International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

ACHIEVING GROUP MEMBERSHIP IN ADHOC MOBILE NETWORKS

K Uday Kumar Reddy[1], Dr P.Subbaiah[2]

[1]*Enrollment No :pp.comp.sci&eng.0374,*
Computer Science and Engineering, Ph.D Scholar,
Rayala Seema University Kurnool.
[2]*Research Supervisor, Rayala Seema University Kurnool,*
Andhra Pradesh, (India)

ABSTRACT

We propose to combine 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 develop a novel model-based approach to identify the best protocol setting under which trust bias is minimized, that is, the peer-to-peer subjective trust as a result of executing our distributed trust management protocol is close to ground truth status over a wide range of operational and environment conditions with high resiliency to malicious attacks and misbehaving nodes.

Keywords—trust management; mobile ad hoc networks; QoS trust; social trust; trust bias minimization.

I. INTRODUCTION

Trust management for mobile ad hoc networks (MANETs) (see [1, 2] for a survey) has emerged as a new active research area as evidenced by the proliferation of trust/reputation protocols to support mobile group based applications in recent years [3-6]. In this paper we address an importance issue of trust management protocol design for MANETs: trust bias minimization despite misbehaving nodes performing trust-based attacks.

Relative to existing works [3-6] for MANET trust management cited above, this paper has two 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, convergence time to reach a steady state in trustworthiness for all participating nodes, percentage of malicious nodes, and fault tolerance, one must also consider *social trust* metrics including friendship, honesty, privacy, similarity, betweenness centrality and social ties for trust management. We note that prior works such as [7, 8] 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) mathematical modeling techniques [9-12] 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 trust bias is minimized, i.e., SQTrust is most accurate compared with global knowledge and actual node status.

II. SQTRUST FOR MANETS

A. 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* and *QoS trust*

[1]. 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, 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.

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.

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 to assess the target node's energy and cooperativeness status.

For a target node more than 1-hop away, a node will refer to a set of recommenders for its trust toward the remote target node.

B. Trust Aggregation

A unique feature of our trust aggregation protocol design is that we identify 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 III 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 [1], 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 by node *i* toward node *j* over the time interval[ ] when node *i* and node *j* are 1-hop neighbors at time *t*. Here is the trust update interval and *d* is a design[collected]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*/ , 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*.Bayesian trust/reputation model [13] with Beta (,) distribution such that /(+) is the estimated direct trust with as the number of positive service experiences and as the number of negative service experiences.

The indirect trust part, in Equation 1 is evaluated by node *i* at time *t* by taking in recommendations from a subset of 1-hop neighbors selected following the which satisfy the *threshold-based filtering* and *relevance*-recommendation to node *i* for evaluating node *j* in trust component *X*, node *i*'s trust in node *m* is also taken into consideration as reflected in the product term on the right hand <side of Equation 3. This accounts for@ *trust*0 *decay over space*. If =0 then to account for *trust decay over time*.

C. Trust Formation

While many trust formation models exist [1], 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 issue of determining optimal trust formation parameters for maximizing application performance is outside the scope of the paper and the reader is referred to [14] for more detail. The *subjective trust* value of node *j* as evaluated by node *i* at time *t*

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

III. ANALYTICAL MODEL

A. Node SPN for Modeling Node Behavior

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

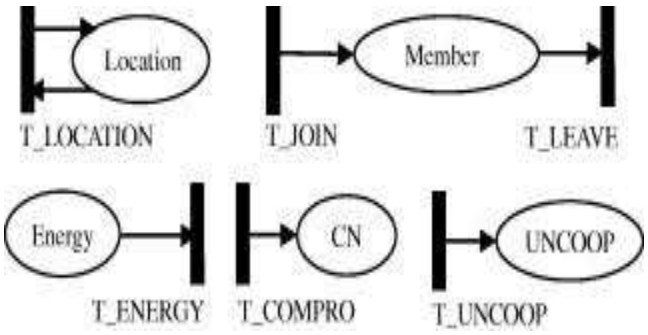

Figure 1: Node SPN Model.

The reason of using node SPN models is to yield a probability model (a semi-Markov chain) to model the stochastic behavior of nodes in the system, given the system's anticipated operational profile as input. The theoretical analysis yields *objective trust* based on ground truth of node status, against which *subjective trust* as a result of executing our proposed trust protocol is compared. This provides the theoretical foundation that subjective trust (from protocol execution) is accurate compared with ground truth. The underlying semi-Markov chain 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. Below we explain how we construct the node SPN model.

Depending on the location a node moves into, the number of tokens in place *Location* is adjusted. 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 gives the probability that a node is at a particular location at time *t*, e.g., the probability that node *i* is located in region *j* at time *t*. This information along with the location information of other nodes at time *t* provides global information if two nodes are 1-hop neighbors at time *t*.

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

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

Healthiness: A node is compromised when transitionMT_COMPRO fires. The rate to transition T_COMPRO is 8 as the node compromising rate (or the capture rate) reflecting the hostility of the application. If the node is compromised, a token goes to *CN*, meaning that the node is already compromised and may perform good-mouthing and bad-mouthing attacks as a recommender by good-mouthing a bad node with a high trust recommendation and bad-mouthing a good node with a low trust recommendation.

Cooperativeness: Place *UNCOOP* represents whether a node is cooperative or not. If a node becomes uncooperative, a token goes to *UNCOOP* by triggering T_UNCOOP. The rate to transition T_UNCOOP is modeled as a function of its remaining energy, the mission difficulty, and the neighborhoodV XI [successful mission execution.

• C \ : If a node's 1-hop neighbors are not very cooperative, the node is more likely to be cooperative to complete a given mission successfully. A compromised node is necessarily uncooperative as it won't follow the protocol execution rules. So if place CN contains a token, place UNCOOP will also contain a token.

B. Obtaining Objective Trust for Validating SQTrust Protocol Design

With the node behaviors modeled by a probability model (a semi-Markov chain) described above, the objectiveE trust

evaluation of node *j* in trust component *X*, i.e., can be obtained based on exact global knowledge about node *j* as modeled by its node SPN model. To calculate each of these objective Ntrust probabilities of node *j*, one would assign a reward of C with state *s* of the underlying semi-Markov chain of the SPN model to obtain the probability weighed average reward as:

Table 2: Operational Profile for a Mobile Group Application.

Parameter	Value	Parameter	Value
# of regions	6x6	*R*	250m
Area	1250mx1250m	*Einit*	[12, 24] hrs
Sinit	(0, 2] m/sec.	*ε*	1.2
$1/_{com}$	18 hrs	*α*	0.8
Tgc	120 sec.		0.6

IV. RESULTS

Table 2 lists the parameter set and their default values specifying the operational profile given as input for testing SQTrust for a mobile group of size of 150 nodes in MANET environments. Initially all nodes are not compromised. When a node is compromised and turns malicious, it performs good-mouthing and bad-mouthing attacks, i.e., it will provide the most positive recommendation (that is, 1) toward a bad node to facilitate collusion, and conversely the most negative recommendation (that is, 0) toward a good node to ruin the reputation of the good node. The initial trust level is set to 1 for healthiness, energy and cooperativeness because all nodes are considered trustworthy initially. The initial trust level of intimacy is set to the probability that a node is found to be in a 5-region neighbor area relative to 6x6 regions in accordance with the intimacy definition. Given this operational profile as input to the mobile group application, we aim to identify the best setting of $_1$: $_2$ (with higher $_1$ meaning more direct observations or self-information being used for subjective trust evaluation) under which trust bias is minimized, i.e.,

objective trust
subjective trust - 90% direct evaluation
subjective trust - 80% direct evaluation
subjective trust - 70% direct evaluation subjective trust - 60% direct evaluation

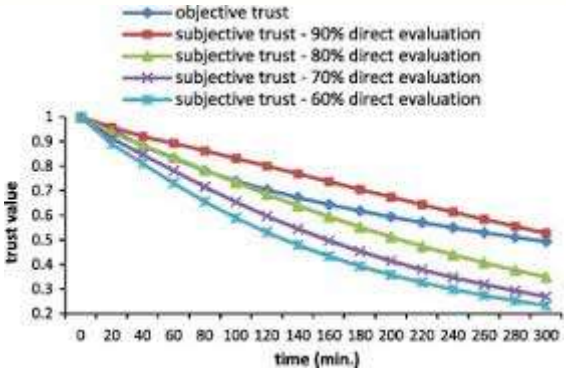

Figure 2: Overall Trust Evaluation: Subjective Trust is Most Accurate

When using 85% Direct Trust Evaluation *(1: 2=0.85:0.15).*

threshold E_T is set to 0.

Figure 2 shows the node's overall trust values obtained

from subjective$_{CDE}$ trust$_E$ evaluation vs. objective trust evaluation, i.e., vs. , for the equal-weight ratio case as a function of time, with $_1$: $_2$ 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 $_1$ allows us to identify the best $_1$: $_2$ 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 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 aresult is validated by ns3 simulation (not shown due to limited space).

V. CONCLUSION

The identification of optimal protocol settings to minimize trust bias and 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 to determine and apply the optimal protocol setting to minimize trust bias in response to environment changes. In the future we plan to consider more sophisticated attacker behaviors including opportunistic, random and insidious attacks [18] to further test the resiliency of our trust protocol design.

REFERENCES

[1] J.H. Cho, A. Swami and I.R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, 2011, pp. 562-583.

[2] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, 2012, pp. 279-298.

[3] P. B. Velloso, et al., "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 172–185, 2010.

[4] 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.

[5] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," *Computer Netwok*, vol. 53, no. 14, pp. 2396–2407, 2009.

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

[7] S. Trifunovic, F. Legendre, and C. Anastasiades, "Social Trust in Opportunistic Networks," *IEEE Conf. on Computer Communications Workshops*, San Diego, CA, USA, March 2010, pp. 1-6.

[8] I. R. Chen, F. Bao, M. Chang, and J. H. Cho, "Trust Management for Encounter-Based Routing in Delay Tolerant Networks," *IEEE Global Communications Conference*, Miami, Florida, USA, Dec. 2010, pp. 1-6.

[9] I.R. Chen, T.M. Chen, and C. Lee, "Performance evaluation of forwarding strategies for location management in mobile networks," *The Computer Journal*, vol. 41, no. 4, pp. 243-253, 1998.

[10] I.R. Chen, D.C. Wang, "Analysis of replicated data with repair dependency," *The Computer Journal*, vol. 39, no. 9, pp. 767-779, 1996.

Bibilography:

Author 1:

K Uday Kumar Reddy[1] ,

Enrollment No :pp.comp.sci&eng.0374,

Computer Science and Engineering, Ph.D Scholar,

Rayala Seema University Kurnool.

Email –id: pranith.dwh@gmail.com ,

Ph-no: +91 9490634569

Author 2:

Dr P.Subbaiah[2] , Research Supervisor,

Rayala Seema University Kurnool,

Andhra Pradesh, India.

Email –id: pranith.dwh@gmail.com ,

Ph-no: +91 9490634569