Modeling and Analysis of Trust Management Protocols: Altruism versus Selfishness in MANETs

Jin-Hee Cho[1], Ananthram Swami[1], Ing-Ray Chen[2]

[1]U.S. Army Research Laboratory
Computational and Information Sciences Directorate
{jinhee.cho, ananthram.swami}@us.army.mil
[2]Virginia Tech
Department of Computer Science
irchen@vt.edu

Abstract. Mobile ad hoc and sensor networks often contain a mixture of nodes, some of which may be selfish and non-cooperative in providing network services such as forwarding packets in order to conserve energy. Existing trust management protocols for mobile ad hoc networks (MANETs) advocate isolating selfish nodes as soon as they are detected. Further, altruistic behaviors are encouraged with incentive mechanisms. In this paper, we propose and analyze a trust management protocol based on the demand and pricing theory for managing group communication systems where system survivability is highly critical to mission execution. Rather than always encouraging altruistic behaviors, we consider the tradeoff between a node's individual welfare (e.g., saving energy for survivability) versus global welfare (e.g., providing service availability) and identify the best design condition so that the system lifetime is maximized while the mission requirements are satisfied.

Keywords: Trust, trust metrics, trust management, mobile ad hoc networks, demand and pricing theory, altruism, selfishness.

1 Introduction

Most existing trust management protocols in mobile ad hoc networks (MANETs) encourage cooperative behaviors while discouraging selfish behaviors of participating nodes, so as to achieve a prescribed system goal such as high service availability. A common approach is to isolate selfish nodes as soon as they are detected and to reward altruistic nodes with incentives to encourage cooperation. However, in MANET environments where resources (e.g., bandwidth, memory, computational power, and energy) are severely constrained, only encouraging altruistic behaviors may adversely shorten the system lifetime. This is because altruistic nodes may die quickly due to energy depletion, thereby possibly resulting in loss of connectivity and system services.

Thomas *et al*. [18] studied system performance in such a scenario, and noted that there is a tradeoff between energy saved by selfish nodes and service availability provided by cooperative nodes. However, no analysis of the tradeoff was given. Papadimitriou [13] coined the term *the price of anarchy* to describe the two conflicting goals of individual welfare versus global welfare, i.e., the local goal of a selfish node to save its energy versus the global goal of an altruistic node to provide high service availability. Similar issues

arise in routing in MANETs (e.g., a local goal through selfish routing versus a global goal for service availability) [15]. The price of anarchy was defined as the performance difference between a system run by an all-knowing benign dictator who can make the right decisions to optimize system performance, versus a system run by a selfish anarchy. We postulate that there should be a tradeoff between system survivability and service availability in terms of these two conflicting goals. As Thomas *et al*. [18] indicated, each node can make a decision for its own benefit as well as for global interest by considering the dynamics of the network as well as its own conditions (e.g., energy level).

We propose and analyze a trust management protocol that trades off node altruism for system survivability for mission-driven group communication system (GCS) in MANETs based on the concept of cognitive networks. In a cognitive network, each node has intelligence to adapt to dynamically changing MANET environments through a learning process, by adjusting its altruistic and selfish behaviors in response to network dynamics. We seek to identify the optimal design settings that maximize system lifetime while satisfying performance requirements such as service availability.

Our trust management protocol adopts *demand and pricing (DP)* theory originally derived from economics [4]; under DP a node decides whether it should behave selfishly or altruistically based on the balance between individual welfare (i.e., saving energy) and global welfare (i.e., providing services). A node's decision may depend on its own energy level, 1-hop neighbors' selfishness levels (i.e., to judge whether the system still has sufficient resources such as an adequate number of cooperative neighboring nodes), and the degree of node importance to mission success (e.g., to judge whether a node's selfish behavior would have a significant detrimental impact on the mission success rate). Social scientists have addressed the tradeoff between local/individual utility and global/collective interest in the area of collaboration theories using the concept of *trust* in groups, teams, and organizations [7]. However, no prior work addresses this tradeoff in the context of trust management in MANETs. A number of prior studies have also taken economic perspectives in modeling communication networks [2, 9, 10, 14, 22]. Unlike these prior studies, our work concerns trust management and we specifically adopt DP theory.

Many routing protocols for MANETs have been developed to isolate selfish nodes and to encourage collaborations among participating nodes [11, 20, 21, 23, 24]. Wang *et al*. [20] devised an efficient incentive mechanism to encourage cooperative behaviors in multipath routing. Zhao [23] investigated the optimal transmission probability and Yan *et al*. [21] developed incentive mechanisms using game theoretic approaches. Miranda *et al*. [11] proposed an algorithm in which routing behaviors are monitored; selfish nodes are penalized (their packets are not forwarded) so as to discourage selfish behaviors, and nodes making heavy demands for services are also penalized to ensure faire allocation of resources. Different from the above work, Zhang *et al*. [24] considered the positive aspect of having selfish nodes in terms of traffic reduction, and established bounds on the probability of a node being selfish to optimize system metrics. Our work in this paper is different in that we investigate and identify the best balance between individual welfare via selfish behaviors versus global interest via altruistic behaviors so as to prolong the system lifetime.

Routing protocols have also been proposed based on the concept of trust (or reputation) to isolate selfish nodes [1, 12, 16] using incentive mechanisms that discourage selfish behaviors. However, the trust metric used often does not adequately consider important properties of trust in a MANET environment, including subjectivity, asymmetry, incomplete transitivity, dynamicity, and context-dependency [5]. Our work takes these properties into consideration by adopting a composite trust metric that incorporates both

social trust and *QoS* (quality-of-service) *trust.* The QoS and social components capture different aspects of trust that are important from the perspective of the user and the end-goal of the mission.

The contributions of this work are as follows. First, we propose a novel composite trust metric encompassing social trust explaining the aspects of internal, interpersonal, and mental aspects of an entity [7] and QoS trust indicating competence for task performance. Second, we develop and analyze a trust-based protocol for a mission-driven GCS in MANETs where nodes may behave selfishly. We use DP theory to quantify the conflicts between individual welfare and global welfare and identify the conditions that best prolong the system lifetime for successful mission execution while satisfying performance requirements. Third, we develop a mathematical model to describe the behaviors of a GCS based on hierarchical stochastic Petri nets (SPN), allowing optimal conditions to be identified to answer what-if type of questions in response to changing operational and environmental conditions. Lastly, through numerical data, we demonstrate that our trust management protocol based on DP theory is capable of maintaining an acceptable trust level for successful mission execution while prolonging system lifetime, when compared with a traditional all-altruistic system.

The rest of this paper is organized as follows. Section 2 describes the system model including the assumptions, trust metric, and energy model. Section 3 develops a performance model to describe the behaviors of a GCS based on hierarchical stochastic Petri nets. Further, Section 3 describes DP theory being applied for the formulation of trust management. Section 4 presents numerical data obtained from the evaluation of our performance model. In particular, we compare the performance of a GCS operating under our proposed trust protocol versus a solely altruistic GCS. Finally, Section 5 concludes the paper and outlines future work.

2 System Model

Due to the unique characteristics of MANETs and unreliable communication in wireless networks, trust management for MANETs should encompass the following trust concepts. Trust should be dynamic to account for uncertainty. Trust should be context-dependent, and subjective, and cannot be assumed to be transitive or reciprocal. To address these unique trust properties, trust management for MANETs should consider the following design features: trust metrics must be customizable, evaluation of trust should be fully distributed without reliance on a centralized authority, and trust management should cope with dynamics and adverse behaviors in a tactical MANET [6].

Cognitive networks are able to reconfigure the network based on past experiences by adapting to changing network behaviors to improve scalability (e.g., reducing complexity), survivability (e.g., increasing reliability), and QoS (e.g., facilitating cooperation among nodes) [18]. We use this concept to indicate a node's ability to adapt to changing network conditions, such as a node's selfish behavior, node failure or mobility, energy exhaustion of a node, or voluntary disconnection for energy savings.

In the initial network deployment, we assume that there is no predefined trust. Without prior interactions, the initial bootstrapping will establish a shallow level of trust based only on indirect information (e.g., reputation from historically collected data or recommendation by third parties) and authentication by a challenge/response process (e.g., public key authentication). Over time, participating nodes will establish a stronger trust

level with more confidence based on direct or indirect interactions. Our trust management protocol allows each node to evaluate the trust levels of other nodes as well as to be evaluated by other nodes based on two factors, social trust and QoS trust. *Social trust* includes trust properties for "sociable" purposes (e.g., intimacy) while *QoS trust* includes trust properties for mission execution purposes (e.g., energy level or cooperation) [5].

Trust decays over time without further updates or interactions between entities. Node mobility also hinders continuous interactions with other group members, lowering the chances of evaluations of each other in the group. This includes cases such as a node moving to other areas causing its disconnection from the current group, leaving a group for mission reasons, voluntary disconnection for saving power or involuntary disconnection due to physical terrain or low energy. We use the concept of a *trust chain* [3] to describe propagation of trust. For example, when *A* trusts *B*, *B* trusts *C*, *C* trusts *D*, and *D* trusts *E*, then, *A* may trust *E* over a trust chain of length 4. However, the longer the trust chain is, the more is the decay in the degree of trust [3].

Our target system is a mission-driven GCS in tactical military MANETs where a symmetric key, called the group key, is used as a secret key for group communications between group members [5]. Upon a node's disconnection from the group, the system generates and redistributes a new key so that non-member nodes will not be able to access a valid secret group key. Nevertheless, each group member keeps old trust information even for non-member nodes so that the information can be reused for future interactions, possibly preventing a newcomer attack.

2.1 Assumptions

We assume that the GCS is in a MANET environment without any centralized trusted authority. Nodes communicate with each node through multiple hops. Nodes have different levels of energy, thus reflecting node heterogeneity. Each node periodically beacons its *id* and *location* information so that node failure is easily detected and accordingly rekeying is done immediately upon every membership change.

We assume that mobile devices are carried by human such as dismounted soldiers. A node dynamically adopts selfish or altruistic behavior depending on the remaining energy level, difficulty level of the given mission (i.e., a tougher mission requires a higher workload), and selfishness level of 1-hop neighbors. That is, a node will behave selfishly when it has low energy, the mission assigned to it is not difficult, and/or there is a sufficient number of cooperating 1-hop neighbors. We consider a node to be selfish when the node drops group communication packets transmitted by other nodes. Even though the node is selfish, we assume that it cooperates to perform rekeying operations upon a membership change. The energy level of each node is adjusted depending on its status. For simplicity, we only consider energy consumption due to packet transmission and reception. Thus, if a node becomes selfish, the rate of energy consumption is slowed down.

We consider a redemption mechanism by which a selfish node can become a normal cooperative node again. Specifically, a selfish node reevaluates its status at the end of each trust update interval and decides whether it will become altruistic or stay selfish. This is described in Section 3.2. A non-member will not consume as much energy as a member because of less involvement with group activities. Upon every membership change due to group join/leave, a rekeying operation will be performed to generate a new group key based on a distributed key agreement protocol such as GDH (Group Diffie-Hellman) [17].

We assume that a node's trust value is evaluated based on direct observations (e.g., packet dropping) as well as indirect observations. Indirect observations are recommendations obtained from 1-hop neighbors whom the evaluator trusts the most. If enough recommenders cannot be found, recommendations from all 1-hop neighbors can be used. A node's trust value may be updated after each status exchange period. A status exchange packet includes a node's own information as well as information of nodes on its trust chain for possible use as recommendations on distant nodes to its 1-hop neighbors.

We assume that existing prevention techniques such as encryption, authentication, or rekeying inhibit outsider attacks. We consider the presence of selfish nodes among legitimate group members. We model the selfish behaviors of a node by DP theory as described in Section 3.2.

2.2 Trust Metric

We consider a trust metric that spans two aspects of the trust relationship [5]. First, we consider intimacy (or friendliness) for *social trust* where intimacy is measured by the degree that two nodes are 1-hop neighbors. Second, *QoS trust* accounts for the capability of a node to complete a given mission. We consider the energy level and degree of unselfishness (or cooperation) to estimate the QoS trust level of a node. A node's trust value changes dynamically to account for trust decay over time due to node mobility or failure, as the trust chain becomes longer, as the node's energy level changes, and as the node becomes selfish or cooperative.

We define a node's trust level as a continuous real number in the range of [0, 1], with 1 indicating complete trust, 0.5 ignorance, and 0 complete distrust. The overall trust value is calculated based on three components: energy level, unselfishness, and intimacy. As will be evident, other components could be added if desired. Based on the trust value calculated by 1-hop neighbors, the trust value can be calculated by *n*-hop neighbors over a trust chain.

The information used for trust evaluation of a particular node *j* includes probability of being alive, e.g., remaining energy > threshold, ($P_j^{energy}(t)$), probability of being unselfish ($P_j^{unselfish}(t)$), and probability of being located in a particular area ($P_j^{loc=k}(t)$) where *k* indicates area *id*, and *t* is time. These three values are obtained from SPN subnets shown in Fig. 2 and the technical method for obtaining them from the SPN subnets is explained in Section 3. We use the term "probability" in a loose sense; one should interpret "probability" here as "value associated with a particular aspect" rather than in the frequentist or Bayesian interpretation.

Now we address how the trust value is calculated. The three trust components, namely, energy level, unselfishness, and intimacy, capture MNAET dynamics. The trust value ($T_{i,j}^{n-hop}(t)$) of node *j* as evaluated by node *i* where *n* indicates the trust chain length used by a node is given by:

$$T_{i,j}^{n-hop}(t) = e^{-\gamma}\left[P_{i,j}^{n-hop,unselfish}(t) + P_{i,j}^{n-hop,energy}(t) + P_{i,j}^{intimacy}(t)\right]/3 \qquad (1)$$

The *n*-hop trust component X, where X represents unselfishness or energy, is calculated based on the trust values obtained from the trust chain with lengths 1 to *n*-1 and is given by:

$$P_{i,j}^{n-hop,X}(t) = \sum_{m=2}^{n} \left(\beta \, P_{i,j}^{(m-1)-hop,X}(t) + (1-\beta) \, P_{i,j}^{m-hop,indirect\ -X}(t) \right) \tag{2}$$

$$where \quad P_{i,j}^{m-hop,indirect\ -X}(t) = \frac{\sum_{k \epsilon S_i} (P_{i,k}^{(m-1)-hop,\ X}(t) \, P_{k,j}^{(m-1)-hop,\ X}(t))}{k_{recom}} \tag{3}$$

Here β is used as a weight for the node's "self-information" and (1- β) is a weight for "other-information." The self-information ($P_{i,j}^{(m-1)-hop,X}(t)$) can be obtained recursively by using Equation 2. In Equation 3, S_i is the set of 1-hop neighbors of node *i,* excluding node *j,* that forward recommendation of node *j* and $|S_i| = k_{recom}$ the number of recommender nodes that have the highest trust values among all 1-hop neighbors on the trust chain of the evaluator. Notice that when calculating the trust value of node *j* via node *k*'s recommendation, node *i*'s trust value on node *k* is used as a weight; this causes trust to decay as the trust chain increases.

Since the *n*-hop trust values are computed based on the basis of (*n-1*)-hop trust values as shown in Equations 2 and 3, the 1-hop trust values are the basis of all trust values and are computed by:

$$P_{i,j}^{1-hop,X}(t) = \left(\beta \, P_{i,j}^{direct\ -X}(t) + (1-\beta) \, P_{i,j}^{1-hop,indirect\ -X}(t) \right) \tag{4}$$

$$P_{i,j}^{1-hop,indirect\ -X}(t) = \frac{\sum_{k \epsilon S_i} \left(P_{i,k}^{1-hop,\ X}(t-\Delta t) \, P_{k,j}^{1-hop,\ X}(t-\Delta t) \right)}{k_{recom}} \tag{5}$$

$$P_{i,j}^{1-hop,unselfis\ h}(0) = 0.5, \qquad P_{i,j}^{1-hop,energy}(0) = 0.5 \tag{6}$$

The direct information for the trust component X of node *j* evaluated by node *i* ($P_{i,j}^{direct\ -X}(t)$) is obtained, by dividing node *j*'s trust component by node *i*'s trust component, $min\left[P_j^X(t)/P_i^X(t), 1\right]$; it is thus a subjective relative evaluation. Note that $P_i^X(t)$ for all *i* where X indicates a trust component obtained from our SPN model as explained in Section 3.3. We assume that the local trust component value of a node at time $t = 0$ are set to ignorance (i.e., ignorance value 0.5 in the trust range of [0, 1]) during the network bootstrapping period, as shown in Equation 6.

In Equation 1, $e^{-\gamma}$ represents a function of $P_{i,j}^{n-hop}(t)$, the probability that nodes *i* and *j* are within *n* hops. $P_{i,j}^{n-hop}(t)$ is computed as:

$$P_{i,j}^{n-hop}(t) = \sum_{k=1}^{n} q_{i,j}^{k-hop}(t) \ \ where \ \ q_{i,j}^{k-hop}(t) = \sum_{(l,m) \epsilon S_k} \left(P_i^{loc=l}(t) \, P_j^{loc=m}(t) \right) \tag{7}$$

Here $P_j^{loc=m}(t)$ is the probability that node *j* is in location *m* at time *t*, and S_k is a set covering all (*l, m*) pairs with the distance between *l* and *m* being *k* hops. Assuming that nodes move independently, we can verify that $P_{i,j}^{n-hop}(t)$ is the probability that nodes (*i, j*) are within *n* hops of each other at time *t*.

In $e^{-\gamma}$, we define γ by:

$$\gamma = \frac{1}{a * P_{i,j}^{n-hop}(t)} \tag{8}$$

where a is a positive constant. The decay factor $e^{-\gamma}$ increases monotonically with $P_{i,j}^{n-hop}(t)$, implying that the trust evaluation is higher if it is more likely that the nodes are closer. The value of the constant a ($a < 1$ versus $a > 1$) dictates whether the decay function is convex or concave increasing in $P_{i,j}^{n-hop}(t)$. The value of the constant a affects the propagation of trust; guidelines for choosing this parameter will be discussed elsewhere. Note that we use Equations 2-6 to compute trust component values of unselfishness and energy.

$P_{i,j}^{intimacy}(t)$, the third component of Equation 1, can be obtained without the help of other nodes' recommendations since each node can detect and keep track of information on who has been with them as 1-hop neighbors through the beacon messages disseminated by each node periodically. $P_{i,j}^{intimacy}(t)$, the degree that nodes *i* and *j* are 1-hop neighbors, is computed by:

$$P_{i,j}^{intimacy}(t) = P_{i,j}^{1-hop}(t) / P_i^{max-intimacy}(t) \tag{9}$$

$$where\ P_i^{max-intimacy}(t) = max\left[P_{i,1}^{1-hop}, \ldots, P_{i,n}^{1-hop}\right] \tag{10}$$

In Equation 9, the normalization by $P_i^{max-intimacy}(t)$ provides relative weights to intimacy, now ranging from 0 to 1. Note that $P_{i,j}^{intimacy}(0)$ can be calculated based on the location information preloaded in the initial network deployment.

We also derive the objective trust values of each node in order to compare it against the trust value calculated by each node, called *subjective trust*. The objective trust is calculated without considering any network dynamics such as node mobility, trust decay over time, and trust decay as the trust chain becomes longer. The objective trust of node *i* is calculated by:

$$T_i^{obj}(t) = \left[P_i^{unselfish}(t) + P_i^{intimacy}(t) + P_i^{energy}(t)\right]/3 \tag{11}$$

$$P_i^{intimacy}(t) = \frac{\left(\sum_{j \in S} P_{i,j}^{1-hop}(t)/N\right)}{P^{avg-obj-intimacy}(t)} \tag{12}$$

Here $P_i^{unselfish}(t)$, $P_i^{intimacy}(t)$, and $P_i^{energy}(t)$ are the three components of trust derived from the SPN subnets explained in Section 3. Ideally, the objective trust value $T_i^{obj}(t)$, of node *j*, would be known to all other nodes. In practice, node *i* estimates the trust value via the subjective trust value $T_{i,j}^{n-hop}(t)$ as discussed earlier in Equation 1. As discussed by Josang *et al.* [8], it is desirable that the subjective trust value is below the objective trust value; this ensures that agents are not exposed to unnecessary risk, but clearly there will be missed reward. We will consider objective intimacy based on the average intimacy degree on node *i* evaluated by all other nodes divided by the average intimacy probability (i.e., the average probability that two nodes will be located as 1-hop neighbors in the operational area). See Section 3 for a specific numeric example. We can then evaluate how accurately subjective trust values are calculated by varying the length of the trust chain through Equation 1, and comparing them with the objective trust shown in

Equation 11. Note that the objective trust is not known in real situations, and so it is predicted and used to conservatively evaluate the validity of the proposed scheme.

In Equation 1, we derive a in order for a trust-based system lifetime based on subjective trust to be at least equal to or less than one based on objective trust. Here by the system lifetime, we mean the the accumulated ime period over which the system trust values are above a certain system drop dead trust level, say T_{value}, as used in Section 4.

2.3 Energy Model

We associate the energy level of a node with its state: selfish or group member. Depending on its remaining energy, a node acts differently. The degree of energy consumption is also affected by the node's state. Thus, these parameters are interwoven and affect a node's lifetime significantly.

A GCS in MANETs must handle events such as beaconing, group communication, rekeying, and status exchange. In particular, after a status exchange event, trust evaluation of 1-hop neighboring nodes as well as of distant nodes is performed. Each node may transmit its own status (e.g., information providing the trust values) as well as status of other nodes (i.e., trust values) on its trust chain. Recall that we use recommendations from 1-hop neighbors for trust evaluation and each status message is disseminated periodically. Due to space constraints, we omit the detail of the energy consumption model and refer the reader to [5].

3 Performance Model

This section describes how our analytical model is developed using SPN and how trust values are obtained from the SPN models.

3.1 Hierarchical Modeling using SPNs

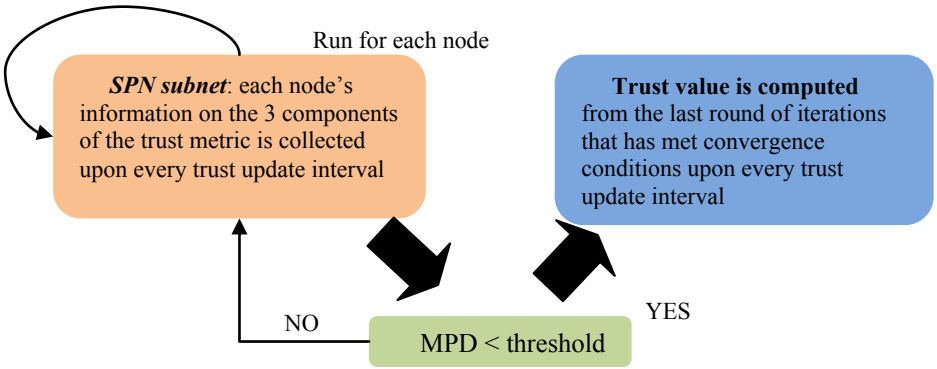

Fig. 1. Hierarchical modeling using SPN subnets.

We develop a mathematical model based on SPN to analyze a GCS with nodes switching between selfish and altruistic behaviors based on the theory and identify design conditions under which the selfish versus altruistic behaviors can be balanced. With system lifetime and mission success probability as our reliability metric, we show that our trust management protocol operating under identified design conditions outperforms one that only encourages altruistic behaviors. We use SPN due to its efficient representation of a large number of states where the underlying models are Markov or semi-Markov models. We develop a hierarchical modeling technique to avoid state explosion problems and to improve solution efficiency for realizing and describing a large scale GCS.

We use an SPN subnet to describe each node's lifetime. The square-shaped operational area consists of $m \times m$ sub-grid areas with the width and height equal to wireless radio range (R). Initially the location of each node is randomly distributed over the operational area based on the uniform distribution. A node randomly moves to one of four locations in four directions (i.e., north, west, south, and east) in accordance with its speed. The speed of each node S_{init} is chosen uniformly over [0, v_{max}) *m/s* where v_{max} is the maximum possible speed, and S_{init} is then fixed during the node's lifetime. The boundary grid areas are wrapped around (i.e., a torus is assumed) to avoid end-effects. The SPN subnet for node i computes the probability that node i is in a particular grid area j at time t. This information along with the information of other nodes' location at time t provides the information about a node's n-hop neighbors at time t, which we will use to compute the trust metric (see Section 2.2). Since node movements are assumed to be independent, the probability that two nodes are in a particular location at time t, is given by the product of the two individual probabilities. The SPN subnet also describes a node's lifetime and can be used to obtain each node's information (amount of energy, unselfishness, and intimacy) to derive the trust relationship with other nodes in the system. This process is done by running the SPN subnet N times for the N nodes in the network.

In the first round of iteration, since there is no information available about 1-hop neighbors, it is assumed that each area has an equal number of nodes and all nodes are unselfish. In the second round of iteration, based on the information collected (e.g., number of unselfish or selfish 1-hop neighbors) from the first round, each node knows how many nodes are 1-hop neighbors that can directly communicate with it, and whether or not they are members of the GCS or selfish. A node also knows how many n-hop neighbors it has at time t. It then adjusts its perceived status of 1-hop neighbors at time t with the output generated from the j^{th} round of iteration as input to the $(j+1)^{th}$ round of iteration. This process continues until a specified convergence condition is met. The Mean Percentage Difference (MPD) is used to measure the difference between critical design parameter values, including a node's energy level, the selfish probability, and the unselfish probability of a node at time t in two consecutive iterations. The iteration stops when the MPD is below a threshold 1 percent (%) for all nodes in the system. The calculation of the MPD of parameter X for node i is given by:

$$MPD_i^X = \frac{\sum_t^{max} D_i^X(t)}{N_{interval}} \quad where \;\; D_i^X(t) = \frac{\left|X_i^{j+1}(t) - X_i^j(t)\right|}{X_i^j(t)} \tag{13}$$

where $X_i^j(t)$ indicates the value of parameter X of node i at time t in the j^{th} round of iterations, *max* is the maximum time measured, and $N_{interval}$ the number of time points. We compute MPD for each node's probabilities of being alive, selfish, and unselfish. The node SPN subnet after convergence yields the trust probabilities for three trust components

(i.e., unselfishness, energy, and intimacy). The trust metric is then calculated as explained in Section 2.2.

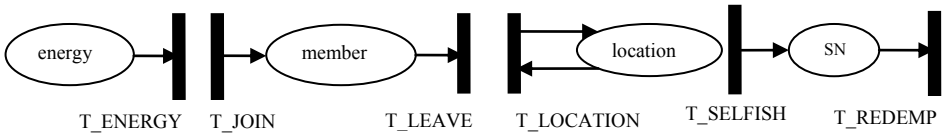

Fig. 2. SPN subnet for describing the status of a node.

Fig. 2 shows the *SPN subnet*. The subnet describes a node's mobility behavior, join and leave events (i.e., GCS membership status), energy consumption, and selfish behaviors with a redemption mechanism provided. The transition T_LOCATION is triggered when a node moves to a randomly selected area in one of four different directions from its current location with the rate calculated as S_{init}/R based on an initial speed (S_{init}) and wireless radio range (R). We assume that inter-arrival times of a node's join and leave requests are exponentially distributed with rates λ and μ respectively. Place *energy* represents the current energy level of a node.

An initial energy level is assigned according to node heterogeneity information. In our analytical model, we randomly generate a number E_{init} in the range of $[E_{min}, E_{max}]$ based on the uniform distribution. A token is taken out when transition T_ENERGY fires. The transition rate of T_ENERGY is adjusted on the fly based on a node's state; it is lower when a node becomes selfish to save energy or when a node changes from a member to a non-member, following the energy consumption model in [5]. We assume that T seconds will be taken to consume one energy token when a member node has no selfish 1-hop neighbors. We use this energy consumption model for adjusting the time taken to consume one token in place *energy* based on a node's status. Therefore, depending on the node's status, its energy consumption behavior is dynamically changed.

Place *SN* represents whether a node is selfish or not. If a node becomes selfish, a token goes to *SN* by triggering T_SELFISH. When a node becomes altruistic again, transition T_REDEMP is triggered. A node switches between selfish and altruistic following the demand and pricing theory described in Section 3.2 below. The SPN model in Fig. 2 yields the trust components $P_j^X(t)$ where X = energy, unselfishness, and location (to derive intimacy), from which the n-hop trust components and the trust metric can be computed via Equations 1-10.

3.2 Demand and Pricing Model

The basic formula to represent the relationship between demand and pricing in a market is given by [4, 2]:

$$\lambda_i = \alpha_i (v_i)^{-\varepsilon_i} \ \ where \ \ \varepsilon_i > 1, \alpha_i > 0 \tag{14}$$

where λ_i is the demand arrival rate and v_i is the pricing of service i while α_i and ε_i are constants correlating λ_i and v_i. Service demand is affected by pricing changes where the elasticity constant ε_i is a key determinant. A market is said to be elastic if $\varepsilon_i > 1$, as assumed here. In such a case lowering the price leads to increase in demand. The elasticity ε_i can be obtained from statistical data describing past market conditions.

We adopt DP theory to decide whether a node should behave selfishly or altruistically based on both individual benefit (i.e., saving energy) and global interest (i.e., serving tasks). We use transition T_SELFISH in our SPN model (described in Section 3) to model a node's changing behavior from altruistic to selfish. Note that remaining energy of a node, mission difficulty, and degree of unselfishness of 1-hop neighbors are used for the place of "price" to apply DP theory in Equation 14. The transition rate to transition T_SELFISH is modeled by:

$$rate(T\_SELFISH) = \frac{f(E_{remain})f(M_{difficulty})f(S_{degree})}{T_{gc}} \quad (15)$$

where $f(x) = \alpha x^{-\varepsilon}$, E_{remain} is the level of current energy (indicated as $mark(energy)$ in SPN model of Section 3), $M_{difficulty}$ is the difficulty level of a given mission where a higher value indicates a tougher mission, and S_{degree} is the degree of selfishness where a higher number refers to more selfishness. We define S_{degree} as the ratio of selfish nodes to unselfish nodes among 1-hop neighbors (refer to [5] for the calculation of the number of selfish/unselfish 1-hop neighboring nodes). T_{gc} is the interval for disseminating a group communication packet where a node's selfishness can be observed. In the context of DP theory, residual energy, mission difficulty and neighborhood selfishness are the prices, and the transition rate from altruistic to selfish is the demand. Equation 15 implies the following:

- $f(E_{remain})$: If a node has a higher level of energy, it is less likely to be selfish.
- $f(M_{difficulty})$: If a node is assigned a tougher mission, it is less likely to be selfish.
- $f(S_{degree})$: If a node observes high selfishness among its 1-hop neighbors, it is less likely to be selfish.

Similarly, we use a transition T_REDEMP in the SPN model (shown in Fig. 2 of Section 3.1) to model the redemption of a node, changing its behavior from selfish to altruistic. The rate to transition T_REDEMP is modeled as:

$$rate(T\_REDEMP) = \frac{f(E_{consumed})f(M_{easiness})f(H_{degree})}{T_{status}} \quad (16)$$

where $f(x) = \alpha x^{-\varepsilon}$, $E_{consumed}$ is the level of consumed energy $(E_{init} - E_{remain})$ where E_{remain} refers to the remaining energy, $M_{easiness}$ is the easiness level of a given mission where a higher number indicates an easier mission (e.g., $M_{max-difficulty} - M_{difficulty}$), and H_{degree} is the degree of unselfishness where a higher number means more unselfishness among 1-hop neighbors. We define $H_{degree} = 1/S_{degree}$ as the ratio of unselfishness to selfishness (refer to [5] for the calculation of the number of selfish/unselfish 1-hop neighboring nodes). A node is given a chance to be redeemed (from selfish to altruistic) in every reevaluation period T_{status} corresponding to the status exchange interval for trust evaluation. Equation 16 implies the following:

- $f(E_{consumed})$: If a node has consumed more energy, it is less likely to redeem itself. This means that if a node has low energy, it may want to further save its energy by staying selfish.
- $f(M_{easiness})$: If a node is assigned an easier mission, it is less likely to redeem itself.

- $f(H_{degree})$: If a node observes high unselfishness among its 1-hop neighbors, it is less likely to redeem itself and may continue to stay selfish in order to save its energy.

3.3 Calculation of Trust Components

The trust value of node *j* by node *i* is calculated based on the information on nodes collected from the *SPN subnet* upon convergence. We calculate the trust probabilities for the three components (i.e., $P_j^X(t)$) of trust based on a reward assignment technique described below. Specifically, the average value, $X(t)$, of a physical property at time *t*, is the state probability weighted sum of the values at various states, i.e.,

$$X(t) = \sum_{i \in S} (r_i * P_i(t)) \tag{17}$$

where *S* is a set of states that meet particular conditions, $P_i(t)$ is the probability that the system is in state *i* at time *t*, and r_i is the reward or value assigned to the physical property in state *i*. The reward assignment technique allows us to compute a node's trust component values, say P_j^X where X can be unselfishness and energy, and location information $P_j^{loc=m}$ to derive intimacy trust component values at time *t*. We use the same reward assignment technique to obtain $P_{j,unselfish}^{loc=k}(t)$ and $P_{j,selfish}^{loc=k}(t)$, the probability that node *i* is located in area *k* as being selfish or unselfish.

Table 1. Reward functions.

Component	Conditions Satisfied in S
$\boldsymbol{P^{energy}(t)}$	$mark(energy) > 0$
$\boldsymbol{P^{unselfish}(t)}$	$(mark(member) > 0)$ & $(mark(SN) == 0)$ & $(mark(energy) > 0)$
$\boldsymbol{P^{loc=k}(t)}$	$(mark(location) == k)$ & $(mark(member) > 0)$& $(mark(energy) > 0)$
$\boldsymbol{P_{unselfish}^{loc=k}(t)}$	$(mark(member) > 0)$ & $(mark(SN) == 0)$ & $(mark(energy) > 0)$ & $(mark(location) == k)$
$\boldsymbol{P_{selfish}^{loc=k}(t)}$	$(mark(member) > 0)$ & $(mark(SN) > 0)$ & $(mark(energy) > 0)$ & $(mark(location) == k)$

Table 1 specifies the conditions to be satisfied for states in set *S* in calculating $P^{energy}(t)$, $P^{unselfish}(t)$, $P^{loc=k}(t)$, $P_{unselfish}^{loc=k}(t)$, and $P_{selfish}^{loc=k}(t)$. When the specified conditions are satisfied, a reward of a 1 is assigned. Based on $P_j^{loc=k}(t)$ so obtained, various *k*-hop trust probabilities can be computed. For example, the trust value for the intimacy component when *i* and *j* are 1-hop apart, $P_{i,j}^{intimacy}$, can also be obtained as described in Section 2.2.

4 Numerical Results and Analysis

This section shows the results obtained through the evaluation of our hierarchical SPN model. Table 2 summarizes the parameters and their default values used in this case study.

Table 2. Default parameter values used.

Param	Value	Param	Value	Param	Value
k_{recom}	3	N	150	α, ε	0.01, 2
R	250 m	T_{status}	60*10 s	E_{init}	[6, 12] hrs
λ	1/(60*60)	T_{beacon}	60*2 s	T_{gc}^{M1}	60*10 s
μ	1/(60*60*4)	T	60*60 s	T_{gc}^{M2}	60*5 s
β	0.8: 0.2	S_{init}	(0, 2) m/s	T_{gc}^{M3}	60 s

As shown in Table 2, we set the elasticity constant ε to 2. To maintain a sufficient number of active nodes in the network, the ratio of node join and leave is set to 4:1. The energy level assigned to each node has an average value of 9 hours, representing a reasonable average battery life for mobile devices.

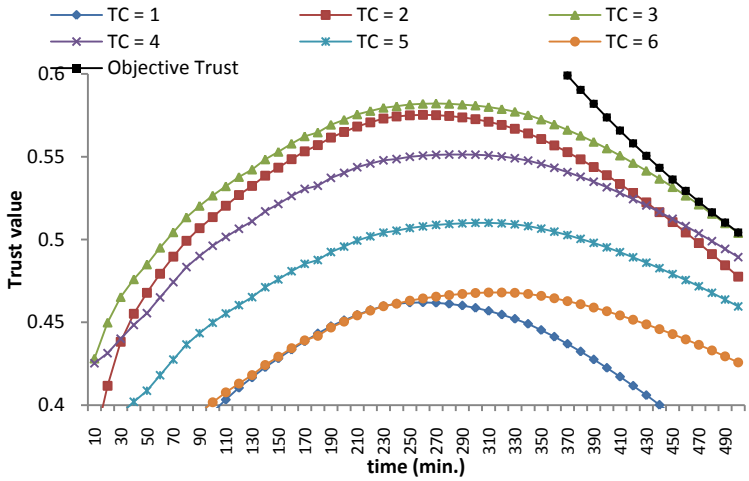

Fig. 3. System trust value versus time, for various trust chain lengths.

Fig. 3 shows the average trust values of all nodes evaluated by all nodes (hereafter called "system trust") over time parameterized by the length of the trust chain (labeled as TC) under M1. We notice that the maximum trust values are obtained with TC = 3. The effect of using different lengths of TC on trust levels is already examined in our prior work [5]. Note that objective trust predicted via Equation 11 is always larger than the subjective trust computed via Equations 1-10. Thus units are not exposed to unnecessary risk (as noted by Josang *et al.* [8]); but this also implies that there is some missed reward.

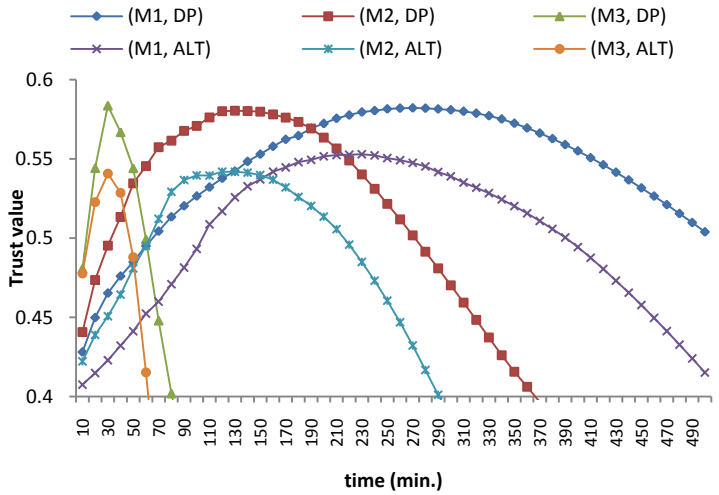

Fig. 4. System trust value over time under DP and ALT, and for various missions with TC = 3.

Fig. 4 depicts the maximum system trust values identified by TC = 3. We compare the demand and pricing based system (labeled as DP) with the solely altruistic system (labeled as ALT) when different missions are given (labeled as M1, M2, and M3, where M3 requires the highest workload in this case study). As expected, the system assigned M3 has the lowest trust values while the system assigned M1 performs the best, showing the highest trust values. Further, DP significantly performs better than ALT for the same mission M1 or M2 and its effect is more pronounced as time progresses. Our composite trust metric takes into account both the energy level as well as the degree of unselfishness (or cooperation). As a result, the use of DP yields higher trust values. Under M3, the mission difficulty is increased; hence, nodes do not behave selfishly in the beginning. Thus, we note that DP performs only slightly better than ALT in the beginning. Because of the increased workload, energy consumption is larger, and the system lifetime is correspondingly shorter under M3 when compared with M1 and M2.

Table 3. Percentage of cooperative nodes versus system lifetime when $T_{value} > 0.5$.

	(M1, DP)	**(M1, ALT)**	**(M2, DP)**	**(M2, ALT)**	**(M3, DP)**	**(M3, ALT)**
% of cooperative nodes when $T_{value} > 0.5$	> 27%	> 65%	> 35%	> 54%	> 25%	> 78%
Lifetime when $T_{value} > 0.5$	26400 s	17400 s	14400 s	9600 s	3200 s	1800 s

Selfish behaviors can increase system lifetime by saving energy; on the other hand, if too many nodes are selfish, there will be not an adequate number of cooperative nodes, and the mission will fail. Next we examine the maximum degree of selfishness that can be allowed in order to improve successful mission completion. Suppose the mission can be executed successfully as long as there is at least one cooperative node in an area and a node maintains its trust level at least above the ignorance level, 0.5. Table 3 shows the percentage of cooperative nodes when the system drop dead trust value (T_{value}) is at least

above 0.5 under DP and ALT for various types of missions. Table 3 also shows the system lifetime, the total time when T_{value} is above 0.5. ALT has a larger number of cooperative nodes; but unlike DP, it does not take into account energy, and thus it is unable to maintain a high trust level. We also see that as the mission difficulty decreases, the system is able to prolong its lifetime under DP, maintaining at least the minimum required number of cooperative nodes.

5 Conclusions

In this paper, we developed and analyzed a trust management protocol for a mission-driven GCS in MANETs; we used demand and pricing theory to model selfish and altruistic behaviors to balance individual welfare (i.e., saving energy) versus global welfare (i.e., serving tasks and completing the mission). Our trust management protocol based on DP theory allows each node to dynamically decide if it should stay selfish or altruistic in response to changing environmental conditions so that the overall system trust level can be maximized. We developed a probability model based on SPN to describe the behavior of a large scale GCS operating under the proposed trust management protocol. The results show that our trust management protocol outperforms one that only encourages altruistic behaviors, especially when the mission assigned to the GCS demands light to medium workloads; under these cases our protocol can best explore the tradeoff between energy saved due to selfishness versus quick energy drainage due to altruism.

As future work, we plan to (1) examine the sensitivity of the results obtained with respect to α and ε which are two important parameters in the demand and pricing theory underlying our trust management protocol; (2) develop a more sophisticated mission model considering the effect of mission attributes such as risk, deadline, and workload requirements; (3) analyze the impact of imperfect detection of node failures and attacks; and (4) consider group-based mobility models.

Acknowledgement

This project is supported in part by an appointment to the U.S. Army Research Laboratory Postdoctoral Fellowship Program administered by the Oak Ridge Associated Universities through a contract with the U.S. Army Research Laboratory.

References

1. Adams, W. J., Hadjichristofi, G. C. and Davis, N. J.: Calculating a node's reputation in a mobile ad hoc network. In Proc. of the 24th IEEE Int'l Performance Computing and Communications Conf. (IPCCC'05), pp. 303-307, Phoenix, AX (April 2005)
2. Aldebert, M., Ivaldi, M., and Roucolle, C.: Telecommunications demand and pricing structure: an economic analysis. Telecommunication Systems, 25(1-2), 89-115 (Jan. 2004)
3. Capra, L.: Toward a human trust model for mobile ad-hoc networks. In Proc. of the 2nd UK-UbiNet Workshop, Cambridge University, Cambridge, UK (May 2004)
4. Case, K. E., and Fair, R. C. : Principles of Economics (5th ed.), Prentice-Hall (1999)

5. Cho, J. H., Swami, A., and Chen, I. R.: Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks. In 2009 IEEE/IFIP Int'l Symposium on Trusted Computing and Communications, Vancouver, Canada (Aug. 2009)
6. Cho, J. H., and Swami, A.: Towards trust-based cognitive networks: a survey on trust management for mobile ad hoc networks. In 14th Int'l Command and Control Research and Technology Symposium, Washington D.C., U.S.A. (June 2009)
7. Falcone, R. and Castelfranci, C.: Social trust: a cognitive approach. Trust and Deception in Virtual Societies, 55-90, Kluwer Academic Publishers (2001)
8. Josang, A. and LoPresti, S.: Analyzing the relationship between risk and trust. In Proc. 2nd Int'l Conf. Trust Management (iTrust'04), LNCS, pp. 135-145, Springer-Verlag (2004)
9. Li, M., Kamioka, E., and Yanada, S.: Pricing to stimulate node cooperation in wireless ad hoc networks. IEICE Transactions on Communications, E90-B (7), 1640-1650 (2007)
10. Marbach, P. and Qiu, Y.: Cooperation in wireless ad hoc networks: a market-based approach. IEEE/ACM Transactions on Networking, 13 (6), 1325-1338 (Dec. 2005)
11. Miranda, H., and Rodrigues, L.: Friends and foes: preventing selfishness in open mobile ad hoc networks. In Proc. of the 23rd Int'l Conf. on Distributed Computing Systems Workshops, pp. 440-445 (May 2003)
12. Moe, M. E. G., Helvik, B. E., and Knapskog, S. J.: TSR: Trust-based secure MANET routing using HMMs. In Proc. of the 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, pp. 83-90, Vancouver, Canada (Oct. 2008)
13. Papadimitriou, C. H.: Algorithms, games, and the Internet. In Proc. of the 33rd Annual ACM Symposium on Theory of Computing, Hersonissos, Crete, Greece, pp. 749-753 (July 2001)
14. Rappaport, P., Alleman, J., and Taylor, L. D.: Household demand for wireless telephony: an empirical analysis. In Proc. of the 31st Annual Telecommunications Policy Research Conf., Arlington, VA (Sept. 2003)
15. Roughgarden, T. : Selfish routing and the price of anarchy," The MIT Press, Cambridge, Massachusetts, London, England (2005)
16. Soltanali, S., Pirahesh, S., Niksefat, S., and Sabaei, M.: An efficient scheme to motivate cooperation in mobile ad hoc networks. In Int'l Conf. on Networking and Services (ICNS'07), pp. 98-103, Athens, Greece (June 2007)
17. Steiner, M., Tsudik, G. and Waidner, M.: Diffie-Hellman key distribution extended to group communication. In CCS'96 Proc. 3rd ACM Conf. on Computer and Communications Security, pp. 31–37, New York, NY, USA(1996)
18. Thomas, R. W., Friend, D. H., DaSilva, L. A., and MacKenzie, A.B.: Cognitive networks: adaptation and learning to achieve end-to-end performance objectives. IEEE Communications Magazine: Topics in Radio Communications, 44(12), 51-57, Toronto, Canada (Dec. 2006)
19. Virendra, M., Jadliwala, M., Chandrasekaran, M., and Upadhyaya, S.: Quantifying trust in mobile ad-hoc networks. In Proc. of the Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems (KIMAS), pp. 65-70 (April 2005)
20. Wang, Y., Giruka, V. C., and Singhal, M.: Truthful multipath routing for ad hoc networks with selfish nodes. Journal of Parallel and Distributed Computing, 68(6), 778-789 (2008)
21. Yan, L., and Hailes, S.: Designing incentive packet relaying strategies for wireless ad hoc networks with game theory. IFIP Int'l Federation for Information Processing: Wireless Sensor and Actor Networks II, 264, 137-148 (2008)
22. Yilmaz, O. and Chen, I. R.: Elastic threshold-based admission control for QoS satisfaction with reward optimization for servicing multiple priority classes in wireless networks. Information Processing Letters, 109 (15), 868-875 (July 2009)
23. Zhao, D.: Access control in ad hoc networks with selfish nodes. Wireless Communications and Mobile Computing, 6(6), 761-772 (2006)
24. Zhang, Q. and Agrawal, D. P.: Impact of selfish nodes on route discovery in mobile ad hoc networks. In IEEE Global Telecommunications Conf. (GLOBECOM'04), vol. 5, pp. 2914-2918 (Dec. 2004)