Ad Hoc Networks 19 (2014) 59–74

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Trust management in mobile ad hoc networks for bias minimization and application performance maximization

Ing-Ray Chen [a],*, Jia Guo [a], Fenye Bao [a], Jin-Hee Cho [b]

[a] Department of Computer Science, Virginia Tech, United States
[b] Computational and Information Sciences Directorate, U.S. Army Research Laboratory, United States

ARTICLE INFO

Article history:
Received 19 August 2013
Received in revised form 21 January 2014
Accepted 17 February 2014
Available online 26 February 2014

Keywords:
Trust management
Mobile ad hoc networks
Trust bias minimization
Model-based analysis
Application-level trust optimization
Reliability assessment

ABSTRACT

Trust management for mobile ad hoc networks (MANETs) has emerged as an active research area as evidenced by the proliferation of trust/reputation protocols to support mobile group based applications in recent years. In this paper we address the performance issue of trust management protocol design for MANETs in two important areas: trust bias minimization and application performance maximization. By means of a novel model-based approach to model the ground truth status of mobile nodes in MANETs as the basis for design validation, we identify and validate the best trust protocol settings under which trust bias is minimized and application performance is maximized. We demonstrate the effectiveness of our approach with an integrated social and quality-of-service (QoS) trust protocol (called SQTrust) with which we identify the best trust aggregation setting under which trust bias is minimized despite the presence of malicious nodes performing slandering attacks. Furthermore, using a mission-oriented mobile group utilizing SQTrust, we identity the best trust formation protocol setting under which the application performance in terms of the system reliability of the mission-oriented mobile group is maximized.

1. Introduction

The concept of "trust" originally derives from social sciences and is defined as the subjective degree of a belief about the behaviors of a particular entity. 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." Many researchers in the networking and communication field have defined trust differently such as "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 [5,31,34,37], key management [9,18], authentication [29], access control [1], and intrusion detection [2,20,23,38,49].

Trust management for mobile ad hoc networks (MANETs) (see [10,48] for a very recent survey of the topic) has emerged as an active research area as evidenced by the proliferation of trust/reputation protocols [2,3,5,6,8–10,14–16,18,19,25–27,29,31,34,35,40,48,50,57–63,72,76,77] to support mobile group based applications in recent years. Untreated in the literature [10,48], in this paper we address the performance issue of trust management protocol design for MANETs in two important areas: trust bias minimization and application performance maximization.

* Corresponding author. Address: Department of Computer Science, Virginia Tech, 7054 Haycock Road, Falls Church, VA 22043, United States. Tel.: +1 (703) 538 8376; fax: +1 (703) 538 8348.

E-mail addresses: irchen@vt.edu (I.-R. Chen), jiaguo@vt.edu (J. Guo), baofenye@vt.edu (F. Bao), jinhee.cho@us.army.mil (J.-H. Cho).

http://dx.doi.org/10.1016/j.adhoc.2014.02.005
1570-8705/© 2014 Elsevier B.V. All rights reserved.

Relative to existing works for MANET trust management cited above, this paper has the following specific 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*. A mobile ad hoc group very frequently comprises human operators carrying communication devices. Thus, in addition to traditional *QoS trust* metrics such as control packet overhead, throughput, packet dropping rate, delay, availability and fault tolerance, one must also consider *social trust* metrics [42] including friendship, honesty, privacy, similarity, betweenness centrality and social ties [12,13] for trust management. We note that prior works such as [12,13,17,20,39,41,44] also considered social trust metrics in communication networks. Our work distinguishes itself from these prior works in that we identify the best *trust aggregation* parameter settings for each individual trust metric (either QoS or social) to minimize trust bias.
- Second, we propose a novel 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 the ground truth against which subjective trust values obtained from executing SQTrust can be compared for validation. Our analysis methodology hinges on the use of Stochastic Petri Net (SPN) modeling techniques [30,36,64–68,73–75] for describing the "actual" dynamic behaviors of nodes in MANETs in the presence of well-behaved, uncooperative and malicious nodes. With this methodology, we identify the optimal trust parameter settings under which SQTrust is most accurate compared with global knowledge and actual node status.
- Finally, we consider a new design concept of *application-level trust optimization* by identifying the best way to form the overall trust out of individual social and QoS trust metrics to maximize application performance. Using a mission-oriented mobile group utilizing SQTrust, we identity the best trust formation protocol setting under which the application performance in terms of the system reliability of the mission-oriented mobile group is maximized.

The rest of the paper is organized as follows. Section 2 describes the system model and assumptions. Section 3 describes SQTrust and explains how it is executed by each node to perform peer-to-peer subjective trust evaluation. Section 4 develops a novel model-based approach to describe dynamic behaviors of nodes in MANETs in the presence of misbehaving nodes with the objective to yield objective trust against which subjective trust from executing SQTrust may be compared for trust bias minimization, including overhead analysis and an application scenario involving a lead node dynamically selecting a number of nodes it trusts most for mission execution for reliability maximization. Section 5 presents analytical results with physical interpretations given. Section 6 presents simulation results for simulation validation. Section 7 discussed related work so as to differentiate our work from existing work and identity unique features and contributions of our trust protocol design for MANETs. Section 8 discusses applicability. Finally, Section 9 summarizes the paper and outlines future research areas.

2. System model

2.1. 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.

2.2. SQTrust design goals

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 satisfy and validate the following two design goals:

- 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.

2.3. 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. Also, mission successful execution is the ultimate goal and means for performance evaluation, so if a mission has a high degree of difficulty, a node tends to be cooperative. In our protocol design, each node (node i) keeps a peer-to-peer trust value in cooperativeness $T_{i,j}^{cooperativeness}$ toward another node (node j) in the same mobile group. With trust bias minimization in effect, $T_{i,j}^{cooperativeness}$ is close to the actual status. Thus, a node can simply use its pee-to-peer subjective cooperativeness trust toward its neighbors to determine if it can conserve energy or not. If a node sees it being a bridge node connecting other nodes in the same mobile group, then it satisfies the 'global welfare' condition for it to be cooperative, because otherwise the mobile group it is a part of will be partitioned into 2.
- A node's vulnerability is reflected by a compromised rate, e.g., a capture by attackers after which the node is compromised. After a node is compromised, we assume it attacks persistently. That is, it attacks whenever it has a chance. More sophisticated attacks such as random and opportunistic attacks [49,53–56] are not considered in this work.
- 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, as it persistently performs attacks which consume energy.
- 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.

2.4. 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 node being the lead node 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. SQTrust – A multi-trust protocol for MANETs

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

3.1. Trust composition

Taking into consideration of the proliferation of mobile devices carried by humans in social ad hoc networks, our trust metric consists of two trust types: *social trust* [42] and *QoS trust* [10]. Social trust is evaluated through interaction experiences in 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 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, given a sufficient contact time, 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. When a monitoring node (node *i*) cannot properly monitor a trustee node (node *j*) because of a short contact time, it adapts to this situation by discarding the current monitoring result and instead updating direct trust by its past direct trust toward node *j* decayed over the time interval Δt to model trust decay over time. 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.

3.2. Trust aggregation

A unique feature of our trust aggregation protocol design is that we discover and apply the optimal trust parameter settings to minimize trust bias, i.e., minimizing the difference between *subjective trust* and *objective trust*. Here we define specific trust parameters used in our trust aggregation protocol design. Later in Section 5.2 we leverage a novel model-based approach developed in this paper to discover the best trust aggregation protocol settings to minimize trust bias.

Like most trust aggregation protocols for MANETs [10], we consider both direct trust and indirect trust. That is, 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 are indirect evidences given to node *i* by a subset of 1-hop neighbors selected based on two mechanisms against slandering attacks: (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*.

Summarizing above, node *i* will compute its trust toward node *j*, $T_{i,j}^{X}(t)$, where *X* is a trust component by:

$$T_{i,j}^{X}(t) = \beta_1 T_{i,j}^{direct,X}(t) + \beta_2 T_{i,j}^{indirect,X} \quad (1)$$

In Eq. (1), 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 $\beta_1 + \beta_2 = 1$.

The direct trust part, $T_{i,j}^{direct,X}(t)$, in Eq. (1) is evaluated by node *i* at time *t* depending on if node *i* is a 1-hop neighbor of node *j* at time *t* and if the data needed by node *i* for assessing *X* of node *j* is obtainable during $[t - d\Delta t, t]$. If yes, then node *i* uses its direct observations toward node *j* to update $T_{i,j}^{direct,X}(t)$ where Δt is the periodic trust evaluation interval. Otherwise, node *i* 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 $T_{i,j}^{direct,X}(t)$ Specifically, node *i* will compute $T_{i,j}^{direct,X}(t)$ by:

$$T_{i,j}^{direct,X}(t) = \begin{cases} T_{i,j}^{1-hop,X}(t) \text{ if } i \text{ is a neighbor to } j \text{ at } t \\ \qquad\qquad \text{and data needed is obtainable} \\ e^{-\lambda_\Delta t} \times T_{i,j}^{direct,X}(t - \Delta t) \text{ otherwise} \end{cases} \quad (2)$$

Here we note that $T_{i,j}^{direct,X}(t)$ replaces $T_{i,j}^{direct,X}(t - \Delta t)$ after the computation. So there will not be a storage overflow problem. 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 $T_{i,j}^{1-hop,X}(t)$ here refers to the new "direct" trust assessment at time *t*. We adopt the Bayesian trust/reputation model [21,43] with the Beta (*A*, *B*) distribution such that $A/(A + B)$ is the estimated direct trust toward a node with A as the number of positive service experiences and *B* as the number of negative service experiences. Below we describe specific detection mechanisms by which node *i* collects direct observations to assess $T_{i,j}^{1-hop,X}(t)$ for the case in which *i* and *j* are 1-hop neighbors at time *t*.

- $T_{i,j}^{1-hop,intimacy}(t)$: Intimacy is for measuring social ties and has a lot to do with if two nodes have a lot of direct or indirect interaction experiences with each other. Since friendship and social circle information is frequently not available in MANET environments, $T_{i,j}^{1-hop,intimacy}(t)$ can be computed based on node *i*'s direct interaction experience toward node *j*. Specifically, it is computed by node *i* by the proportion of time nodes *i* and *j* are 1-hop neighbors directly interacting with each other during $[t - d\Delta t, t]$. Note that intimacy is about node *i*'s interaction experience with only node *j*. It is orthogonal to other trust properties such as healthiness, energy or cooperativeness introduced below.
- $T_{i,j}^{1-hop,healthiness}(t)$: This refers to the belief of node *i* that node *j* is honest (or not malicious) based on node *i*'s direct observations during $[t - d\Delta t, t]$. Node *i* estimates $T_{i,j}^{1-hop,healthiness}(t)$ 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., $T_{i,j}^{1-hop,healthiness}(t) = 0$. 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_{fn}^{H}) of misidentifying an unhealthy node as a healthy node, and a false positive probability (P_{fp}^{H}) of misidentifying a healthy node as an unhealthy node.

- $T_{i,j}^{1-hop,energy}(t)$: This is the belief of node *i* that node *j* is competent or capable (in terms of energy status) of performing prescribed protocol functions. Node *i* uses the ratio of the number of acknowledgement packets received from node *j* (at the MAC layer) over transmitted packets to node *j* during $[t - d\Delta t, t]$ to estimate energy capability in node *j*. Here we note that if node *j* acknowledges every packet sent from node *i* to node *j*, $T_{i,j}^{1-hop,energy}(t) = 1$. So it will not penalize a socially active node.
- $T_{i,j}^{1-hop,cooperativeness}(t)$: 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 $T_{ij}^{1-hop,cooperativeness}(t)$ 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.

Although $T_{i,j}^{1-hop,energy}(t)$ and $T_{i,j}^{1-hop,cooperativeness}(t)$ above are measured based on behavior exhibited during protocol execution, they refer to very distinct trust concepts. The first, energy trust, is about if node *j* is *competent* in executing protocol functions, measured by if node *j* is capable of responding to node *i*'s requests, while the second, cooperativeness trust, is about if node *j* is *protocol compliant*, measured by observing if node *j* follows the prescribed protocol execution sequence.

The indirect trust part, $T_{i,j}^{indirect,X}(t)$ in Eq. (1) 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 $T_{i,j}^{indirect,X}(t)$ by:

$$T_{i,j}^{indirect,X}(t) = \begin{cases} \frac{\sum_{mV}\left(T_{i,m}^{X}(t)\times T_{m,j}^{direct,X}(t)\right)}{n_r} & \text{if } n_r > 0 \\ e^{-\lambda_d t} \times T_{i,j}^{indirect,X}(t - \Delta t) & \text{if } n_r = 0 \end{cases} \tag{3}$$

In Eq. (3), the trustor node (node *i*) first selects n_r recommenders (node *m*'s) with which it trusts the most in trust component *X* among its one-hop neighbors and then requests these recommenders to send their recommendations. A recommender (node *m*) provides its direct trust in *X* toward node *j* (the trustee node), $T_{m,j}^{direct,X}(t)$, as a recommendation to node *i* through one-hop communication. *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 $T_{i,m}^{X}(t)$ in trust component *X* is higher than a minimum threshold denoted by T_t^X. 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 Eq. (3). This accounts for trust decay over space. If n_r = 0 then $T_{i,j}^{indirect,X}(t) = e^{-\lambda_d \Delta t} \times T_{i,j}^{indirect,X}(t - \Delta t)$ to account for trust decay over time.

3.3. Trust formation

In this section we define trust parameters used for our trust formation protocol design. Later in Section 5.3 we discuss how the system can discover and apply the best trust formation parameters to maximize application performance, given the operational profile as input.

While many trust formation models exist [10], we adopt the importance-weighted-sum model with which trust is an importance-weighted sum of social trust and QoS trust. It encompasses more-social-trust, more-QoS-trust, social-trust-only, and QoS-trust-only in trust formation. It is particularly applicable to missions where context information is available about the importance of social or QoS trust properties for successful mission execution. For example, for a mission consisting of unmanned mobile nodes, the more-QoS-trust or QoS-trust-only trust formation model will be appropriate. The *subjective trust* value of node *j* as evaluated by node *i* at time *t*, denoted as $T_{i,j}(t)$, thus 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:

$$T_{i,j}(t) = \sum_X w^X \times T_{i,j}^X(t) \tag{4}$$

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:w_2:w_3:w_4 for $w^{intimacy}$:$w^{healthiness}$:w^{energy}:$w^{cooperativeness}$ for notational convenience. For a trust-based application, the best setting of w_1:w_2:w_3:w_4 exists to maximize the application performance. Our model-based analysis allows the best weight setting to be determined, given the operational profile as input. In this paper, we shall demonstrate this with a MANET mobile group application.

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, $T_{i,j}(t) = e^{-\lambda_d \Delta t} \times T_{i,j}(t - t)$.

An interesting metric is the overall average "subjective" trust level of node *j*, denoted by $T_j^{sub}(t)$, as evaluated by all active nodes. Once we obtain $T_{i,j}(t)$ from Eq. (4), $T_j^{sub}(t)$ can be computed by:

$$T_j^{sub}(t) = \frac{\sum_{alli\neq j} T_{i,j}(t)}{\sum_{alli\neq j} 1} \quad (5)$$

In this paper, we compare $T_j^{sub}(t)$ with the "objective" trust of node j, denoted by $T_j^{obj}(t)$, calculated based on actual, global information to see how much deviation subjective trust evaluation is from objective trust evaluation. Specifically, let $T_j^{obj,X}(t)$ 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). Then, following Eq. (4), $T_j^{obj}(t)$ is calculated by:

$$T_j^{obj}(t) = \sum_X w^X \times T_j^{obj,X}(t) \quad (6)$$

By means of a novel mathematical model 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 identifying SQTrust protocol settings for minimizing trust bias as well as for validating SQTrust design.

3.4. Trust protocol computational and communication overhead

In our protocol design, a trustor node (node i) performs direct trust update periodically in every Δt interval according to Eq. (2). Then it selects n_r recommenders among its one-hop neighbors (if any exists) and requests these recommenders to send their recommendations through 1-hop communication to perform indirect trust update according to Eq. (3). Lastly, it merges direct and indirect trust in accordance with Eq. (1) to update its trust towards a trustee node (node j). The computational and communication complexity of SQTrust is therefore $O(N \times n_r/\Delta t)$ where N is the number of nodes in the MANET, n_r is the number of recommenders for indirect trust recommendations in Eq. (3), and Δt is the trust update interval. The communication cost is normalized with respect to one-hop communication cost, as each trustor node only solicits 1-hop neighbors to provide indirect trust recommendations. For the same reason, the number of recommenders n_r also is substantially smaller than N, especially the recommenders must satisfy the *threshold-based filtering* and *relevance-based trust* selection criteria proposed in our protocol design. The computational complexity of finding the best protocol settings in response to dynamically changing environments is O(1) (see Section 8 for more detail). Therefore, the computational and communication overhead for executing SQTrust to minimize trust bias and maximize application performance by individual nodes is at most polynomial in N and very manageable.

3.5. Mission-oriented mobile group applications

To illustrate our *application-level trust optimization* design concept, we consider mission-oriented mobile groups as an application of SQTrust. A lead node (which could be any behaving node in the system) wants to assemble and dynamically manage a mobile task group to achieve a mission assigned despite failure, disconnection or compromise of member nodes. This lead node, say node i, can use $T_{i,j}(t)$ based on its own view towards node j as an indicator to judge if node j satisfies the mission-specific trust requirements for successful mission execution. This node likes to estimate the mission success probability as a mission reliability metric when given knowledge regarding the mission failure definition, member failure definition and mission time. Here we note that the mission reliability metric is measured from the lead node's perspective and presumably the lead node is not a malicious node, or the mission reliability is simply zero.

Let $R(t)$ be the mission reliability given that the mission time is t. Then, the mission success probability, denoted by $P_{mission}$, from the lead node's perspective is simply $R(TR)$ when the lead node is given TR as the mission time, i.e.,

$$P_{mission} = R(TR) \quad (7)$$

The *mission failure definition* is application dependent. 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. Let J be a set of members with range $[k, n]$. Then,

$$R(t) = \sum_{|J|\geqslant k} \left(\prod_{j\in J} R_j(t) \prod_{j\notin J} (1 - R_j(t)) \right) \quad (8)$$

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.

Let $X_j(t)$ be the *instantaneous trustworthiness* of node j at time t. If at any time t, node j's trust level is above M_1 then node j is completely trustworthy, so its *instantaneous trustworthiness* $X_j(t)$ 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. Specifically, the *instantaneous trustworthiness* of node j at time t is given by:

$$X_j(t) = \begin{cases} 1, & \text{if } T_{i,j}(t) \geqslant M_1 \\ 0, & \text{if } T_{i,j}(t) < M_2 \\ T_{i,j}(t)/M_1, & \text{otherwise} \end{cases} \quad (9)$$

The lead 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 $t' \leqslant t, X_j(t') = 0$,then the trust level of node j is not acceptable, so $R_j(t)$ is 0; otherwise, $R_j(t)$ is the average trust value of node j over [0, t] computed by the expected value of $X_j(t')$, $0 \leqslant t' \leqslant t$, over [0, t]. Summarizing above, node i computes member j's reliability $R_j(t)$ by:

$$R_j(t) = \begin{cases} 0, if\ X_j(t') = 0 \text{ for any } t' \leqslant t \\ E[X_j(t')], t' \leqslant t, \text{ otherwise} \end{cases} \quad (10)$$

Here $X_j(t')$ is the instantaneous trustworthiness of node j at time t' defined by Eq. (9) and $E[X_j(t')]$ is the expected value of $X_j(t'), 0 \leqslant t' \leqslant t$, over [0, t]. One can see that the knowledge of $T_{i,j}(t)$ is very desirable for the lead node to compute $P_{mission}$ given knowledge regarding the mission execution time, member failure definition, and mission failure definition.

4. Analytical 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 yield "objective" trust against which "subjective" trust obtained through protocol execution can be compared for identifying optimal protocol settings to minimize trust bias and to maximize application performance.

4.1. Node SPN for modeling node behavior

We consider a square-shaped operational area consisting of $M \times M$ regions each with the width and height equal to radio radius R. The node mobility model is specified as part of the operational profile. Fig. 1 illustrates 3 nodes moving in a 6 × 6 regions. The regions are given location identifiers from 1 to 36 in top–bottom and then left–right order, as illustrated in Fig. 1. To avoid end-effects, movement is wrapped around (i.e., a torus is assumed). Two nodes are within 1-hop if there are in the same region or in neighbor regions.

Fig. 2 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.

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.

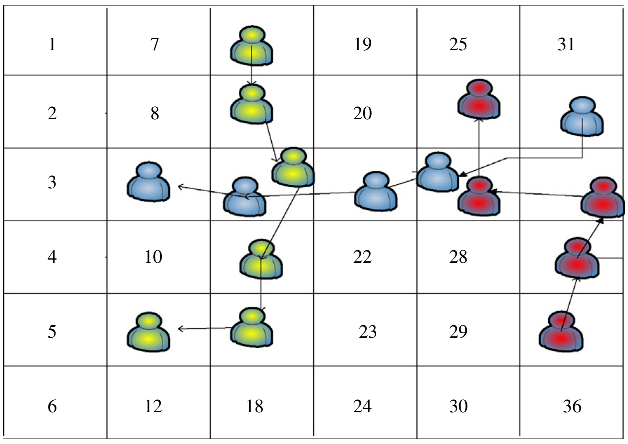


Fig. 1. Nodes moving in a 6 × 6 grid based on their operational profiles.

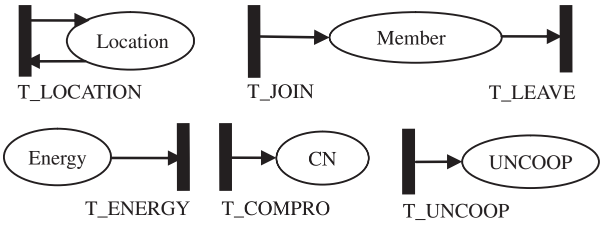


Fig. 2. Node SPN model.

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. For example in Fig. 1 after user 1 (in green color) moves from region 17 to region 11, place *Location* will flush out 17 tokens originally there and hold 11 tokens afterward. 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.

4.2. 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 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. 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*.

4.3. 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 $T_{i,j}^{1\text{-}hop,intimacy}(t)$ (see Eq. (2) 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*.

4.4. 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 and 24 h 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 (assuming persistent attack behavior) and consumes energy more. Therefore, depending on the node's status, its energy consumption is dynamically changed.

4.5. 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.

4.6. 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 3. 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:

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

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. We adopt the demand-pricing relationship in Economics theory [4,51,52] in the form of $f(x) = \alpha x^{-\varepsilon}$ with $f(x)$ being the demand and x being the pricing to model the relationship between node uncooperativeness ($f(x)$) vs. E_{remain}, $M_{difficulty}$ or S_{degree} (x). In Economics theory with $f(x) = \alpha x^{-\varepsilon}$ and $\varepsilon > 1$, lower pricing would stimulate higher demand, and conversely high pricing would suppress demand. In a mission-oriented mobile group in which successful mission execution is the ultimate goal for performance evaluation, we draw the following analogues to model a node's uncooperative behavior:

- $f_e(E_{remain})$: Low energy would stimulate uncooperativeness. Every node conserves its energy as long as it does not jeopardize the global welfare (i.e., successful mission execution). That is, when a nod's energy is low it tends to conserve its energy so as to best serve the mission, so it tends to be uncooperative. This is to consider a node's individual utility in resource-constrained environments.
- $f_m(M_{difficulty})$: High mission difficulty would suppress uncooperativeness. That is, if a node is assigned to a more difficult mission, it tends to be less uncooperative (or more cooperative) to ensure successful mission execution.
- $f_s(S_{degree})$: High S_{degree} would suppress uncooperativeness. That is, if a node's 1-hop neighbors are not very cooperative, the node tends to less uncooperative (or more cooperative) in order to complete a given mission successfully.

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

4.7. Obtaining objective trust for validating SQTrust protocol design

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:

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

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

$$T_j^{obj,X}(t) = \frac{\int_{t-d\Delta t}^{t} \sum_{s \in S} (r_s \ * \ P_s(t'))dt'}{d\Delta t} \tag{13}$$

for *X* = intimacy. The reason we use a different equation for *X* = intimacy is that in the node SPN model, there is no place holder modeling intimacy directly. Here *S* indicates the set of states in the underlying semi-Markov chain of our SPN model, r_s is the reward 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_r 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 Eq. (6). It is compared with average subjective trust of node *j*, $T_j^{sub}(t)$, defined in Eq. (5) to compute trust bias obtained to validate our trust aggregation protocol design.

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.

5. Analytical results

5.1. Operational profile as input

Table 2 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 *n* = 150 nodes moving randomly with speed S_{init} in the range of (0,2] m/s in a 6 × 6 operational region in a 1250 m × 1250 m area, with each region covering *R* = 250 m radio radius. The environment being considered is assumed hostile and insecure with the average compromising rate λ_{com} set to once per 18 h. Each node's energy is in the range of [12,24] h. Further each node observes the node behavior model as specified in Sections 3.3 and 4.1 with ε = 1.2, α = 0.8 and T_{gc} = 120 s. 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 6 × 6 regions (as illustrated in Fig. 1) 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 Δt = 20 min, resulting in $e^{-\lambda_d t} = 0.98$ 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.

5.2. Identifying best trust aggregation protocol settings to minimize trust bias

Fig. 3 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 (and thus smaller trust bias) as we use more conservative direct

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*′*slocation*) is within a 5-region neighbor area at time *t*; 0 otherwise
$T_j^{obj,healthiness}(t)$	1 *if* (*mark*(*j*′*sCN*) = 0); 0 *otherwise*
$T_j^{obj,energy}$	1 *if* (*mark*(*j*′*sEnergy*) > E_T); 0 *otherwise*
$T_j^{obj,cooperativeness}(t)$	1 *if* (*mark*(*j*′*s UNCOOP*) = 0); 0 *otherwise*

Table 2
Operational profile for a mobile group application.

Parameter	Value	Parameter	Value
# of Regions	6 × 6	R	250 m
Area	1250 m × 1250 m	E_{init}	[12, 24] h
S_{init}	(0, 2] m/s.	ε	1.2
$1/\lambda_{com}$	18 h	α	0.8
T_{gc}	120 s	P^H_{fn}, P^H_{fp}	0.5%

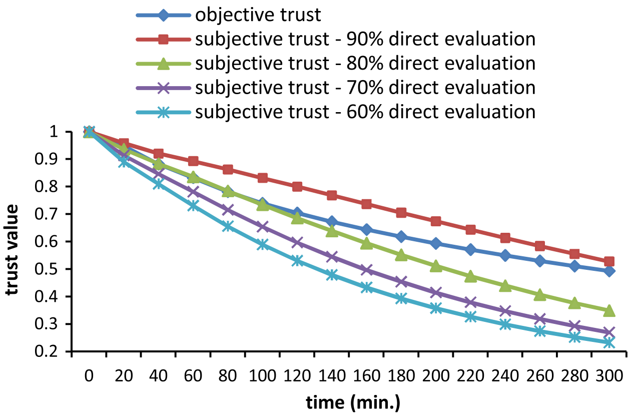


Fig. 3. Overall trust evaluation: subjective trust is most accurate when using 85% direct trust evaluation (β_1:β_2 = 0.85:0.15).

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 ($e^{-\lambda_d t} = 0.98$ for direct trust decay in our case study).

5.3. Identifying best trust formation setting to maximize application performance

We consider a mission-oriented mobile group application scenario in which a lead 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 lead 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 Eq. (4). The rationale behind dynamic membership is that the lead 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 Eqs. (7) and (8) 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 $[0, \Delta t]$, $[\Delta t, 2\Delta t], \ldots, [TR - \Delta t, TR]$.

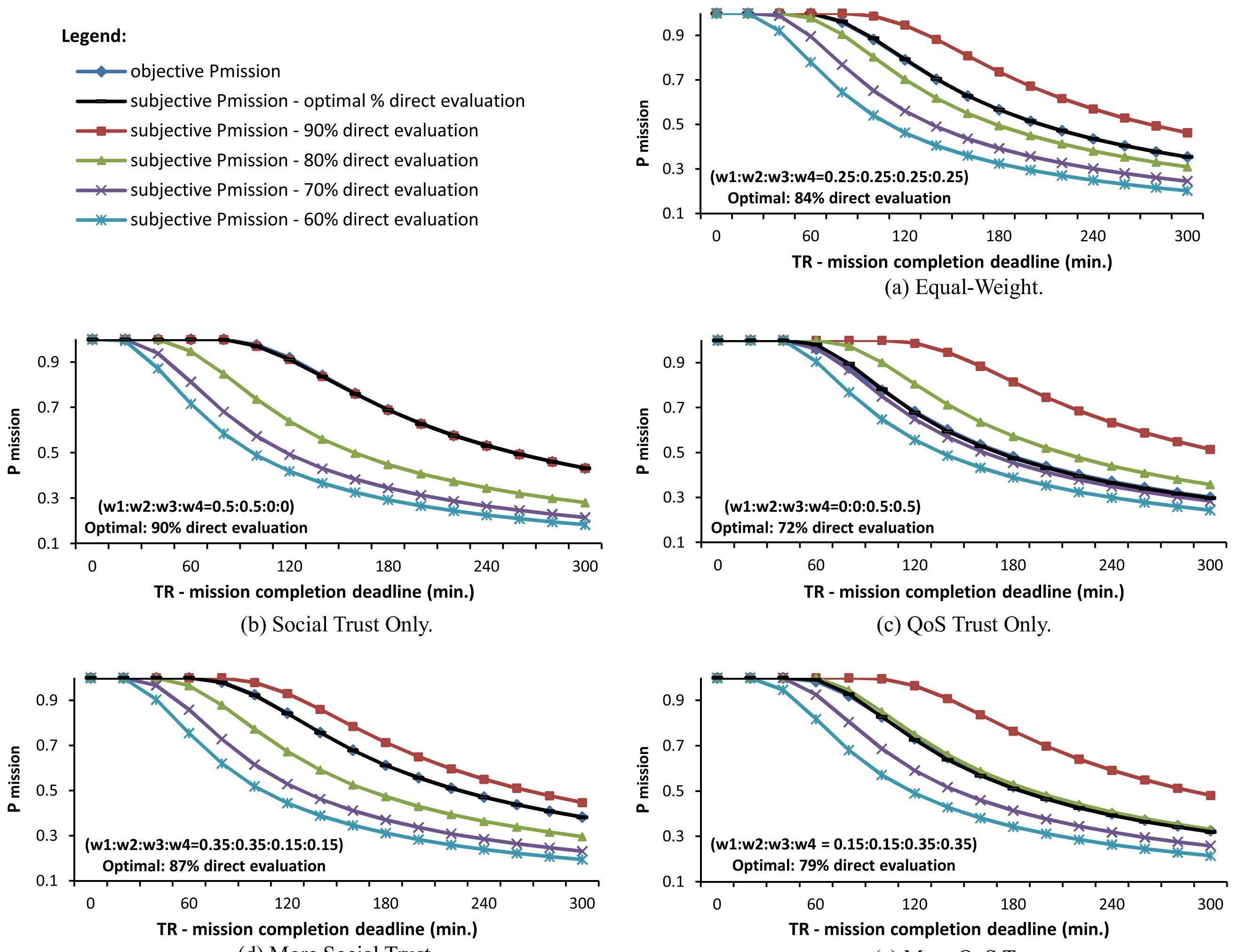
Fig. 4 shows the mission success probability $P_{mission}$ as a function of mission completion deadline TR. To examine the effect of w_1:w_2:w_3:w_4 (the weight ratio for the 4 trust components considered in this paper), we consider 5 test cases: (a) *equal-weight*, (b) *social trust only*, (c) *QoS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

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.

In summary Fig. 4 demonstrates the effectiveness of SQTrust. When given an operational profile characterized by a set of model parameter values defined in Table 2, 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 Fig. 5 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 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



(a) Equal-Weight.

(b) Social Trust Only.

(c) QoS Trust Only.

(d) More Social Trust.

(e) More QoS Trust.

Fig. 4. Mission success probability: subjective vs. objective evaluation.

Table 3
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

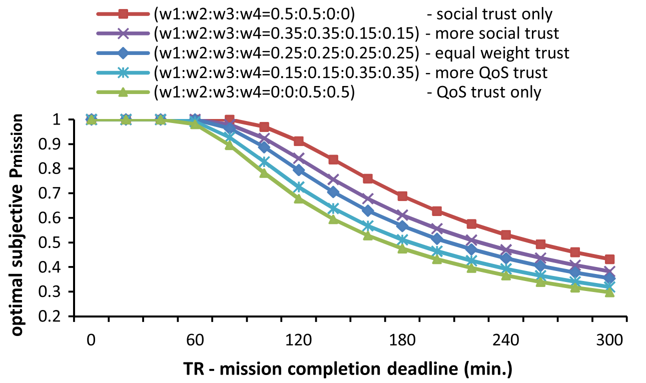


Fig. 5. Effect of w_1:w_2:w_3:w_4 on mission success probability: using more social trust increases mission success probability.

methodology developed in this paper helps identify the best w_1:w_2:w_3:w_4 weight ratio to maximize the system reliability.

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). Figs. 5 and 6 show $P_{mission}$ vs. *TR* for the system operating under best β_1:β_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 Fig. 6, 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 Fig. 7, 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

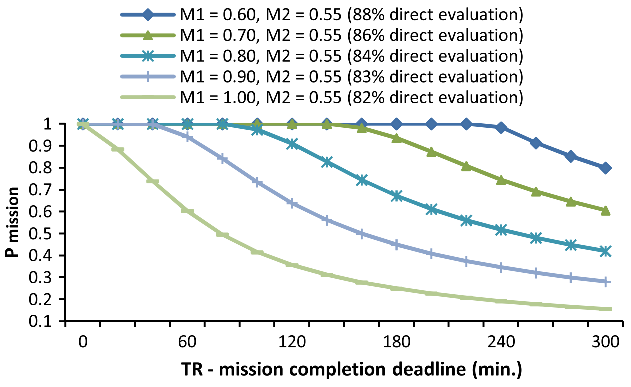


Fig. 6. Effect of M_1 on mission success probability: using higher M_1 (minimum trust level) decreases mission success probability.

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 2. 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] h 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 Eq. (10). 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. Fig. 8 shows the simulation results for the overall *subjective trust* obtained under the equal-weight case, corresponding to Fig. 3 obtained earlier from theoretical analysis. As in Fig. 3, 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 Fig. 8 are remarkably similar to the analytical results shown in Fig. 3, with the average mean square error (MSE) between the simulation results vs. the analytical results less than 5%.

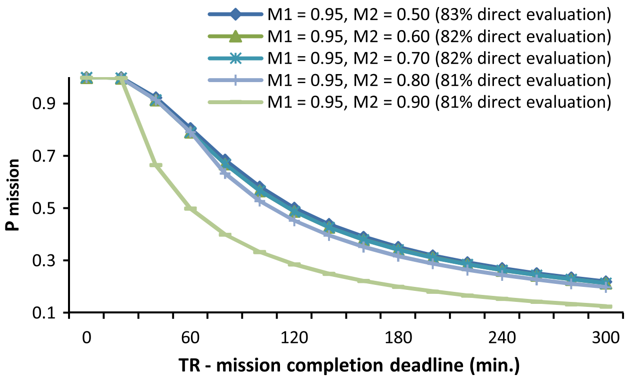


Fig. 7. Effect of M_2 on mission success probability: using higher M_2 (drop dead trust level) decreases mission success probability.

Fig. 9 shows the simulation results for the effect of w_1:w_2:w_3:w_4 on mission success probability $P_{mission}$, corresponding to Fig. 5 obtained earlier from analytical calculations. As in Fig. 5, we simulate 5 cases for the w_1:w_2:w_3:w_4 weight ratio (see Table 3). We observe that Fig. 9 is virtually identical to Fig. 5 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 Figs. 3–7 are accurate and valid.

7. Related work

In this section, we survey recently proposed trust management protocols for MANETs. We contrast and compare our work with existing work so as to differentiate our work from existing work and identity unique features and contributions of our trust protocol design for MANETs. We discuss related work in three areas: *trust management framework*, *trust metrics*, and *trust resiliency and accuracy*.

7.1. Trust management framework

Michiardi and Molva [60] proposed a collaborative reputation mechanism to enforce node cooperation (CORE) in MANETs. The CORE scheme relies on two key designs: a reputation table stored by each node to maintain the reputation toward others and a watchdog mechanism for detecting cooperative behavior. The reputation table combines the reputation from both direct observations obtained from the watchdog and indirect recommendations from other nodes. Buchegger and Boudec [57] proposed CONFIDANT and applied it to dynamic source routing in MANETs. They used a *neighborhood watch* (similar to the watchdog mechanism in CORE) to detect non-compliant

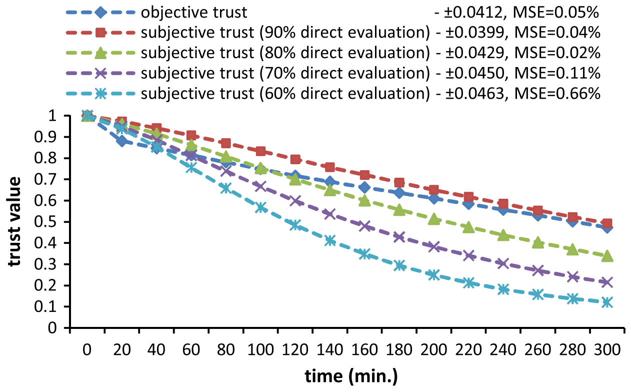


Fig. 8. Simulation results of overall trust corresponding to Fig. 3.

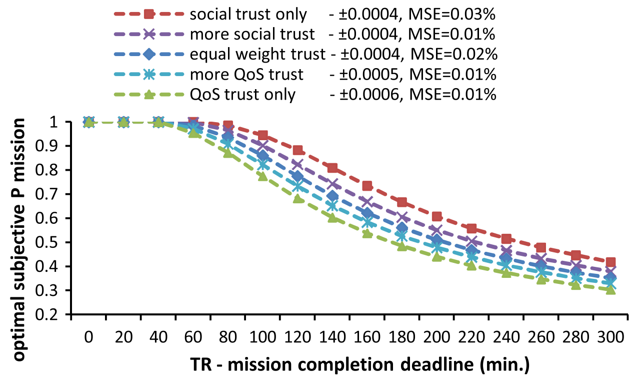


Fig. 9. Simulation results of reliability assessment corresponding to Fig. 5.

behaviors of neighboring nodes. Once a node detects malicious evidence, it sends an *alarm* message to others to propagate the evidence. Theodorakopoulos and Baras [35] modeled the trust evaluation process in MANETs as a path finding problem on a directed graph, where nodes represent entities and edges represent trust relations. Using the theory of semirings on an established direct graph, two nodes without previous direct interaction can establish indirect trust relation. Sun et al. [34] presented an information theoretic framework for modeling trust propagation and aggregation in ad hoc networks. The framework comprises four axioms as the basis for trust propagation and aggregation. Under this framework, *entropy-based* and *probability-based* trust models are proposed.

Compared to the works cited above, we also consider both direct observations and indirect recommendations for trust management. However, we develop new mechanisms based on *threshold-based filtering* and *relevance-based trust selection* to select trustworthy recommenders to mitigate slandering attacks, and consider trust decay over space and time during trust merging. More importantly, SQTrust adjusts the weights associated with direct trust and indirect trust to minimize trust bias in response to changing environments.

The above trust management protocols assume a flat structure in MANETs and have scalability issues when the network size increases. Verma et al. [61] and Davis [62] considered hierarchical trust management for MANETs. In their hierarchical trust management schemes, each node performs trust evaluation locally. However, their schemes heavily rely on the certificates issued off-line or by trusted third parties which typically are not available in MANET environments.

Our trust management protocol design when applying to MANETs can handle small, flat MANETs as well as large, hierarchically-structured MANETs. A major distinction of our work from the above cited works is that our trust framework covers all aspects of trust management, namely, trust composition, trust aggregation, trust propagation, and trust formation. In trust composition, we explore novel QoS and social trust metrics pertinent for modeling node behaviors in MANET environments. In trust propagation and aggregation, we investigate the best way to combine direct trust with indirect trust for individual trust metrics to minimize trust bias. In trust formation, we investigate the best way to combine multidimensional trust properties for application-level performance optimization illustrated with reliability assessment of a mission-oriented mobile group.

7.2. Trust metrics

Many QoS performance metrics have been used for trust evaluation in MANETs, such as control packet overhead, throughput, goodput, packet dropping rate and delay. Dependability metrics such as availability, convergence time to reach a steady state in trustworthiness for all participating nodes, percentage of malicious nodes, result of intrusion detection and fault tolerance based on reputation thresholds also have been employed. Social trust metrics have also been employed to deal with malicious and uncooperative behaviors in MANETs. Golbeck [17] 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. [39] used social networks to evaluate trust values in the presence of Sybil attacks. Very recently, Cho et al. [10,63] surveyed trust management schemes for MANETs and suggested both QoS trust and social trust be considered for trust composition.

Contrast to the works cited above, we propose combining social trust derived from social networks with QoS trust derived from communication networks to obtain a composite trust metric as a basis for evaluating trust of mobile nodes in MANET environments, recognizing that a mission-oriented mobile group often comprises both human and non-human operators so that both social and QoS trust metrics must be considered for mission-oriented mobile.

7.3. Trust resiliency and accuracy

Trust management aims to provide a secure mechanism for MANETs. However, trust management itself faces attacks from malicious nodes, including good-mouthing attacks (recommending a bad node as a good node), bad-mouthing attacks (recommending a good node as a bad node), and white-washing attacks (recommending itself as a good node). Mundinger and Boudec [27] performed a theoretical analysis on the robustness of a reputation system in the presence of liars (providing false recommendations). They claimed that there is a liar percentage threshold above which lying has an impact and can finally corrupt the reputation system. The reputation system needs to compromise between *fast-convergence* and *accurate trust evaluation*. These attacks can be alleviated by taking trust recommendation only from trusted recommenders or performing statistical analysis on the recommendation values to remove bias. Zouridaki et al. [40] proposed a robust cooperative trust scheme for secure routing in MANETs. In their scheme, recommenders are chosen in the order of: (1) good recommenders, (2) nodes with recommender trustworthiness higher than a threshold, and (3) all other recommenders. Balakrishnan et al. [59] proposed a trust protocol for MANETs to address similar issues (i.e., *recommender's bias*, *honest elicitation*, and *free riding*) in trust recommendations. Buchegger and Boudec [58] analyzed the effect of combining rumors (second-hand information) with direct observations (first-hand information) during trust merging and concluded that using second-hand information not deviating too much from the first-hand information can significantly accelerate the detection and subsequent isolation of malicious nodes.

Contrast to the works cited above which used simulation to test trust resiliency and accuracy, we address the issue of trust protocol resiliency and accuracy by design and validation. For design, we develop new mechanisms based on *threshold-based filtering and relevance-based trust selection* against good-mouthing or bad-mouthing attacks, and *dynamic weight adjustment* of the direct and indirect trust components to minimize trust bias. For validation, we demonstrate our protocol's resiliency and accuracy by developing a novel model-based analysis methodology with simulation validation.

8. Applicability

The identification of optimal protocol settings in terms of β_1:β_2 to minimize trust bias, and the best application-level trust optimization setting in terms of w_1:w_2:w_3:w_4 to maximize application performance is performed at static time. One way to apply the results for dynamic trust management is to build a lookup table at static time listing the optimal protocol settings discovered over a perceivable range of parameter values. Then, at runtime, upon sensing the environment conditions matching with a set of parameter values, a node can perform a simple table lookup operation augmented with extrapolation/interpolation techniques [69] to determine and apply the optimal protocol setting to minimize trust bias and/or to maximize application performance dynamically in response to environment changes. The complexity is O(1) because of the table lookup technique employed.

9. Conclusion

In this paper we addressed the performance issue of trust management protocol design for MANETs in two important areas: trust bias minimization and application performance maximization. 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 derive the *objective* trust based on ground truth status of nodes as time progresses, which serves as the basis for identify the best aggregation protocol setting in terms of β_1:β_2 to minimize trust bias, and the best application-level trust optimization setting in terms of w_1:w_2:w_3:w_4 to maximize application performance.

The analytical results validated by extensive simulation demonstrate that our integrated social and QoS trust protocol (SQTrust) operating at its optimizing settings is able to minimize trust bias, thus supporting its resiliency property to bad-mouthing and good-mouthing attacks by malicious nodes. Using mission-oriented mobile groups as an application, we demonstrated that one can identify and apply the best trust formation to maximize the application performance in terms of the system reliability.

In the future we plan to explore other trust-based MANET applications such as trust-based intrusion detection [2,11,20,23,38] and service composition [70,71] with which we could further demonstrate the design notion of application-level trust optimization proposed in this paper. We also plan to investigate if other trust formation methods (other than the linear function considered in this paper) would be more effective for such MANET applications, and perform a comparative performance analysis with existing methods (e.g., Bayesian [21] or fuzzy logic [14]). Lastly, the node behavior model is based on persistent attacks. We plan to consider more sophisticated attacker models such as random, opportunistic, and insidious attacks [49,53–56] with fuzzy failure criteria [45–47] applied to further test the resiliency of our trust protocol design.

Acknowledgement

This work was supported in part by the Army Research Office under Grant W911NF-12-1-0445.

References

[1] W.J. Adams, N.J. Davis, Validating a trust-based access control system, in: IFIP International Conference on Trust Management, New Brunswick, Canada, July 2007, pp. 91–106.

[2] F. Bao, I.R. Chen, M. Chang, J.H. Cho, Trust-based intrusion detection in wireless sensor networks, in: IEEE Int'l Conf. on Communication, Kyoto, Japan, June 2011, pp. 1–6.

[3] E. Aivaloglou, S. Gritxalis, C. Skianis, Trust establishment in ad hoc and sensor networks, in: 1st Int'l Conf. on Critical Information Infrastructure Security, Samos, Greece, vol. 4347, August 2006, pp. 179–192.

[4] O. Yilmaz, I.R. Chen, Utilizing call admission control for pricing optimization of multiple service classes in wireless cellular networks, Comput. Commun. 32 (2009) 317–323.

[5] V. Balakrishnnan, V. Varadharajan, U.K. Tupakula, P. Lucs, Trust and recommendations in mobile ad hoc networks, in: Int'l Conf. on Networking and Services, Athens, Greece, June 2007, pp. 64–69.

[6] J.H. Cho, M. Chang, I.R. Chen, A. Swami, A provenance-based trust model for delay tolerant networks, in: 6th IFIP International Conference on Trust Management (IFIPTM), Surat, India, May 2012, pp. 52–67.

[7] M. Blaze, J. Feigenbaum, J. Lacy, Decentralized trust management, in: IEEE Symposium on Security and Privacy, May 1996, pp. 164–173.

[8] Y. Ren, A. Boukerche, Modeling and managing the trust for wireless and mobile ad-hoc networks, in: IEEE International Conference on Communications, Beijing, China, May 2008, pp. 2129–2133.

[9] B.J. Chang, S.L. Kuo, Markov chain trust model for trust value analysis and key management in distributed multicast MANETs, IEEE Trans. Veh. Technol. 58 (4) (2009) 1846–1863.

[10] J.H. Cho, A. Swami, I.R. Chen, A survey on trust management for mobile ad hoc networks, IEEE Commun. Surv. Tutorials 13 (4) (2011) 562–583.

[11] J.H. Cho, I.R. Chen, Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks, IEEE Trans. Reliab. 59 (1) (2010) 231–241.

[12] E.M. Daly, M. Haahr, Social network analysis for information flow in disconnected delay-tolerant MANETs, IEEE Trans. Mob. Comput. 8 (5) (2009) 606–621.

[13] W. Gao, G. Cao, T.F. La Porta, J. Han, On exploiting transient social contact patterns for data forwarding in delay-tolerant networks, IEEE Trans. Mob. Comput. 12 (1) (2013) 151–165.

[14] J. Luo, X. Liu, M. Fan, A trust model based on fuzzy recommendation for mobile ad-hoc networks, Comput. Netw. 53 (14) (2009) 2396–2407.

[15] B.K. Chaurasia, R.S. Tomar, Trust management model for wireless ad hoc networks, in: International Conference on Soft Computing for Problem Solving, Dec. 2011, pp. 201–206.

[16] J.H. Cho, A. Swami, I.R. Chen, Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks, J. Netw. Comput. Appl. 35 (3) (2012) 1001–1012.

[17] J. Golbeck, Computing with Trust: Definition, Properties, and Algorithms, Securecomm, Baltimore, MD, 2006. August, pp. 1–7.

[18] J.H. Cho, K.S. Chan, I.R. Chen, Composite trust-based public key management in mobile ad hoc networks, in: ACM 28th Symposium on Applied Computing, Coimbra, Portugal, March 2013.

[19] C. Hui, M. Goldberg, M. Magdon-Ismail, W. Wallace, Simulating the diffusion of information: an agent-based modeling approach, Int. J. Agent Technol. Syst. 2 (3) (2010) 31–46.

[20] F. Bao, I.R. Chen, M. Chang, J.H. Cho, Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, IEEE Trans. Netw. Serv. Manage. 9 (2) (2012) 161–183.

[21] A. Josang, R. Ismail, The beta reputation system, in: 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] E. Ayday, F. Fekri, An iterative algorithm for trust management and adversary detection for delay-tolerant networks, IEEE Trans. Mob. Comput. 11 (9) (2012) 1514–1531.

[24] H. Li, M. Singhal, Trust management in distributed systems, IEEE Computers 40 (2) (2007) 45–53.

[25] Z. Liu, A.W. Joy, R.A. Thompson, A dynamic trust model for mobile ad hoc networks, in: 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, S.J. Knapskog, TSR: Trust-based secure MANET routing using HMMs, in: 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Vancouver, Canada, Oct. 2008, pp. 83–90.

[27] J. Mundinger, J. Le Boudec, Analysis of a reputation system for mobile ad hoc networks with liars, Perform. Eval. 65 (3–4) (2008) 212–226.

[28] J.D. Musa, Operational profiles in software-reliability engineering, IEEE Softw. 10 (2) (1993) 14–32.

[29] E.C.H. Ngai, M.R. Lyu, Trust and clustering-based authentication services in mobile ad hoc networks, in: 24th Int'l Conf. on Distributed Computing Systems Workshops, March 2004, pp. 582–587.

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

[31] J. Sen, P. Chowdhury, I. Sengupta, A distributed trust mechanism for mobile ad hoc networks, in: 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, H. Wong, Decentralized intrusion detection in wireless sensor networks, in: ACM 1st International Workshop on Quality of Service and Security in Wireless and Mobile Networks, Montreal, Quebec, Canada, 2005.

[33] M. Steiner, G. Tsudik, M. Waidner, Diffie-Hellman key distribution extended to group communication, in: Proc. 3rd ACM Conf. on Computer and Communications, Security, Jan. 1996, pp. 31–37.

[34] Y.L. Sun, W. Yu, Z. Han, K.J.R. Liu, Information theoretic framework of trust modeling and evaluation for ad hoc networks, IEEE J. Sel. Areas Commun. 24 (2) (2006) 305–317.

[35] G. Theodorakopoulos, J.S. Baras, On trust models and trust evaluation metrics for ad hoc networks, IEEE J. Sel. Areas Commun. 24 (2) (Feb. 2006) 318–328.

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

[37] B. Wang, S. Soltani, J. Shapiro, P. Tab, Local detection of selfish routing behavior in ad hoc networks, in: 8th Int'l Symposium on Parallel Architectures, Algorithms and Networks, Dec. 2005, pp. 392–399.

[38] H. Zhu, S. Du, Z. Gao, M. Dong, Z. Cao, A probabilistic misbehavior detection scheme towards efficient trust establishment in delay-tolerant networks, IEEE Trans. Parallel Distrib. Syst. (2013).

[39] H. Yu, M. Kaminsky, P.B. Gibbons, A.D. Flaxman, SybilGuard: defending against sybil attacks via social networks, IEEE/ACM Trans. Network. 16 (3) (2008) 576–589.

[40] C. Zouridaki, B.L. Mark, M. Hejmo, R.K. Thomas, Robust cooperative trust establishment for MANETs, in: 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, Oct. 2006, pp. 23–34.

[41] L. Capra, M. Musolesi, Autonomic trust prediction for pervasive systems, in: International Conference on Advanced Information Networking and Applications, April 2006, pp. 1–5.

[42] S. Trifunovic, F. Legendre, C. Anastasiades, Social trust in opportunistic networks, in: IEEE Conference on Computer Communications Workshops, San Diego, March 2010, pp. 1–6.

[43] M.K. Denko, T. Sun, I. Woungang, Trust management in ubiquitous computing: a Bayesian approach, Comput. Commun. 34 (3) (2011) 398–406.

[44] I.R. Chen, F. Bao, M. Chang, J.H. Cho, Trust management for encounter-based routing in delay tolerant networks, in: IEEE Global Communications Conference, Miami, Florida, USA, Dec. 2010, pp. 1–6.

[45] F.B. Bastani, I.R. Chen, T.W. Tsao, Reliability of systems with fuzzy-failure criterion, in: Annual Reliability and Maintainability Symposium, Anaheim, California, USA, 1994, pp. 442–448.

[46] I.R. Chen, F.B. Bastani, T.W. Tsao, On the reliability of AI planning software in real-time applications, IEEE Trans. Knowl. Data Eng. 7 (1) (1995) 4–13.

[47] I.R. Chen, F.B. Bastani, Effect of artificial-intelligence planning-procedures on system reliability, IEEE Trans. Reliab. 40 (3) (1991) 364–369.

[48] K. Govindan, P. Mohapatra, Trust computations and trust dynamics in mobile ad hoc networks: a survey, IEEE Commun. Surv. Tutorials 14 (2) (2012) 279–298.

[49] R. Mitchell, I.R. Chen, Effect of intrusion detection and response on reliability of cyber physical systems, IEEE Trans. Reliab. 62 (1) (2013) 199–210.

[50] P.B. Velloso, R.P. Laufer, D. de O Cunha, O.C. Duarte, G. Pujolle, Trust management in mobile ad hoc networks using a scalable maturity-based model, IEEE Trans. Netw. Serv. Manage. 7 (3) (2010) 172–185.

[51] I.R. Chen, T.H. Hsi, Performance analysis of admission control algorithms based on reward optimization for real-time multimedia servers, Perform. Eval. 33 (2) (1998) 89–112.

[52] S.T. Cheng, C.M. Chen, I.R. Chen, Dynamic quota-based admission control with sub-rating in multimedia servers, Multimedia Syst. 8 (2) (2000) 83–91.

[53] R. Mitchell, I.R. Chen, Adaptive intrusion detection for unmanned aircraft systems based on behavior rule specification, IEEE Trans. Syst. Man Cybernet. (2013).

[54] H. Al-Hamadi, I.R. Chen, Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensor networks, IEEE Trans. Netw. Serv. Manage. 19 (2) (2013) 189–203.

[55] I.R. Chen, A.P. Speer, M. Eltoweissy, Adaptive fault tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks, IEEE Trans. Dependable Secure Comput. 8 (2) (2011) 161–176.

[56] R. Mitchell, I.R. Chen, Behavior rule based intrusion detection systems for safety critical smart grid applications, IEEE Trans. Smart Grid 4 (3) (2013) 1254–1263.

[57] S. Buchegger, J.-Y.L. Boudec, Performance analysis of the confidant protocol: cooperation of nodes – fairness in dynamic ad-hoc networks, in: ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 2002, pp. 226–236.

[58] S. Buchegger, J.-Y. Le Boudec, The effect of rumor spreading in reputation systems for mobile ad-hoc networks, WiOpt'03, Sophia-Antipolis, France, March 2003.

[59] V. Balakrishnan, V. Varadharajan, U.K. Tupakula, P. Lucs, Trust and recommendations in mobile ad hoc networks, in: International Conference on Networking and Services, Athens, Greece, June 2007, pp. 64–69.

[60] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, IFIP TC6/TC11 Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia, Security, 2002, pp. 107–121.

[61] R.R.S. Verma, D. O'Mahony, H. Tewari, NTM – progressive trust negotiation in ad hoc networks, in: IEI/IEE Symposium on Telecommunications Systems Research, Dublin, Ireland, Nov. 2001, pp. 1–8.

[62] C.R. Davis, A localized trust management scheme for ad hoc networks, Int. Conf. Network. (2004) 671–675.

[63] J.H. Cho, A. Swami, I.R. Chen, Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks, IEEE International Conference on Computational Science and Engineering, Vancouver, BC, Canada, August 2009, pp. 641–650.

[64] I.R. Chen, D.C. Wang, Analyzing dynamic voting using Petri nets, in: 15th IEEE Symposium on Reliable Distributed Systems, Niagara Falls, Canada, 1996, pp. 44–53.

[65] I.R. Chen, D.C. Wang, Analysis of replicated data with repair dependency, The Computer Journal 39 (9) (1996) 767–779.

[66] Y. Li, I.R. Chen, Design and performance analysis of mobility management schemes based on pointer forwarding for wireless mesh networks, IEEE Trans. Mob. Comput. 10 (3) (2011) 349–361.

[67] I.R. Chen, T.M. Chen, C. Lee, Performance evaluation of forwarding strategies for location management in mobile networks, Comput. J. 41 (4) (1998) 243–253.

[68] B. Gu, I.R. Chen, Performance analysis of location-aware mobile service proxies for reducing network cost in personal communication systems, Mob. Netw. Appl. 10 (4) (2005) 453–463.

[69] L.E. Bengtsson, Lookup table optimization for sensor linearization in small embedded systems, J. Sensor Technol. 2 (4) (2012) 177–184.

[70] E. Karmouch, A. Nayak, A distributed constraint satisfaction problem approach to virtual device composition, IEEE Trans. Parallel Distrib. Syst. 23 (11) (2012) 1997–2009.

[71] C.W. Hang, M.P. Singh, Trustworthy service selection and composition, ACM Trans. Autonomous Adapt. Syst. 6 (1) (2011). article 5.

[72] J.H. Cho, I.R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, Ad Hoc Netw. 11 (8) (2013) 2217–2234.

[73] I.R. Chen, O. Yilmaz, I.L. Yen, Admission control algorithms for revenue optimization with QoS guarantees in mobile wireless networks, Wireless Pers. Commun. 38 (3) (2006) 357–376.

[74] I.R. Chen, T.M. Chen, C. Lee, Agent-based forwarding strategies for reducing location management cost in mobile networks, Mobile Netw. Appl. 6 (2) (2001) 105–115.

[75] I.R. Chen, N. Verma, Simulation study of a class of autonomous host-centric mobility prediction algorithms for wireless cellular and ad hoc networks, in: ACM 36th Annual Symposium on Simulation, Orlando, Florida, USA, 2003, pp. 65–72.

[76] I.R. Chen, J. Guo, F. Bao, J.H. Cho, Integrated social and quality of service trust management of mobile groups in ad hoc networks, in: 9th IEEE Conference on Information, Communications and Signal Processing, Tainan, Taiwan, Dec. 2013.

[77] I.R. Chen, F. Bao, M. Chang, J.H. Cho, Dynamic trust management for delay tolerant networks and its application to secure routing, IEEE Trans. Parallel Distrib. Syst. (2014), http://dx.doi.org/10.1109/TPDS.2013.116.

Ing-Ray Chen received the BS degree from the National Taiwan University, Taipei, Taiwan, and the MS and PhD degrees in computer science from the University of Houston. He is a professor in the Department of Computer Science at Virginia Tech. His research interests include mobile computing, wireless systems, security, trust management, data management, real-time intelligent systems, and reliability and performance analysis. Dr. Chen currently serves as an editor for *IEEE Communications Letters, IEEE Transactions on Network and Service Management, Wireless Personal Communications*, *The Computer Journal*, and *Security and Network Communications*. He is a member of the IEEE and ACM.

Jia Guo received the B.S. degree in Computer Science from Jilin University, China in 2012. Currently he is pursuing his Ph.D. degree in the Computer Science Department at Virginia Tech. His research interests include trust management, security, wireless networks, wireless sensor networks, mobile computing, dependable computing, system modeling, and performance analysis.

Fenye Bao received the B.S. degree in computer science from Nanjing University of Aeronautics and Astronautics, Nanjing, China in 2006 and the M.E. degree in software engineering from Tsinghua University, Beijing, China in 2009. He received his PhD degree in Computer Science from Virginia Tech in 2013. Currently he is a technical staff member of LinkedIn. His research interests include trust management, security, wireless networks, wireless sensor networks, mobile computing, and dependable computing.

Jin-Hee Cho received the BA from the Ewha Womans University, Seoul, Korea and the MS and PhD degrees in computer science from the Virginia Tech. She is currently a computer scientist at the U.S. Army Research Laboratory (USARL), Adelphi, Maryland. Her research interests include wireless mobile networks, mobile ad hoc networks, sensor networks, secure group communications, group key management, network security, intrusion detection, performance analysis, trust management, cognitive networks, social networks, dynamic networks, and resource allocation. She is a member of the IEEE and ACM.