, energy and unselfishness, respectively, with β_1: β_2 varying from 0.3: 0.7 (30% direct evaluation: 70% indirect evaluation) to 0.9: 0.1 (90% direct evaluation: 10% indirect evaluation). We see that for all 4 trust components, 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 75%) after which subjective trust evaluation overshoots. This indicates that using too much direct observations for subjective trust evaluation may 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.

Figure 6 shows the node's overall trust values obtained from subjective trust evaluation vs. objective trust evaluation, also as a function of time. We observe that the subjective trust evaluation curve is reasonably close to the objective trust evaluation curve, but again there is a cutoff point after which SQTrust overestimates trust compared to objective trust. Nevertheless, Figures 2-6 demonstrate that subjective trust evaluation results can be very close to objective trust evaluation results when the right amount of direct observations is used for subjective trust evaluation.

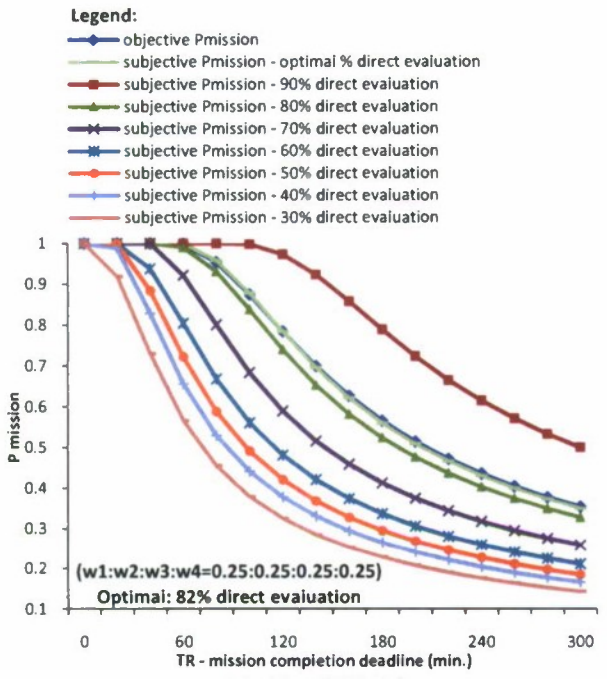
6 Effect of Trust Management on Reliability

To demonstrate the effect of subjective trust evaluation on the reliability of mission-oriented mobile groups in MANETs, we turn our attention to the mission success probability defined by Equation 10. We consider an 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 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 $[t, t+\Delta t]$ so that if any one node selected fails, the mission fails. We can then apply Equations 10 and 11 to compute $P_{mission}$ over an interval $[t, t+\Delta t]$. 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 $[0, \Delta t]$, $[\Delta t, 2\Delta t]$, ..., $[TR-\Delta t, TR]$.

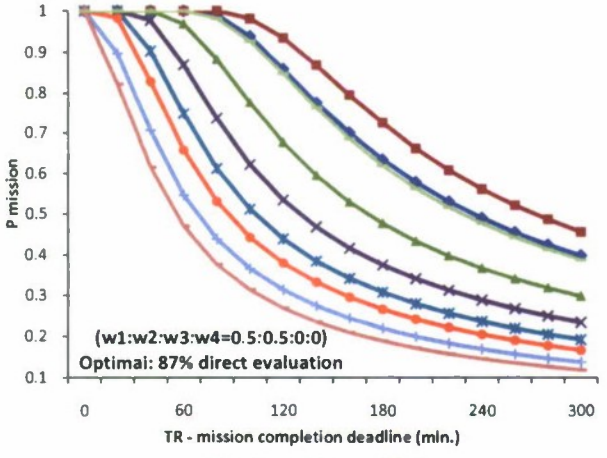
Figure 7 shows the mission success probability $P_{mission}$ as a function of TR. To examine the effect of $w_1:w_2:w_3:w_4$ (the weight ratio for the 4 trust components considered in this paper), we consider 5 test cases: (a) *equal-weight*, (b) *social trust only*, (c) *QoS trust only*, (d) *more social trust*, and (e) *more QoS trust* as listed in Table 4.

Table 4: Test Cases for Weight Ratio.

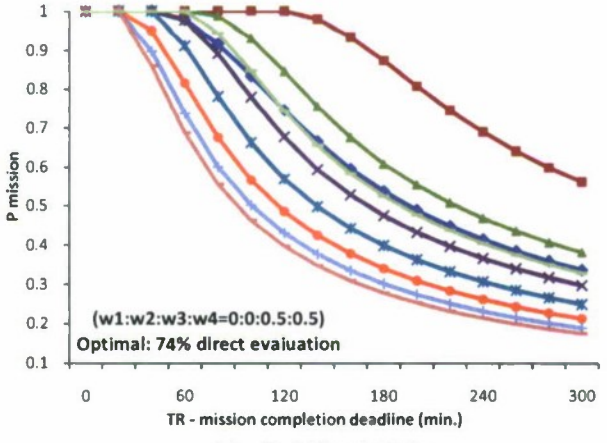
Test case	Weight ratio
Equal-weight	$w_1:w_2:w_3:w_4 = 0.25:0.25:0.25:0.25$
Social trust only	$w_1:w_2:w_3:w_4 = 0.5:0.5:0:0$
QoS trust only	$w_1:w_2:w_3:w_4 = 0:0:0.5:0.5$
More social trust	$w_1:w_2:w_3:w_4 = 0.35:0.35:0.15:0.15$
More QoS trust	$w_1:w_2:w_3:w_4 = 0.15:0.15:0.35:0.35$



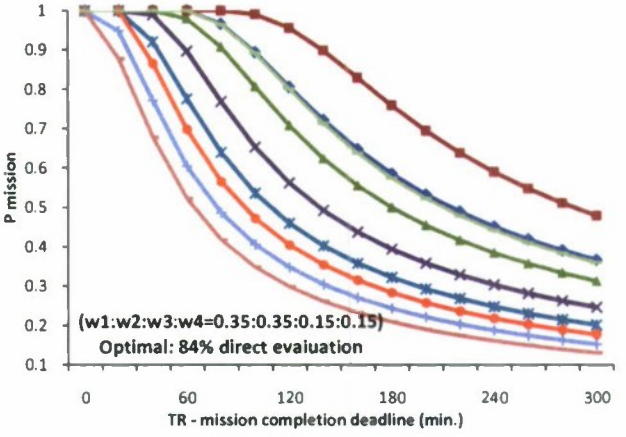
(a) Equal-Weight.



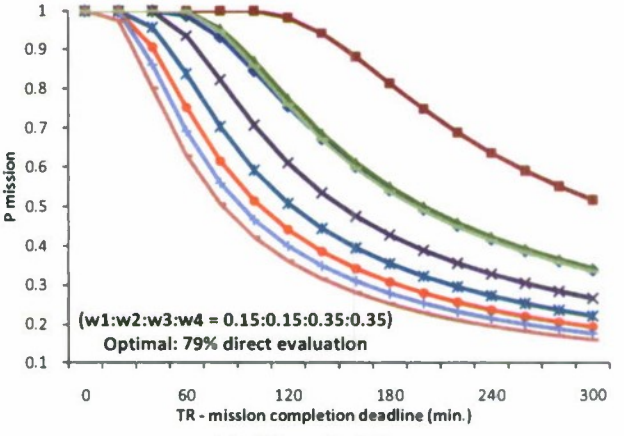
(b) Social Trust Only.



(c) QoS Trust Only.



(d) More Social Trust.



(e) More QoS Trust.

Figure 7: Mission Success Probability: Subjective vs. Objective Evaluation.

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 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.

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 bringing subjective $P_{mission}$ closer to objective $P_{mission}$, and there is a cutoff point after which subjective trust evaluation overshoots.

Figure 7 demonstrates the effectiveness of SQTrust. We see that the mission success probability as a result of executing subjective trust evaluation is very close to that from objective trust evaluation, especially when we use more but not excessive direct observations for subjective trust evaluation. When given a mission context 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 (i.e., β_1: β_2) to be used for subjective trust evaluation, so that SQTrust can be fine-tuned to yield results close to those by objective trust evaluation based on actual knowledge of node status.

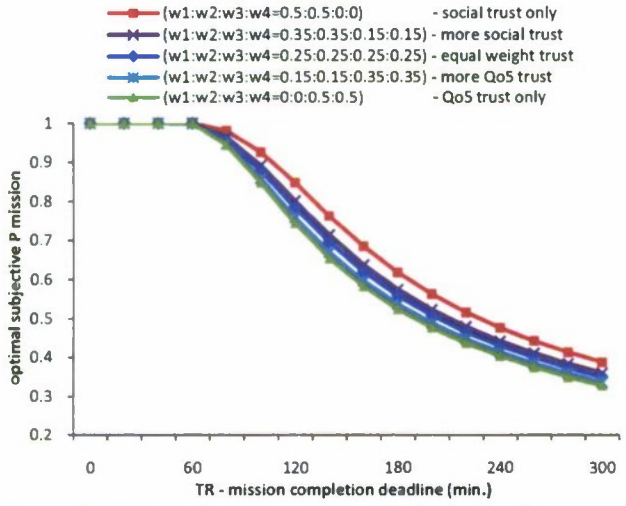


Figure 8: Effect of w_1: w_2: w_3: w_4 on Mission Success Probability.

In Figure 8 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 optimal β_1:β_2 ratio so that 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 selfishness). Certainly, this result should not be construed as universal. When given a mission context characterized by a set of model parameter values defined in Table 3, the model-based analysis methodology developed in this paper helps identify the best w_1: w_2: w_3: w_4 ratio to be used to maximum the system reliability.

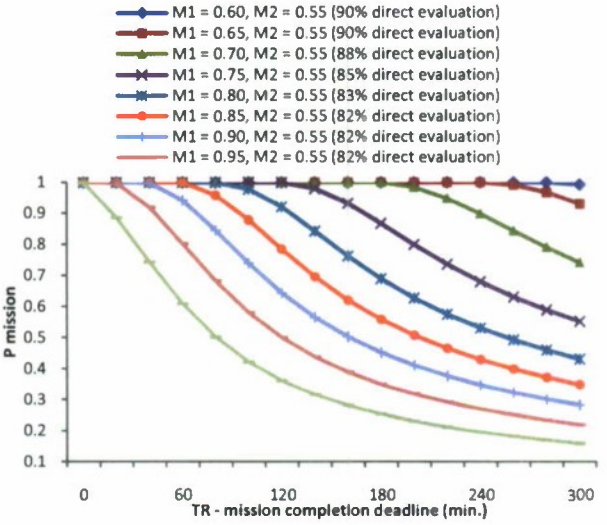


Figure 9: Effect of M1 on Mission Success Probability.

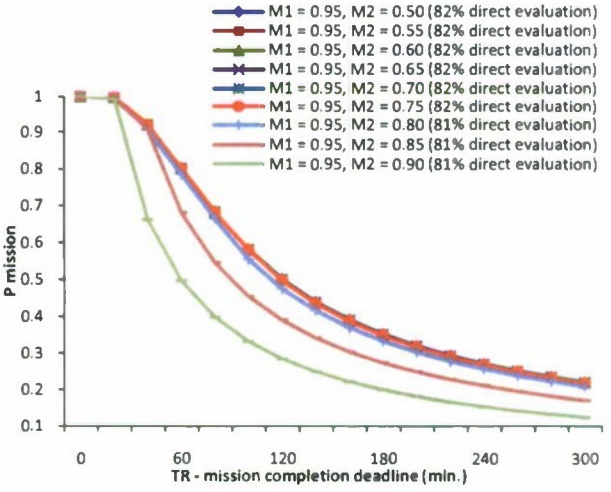


Figure 10: Effect of M_2 on Mission Success Probability.

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 9 and 10 show $P_{mission}$ vs. TR for the system operating under optimal w_1: w_2: w_3: w_4 and β_1:β_2 settings for each (M_1, M_2) combination. Recall that M_1 and M_2 represent the belief if a node is considered trustworthy for mission execution. From Figure 9, 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 10, 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.

7 Conclusion

In this paper we have 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 model-based methodology based on SPN techniques for describing the behavior of a mobile group consisting of behaved, malicious and selfish nodes. By applying an iterative technique for solving the large SPN model, we allow the *objective* trust values of nodes to be calculated based on global knowledge regarding status of nodes as time progresses, which serves as the basis for performance evaluation against SQTrust. We demonstrated that SQTrust is able to provide subjective trust evaluation results close to 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, verified by the exact match between subjective mission success probability and objective mission success probability. Finally, we analyzed the effects of key design parameters such as β_1: β_2 (with higher β_1 meaning more direct observations or self-information being used for subjective trust evaluation), w_1: w_2: w_3: w_4 (the weight ratio for the 4 trust components considered), M_1 and M_2 (the minimum trust level and drop-dead trust level), and TR (the mission completion deadline) on the system reliability of a mission-oriented mobile group and provided guidelines for fine-tuning these parameters so as to maximize the system reliability.

In the future, we plan to extend SQTrust to apply to wireless sensor actuator networks with a hierarchical infrastructure, and we plan to investigate a class of mission-critical applications which can benefit from subjective trust evaluation protocols that consider both social and QoS trust such as SQTrust developed in this paper.

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," *Proc. 6th Annual IEEE SMC Information Assurance Workshop*, June 2005, West Point, NY, pp. 317-324.

[2] 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, 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, Lecture Notes in Computer Science*, Samos, Greece, vol. 4347, Aug. 2006, Springer, 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," *Proc. 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," *Proc. 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," *Proc. Int'l Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, Vancouver, British Columbia, 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, May 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*, accepted to appear, 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] T. Ghosh, N. Pissinou, and K. Makki, "Towards Designing a Trust Routing Solution in Mobile Ad Hoc Net-

works," *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, Aug. 2006, pp. 1-7.

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

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

[18] A. Josang and S. Pope, "Semantic Constraints for Trust Transitivity," *Proc. 2nd Asia-Pacific Conf. on Conceptual Modeling*, Newcastle, Australia, 2005.

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

[20] 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*, Suzhou, China, May 2004, pp. 80-85.

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

[22] 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.

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

[24] 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.

[25] 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.

[26] 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.

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

[28] 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.

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