On Tradeoffs between Trust and Survivability Using a Game Theoretic Approach

Jin-Hee Cho, Ananthram Swami

On Tradeoffs between Trust and Survivability using a Game Theoretic Approach

Jin-Hee Cho and Ananthram Swami

U.S. Army Research Laboratory, Communication and Information Sciences Directorate,
2800 Powder Mill Rd., Adelphi, MD 20783
{jinhee.cho, ananthram.swami}@us.army.mil

Abstract. Military communities in tactical networks must often maintain high group solidarity based on the trustworthiness of participating individual entities where collaboration is critical to performing team-oriented missions. Group trust is regarded as more important than trust of an individual entity since consensus among or compliance of participating entities with given protocols may significantly affect successful mission completion. This work introduces a game theoretic approach, namely *Aoyagi*'s game theory based on positive collusion of players. This approach improves group trust by encouraging nodes to meet unanimous compliance with a given group protocol. However, when any group member does not follow the given group protocol, they are penalized by being evicted from the system, resulting in a shorter system lifetime due to lack of available members for mission execution. Further, inspired by aspiration theory in social sciences, we adjust an expected system trust threshold level that should be maintained by all participating entities to effectively encourage benign behaviors. The results show that there exists the optimal trust threshold that can maximize group trust level while meeting required system lifetime (survivability).

Keywords: economic modeling, trust network, positive collusion, aspiration, rationality, wireless mobile networks.

1 Introduction

Collaboration is critical in team-oriented missions. This is particularly important in military communities engaged in tactical operations where it is important to maintaining group solidarity based on the trustworthiness of the individual entities. Communal compliance to a common protocol can significantly affect successful mission completion. In the military, group trust is often considered to be more important than the trust of any single entity. Rewards and penalties are natural ways of enforcing or encouraging expected behaviors.

Economic models have been used to support decision making problems such as efficient resource allocations or encouraging cooperative behaviors in the communication and networking field [17]. We employ a game theoretic approach, namely *Aoyagi*'s game theory [2], to introduce the concept of positive collusion that has been used in economics. This approach improves group trust by using positive

collusion to encourage unanimous compliance with a given group protocol. That is, the entire system is penalized or rewarded regardless of which individual entity misbehaved or behaved, so that group members are stimulated to pressure each other to reach their common goal [16]. As motivation, consider the scenario in which a commander expects all participating members in a mission team to maintain an expected trust threshold. The overall trust metric is based on trust components derived from the characteristics of the composite network. The trust components include processing delay per packet, cooperativeness (i.e., packet dropping or forwarding), data integrity (i.e., message forgery or modification or lying), and inherent rationality referring to the degree of willingness to follow a given protocol in order to maximize an entity's utility. Further, we assume that an entity is cognitive in that it will make a decision to improve its behavior only when the changed behavior will immediately or ultimately increase its own trust or group trust as well as help the system avoid penalties.

This work is also inspired by aspiration theory in social sciences in that an appropriate aspiration (or goal) level given to a group will effectively increase the group's performance without letting group members feel frustrated or failed. Hoppe [10] defined *aspiration* as "a person's expectations, goals, or claims on his own future achievement." He emphasized that determining "success" or "failure" does not depend only on its objective goodness, but also on whether the level of aspiration may be reached or not. The underlying idea is that entities work hard to avoid failure where failure is defined as being below the aspiration level, a standard set implicitly or explicitly by peers or the community at large. Aspiration theory has been used in fields such as psychology [8], sociology [3], education [16], economics [7], and computer science (artificial intelligence) [9].

Economic theories are popularly applied where resources are restricted such as in wireless networks (e.g., mobile ad hoc networks, sensor networks, wireless tactical networks) [11], [12]. Very recently, Ng and Seah [14] used *Aoyagi*'s game theory to improve cooperation of nodes in resource-restricted wireless networks where nodes are more likely to be selfish. In [14], a node's selfishness is assessed by examining its packet forwarding or dropping behaviors. Our work differs from [11], [12], [14] in that we consider multi-layer composite trust as behaviors to improve and investigate the tradeoff between trust and system survivability.

Aspiration level has been used as an attribute that an agent considers to express its preference [4], [9]. However, our work applies a group aspiration level based on the idea that individuals tend to follow the collective norm of the group to which they belong. Our work models a wireless tactical network where an entity is a mobile device carried by a human being (e.g., soldier) and identifies optimal trust threshold (as the goal level for members to achieve) to maximize group trust while meeting system survivability.

The main contributions of this paper are as follow. First, we employ a unique game theoretic approach, called *Aoyagi*'s game theory, to model a tactical network where a trusted commander desires participating entities to follow a given protocol with the goal of reaching an acceptable system trust level. Second, we propose a composite trust metric that captures various aspects of an entity in a composite network comprising communication, information, social, and cognitive networks. Third, inspired by aspiration theory from social sciences, we adopt aspiration level (i.e., trust

threshold in this study) to effectively stimulate an entity towards desired behaviors. Fourth, we develop a mathematical model using Stochastic Petri Nets (SPN) [5] to study the tradeoff between group trust and system survivability in the presence of misbehaving nodes and under resource constraints. Lastly, we identify the optimal trust threshold that maximizes group trust level while meeting system survivability.

The rest of this paper is organized as follows. Section 2 describes the system designs, assumptions, proposed composite trust metric, system failure conditions, and computations of performance metrics. Section 3 shows our performance model developed using SPN techniques and how to compute the metrics in our SPN model. Section 4 discusses numerical results obtained from our SPN model, and provides physical interpretations. Section 5 concludes this paper and suggests future research directions.

2 System Model

We consider a wireless tactical network where a trusted third party, called a commander node (CN), coordinates or gives orders to member nodes in the network, the so called "mission group." Communications in the network may require multiple hops. A group maintains a symmetric key, called a group key, in order to maintain secrecy (forward and backward secrecy) among legal members [15]. We assume that when nodes are evicted from the mission group, a new key is distributed to the remaining members by the CN based on a centralized key management protocol [15] Each node disseminates its beacon message (e.g., "I am alive") to stay connected to the group. Each node is also assumed to periodically disseminate packets related to group activities in terms of group communication, trust update, and neighbors' monitoring.

The network is heterogeneous where each node can have different characteristics such as different degree of cooperativeness (propensity to forward packets), integrity (message forgery or modification, or lying), processing delay per packet, and rationality (willingness to follow a given protocol). Except for the processing delay, the three characteristics are assumed to be drawn from a uniform distribution with a prescribed range, and are assumed known in advance to the CN. These four characteristics are reflected as components of our proposed composite trust metric, discussed in Section 2.1. Note that an entity is assumed to be a mobile device carried by a human (e.g., soldier). We model dynamically changing behaviors related to cooperativeness, data integrity, and capability in processing delay. However, we model a node's rationality as a static trust value that affects the attitude to improve its behavior. This is because we assume that an entity's rationality or disposition does not change over the short period of mission duration. Further, we assume that an entity's willingness to comply with a common protocol is related to its rationality, seeking to increase its utility by avoiding penalty. If the entity is an attacker and has a different goal such as disrupting the entire system, it may not improve its behaviors to attain the given trust threshold. However, in this case, the system penalizes the misbehaving node by evicting it, ultimately eliminating any chance of participation in any group

activities as a legal member. Thus, a smart attacker may not easily manifest misbehaviors that can be promptly penalized by the system.

In our proposed protocol, we follow a rule similar to that described in *Aoyagi*'s game theory with some modifications. All nodes are expected to maintain the trust threshold given by the CN. The trust threshold is an expected goal that each node needs to achieve in order to avoid penalty. Each node periodically reports its self-computed trust value to the CN, the so called "public signal." The CN collects trust values of all participating nodes based on each node's self-reported *public* signals and computes the group trust, an average trust level of all group members. Only when *all* nodes say they are observing the target trust level, do they not receive any penalty. We call this the "collusion phase." We use "collusion" as a positive term different from "collusion" among compromised nodes. Otherwise, a certain number of the nodes that are not maintaining the given trust threshold will be evicted from the mission group. We call this "feedback phase," meaning that some nodes are penalized by being evicted and the existing members need to improve their behaviors so as not to be penalized again. The CN checks the degree of rationality of the nodes and evicts a certain portion of them.

On the other hand, a rational node also may lie to avoid the penalty even if it is not maintaining the given trust threshold. Further, a node may not follow the rule in order to achieve its attack goals if it is an attacker. To alleviate this effect, we assume that each node is capable of monitoring its neighboring nodes (e.g., via Pathrater [13]) based on direct observations and can detect whether public signals of its neighbors are true; nodes report lying behaviors to the CN. If a lying node is reported, even if all nodes claim compliance to the given trust threshold, the CN will proceed with "feedback phase" so that the lying nodes are all evicted from the system and the remaining member nodes may need to improve their behaviors. Since each node's direct monitoring capability is not perfect, we also consider false positive and false negative probabilities of the monitoring mechanism of each node.

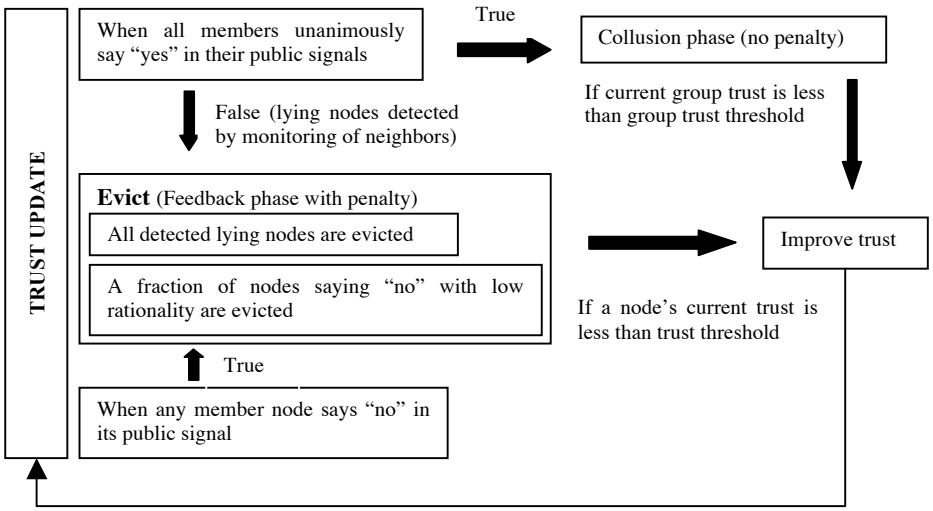

Fig. 1. The proposed protocol.

In our model, each node is required to keep its trust level above the threshold as noted earlier; in addition, the average trust level of the group must exceed a desired value which we call the group trust threshold. Thus even if an individual node's trust value exceeds the individual trust threshold, it could make an extra effort to improve the average group trust level. Upon the end of each trust update, the CN will inform the current group trust level to group members. Thus, each node can make use of the informed current group trust value to decide whether it will improve its behaviors, as explained in Fig. 1. There is no penalty if the group threshold is not met, so far as all nodes are maintaining the given trust threshold individually. Fig.1 describes the proposed protocol. Notice that all detected lying nodes are evicted without forgiveness. However, if a node is not maintaining the prescribed trust threshold, but honestly says so, then it is only penalized if its rationality is low. We model a node's ability to change its behaviors is directly proportional to its degree of rationality since nodes with low rationality are assumed to be not capable of changing their behaviors sufficiently. Hence, a fraction of the honest but underperforming nodes with lowest rationality values are evicted from the mission group. This discourages a node's lying behavior by giving higher penalty than not lying. We assume that a node does not lie about its trust status when it is above the trust threshold. That is, we do not consider the case when a node with the trust value above the trust threshold says "no" in its public signal to trigger the feedback phase.

We assume that a node's misbehaviors including dropping packets or modifying messages are only observed in packets related to group communications for mission execution, and not other activities such as disseminating packets related to trust update or neighbor monitoring. The trust update related packets (i.e., public signals by group members, group trust values by the CN) are assumed to be acknowledged by recipients and error-free.

We define two security failure conditions that affect system lifetime. First, the system fails when a certain fraction of member nodes are malicious. Second, the system fails when too few member nodes are available for successful mission completion due to the eviction process. We give detailed definitions of the two failure conditions in Section 2.2.

The mission group is penalized by evicting detected lying nodes and a fraction of nodes not maintaining the trust threshold (but honestly saying so) as shown in Fig. 1. The procedure described in Fig.1 is regarded as one game where the proposed mission group plays a repeated game upon every trust update during mission execution. Each node, as a *self-interested agent* [6], seeks to maintain high trust level by improving its benign behaviors so that it can stay in the system with full access to resources as a legal group member.

We observe that there is a tradeoff between maintaining trust level and system survivability. If the trust threshold is high, the system is more prone to be penalized; it will take a longer time for the system to reach the required trust level, and more nodes are likely to be evicted in this longer convergence period. Consequently, system survivability will be low. However, the efforts to reach the trust threshold will allow surviving entities to increase their trust level ultimately.

2.1 Composite Trust Metric

We consider four components of trust derived from four different network layers: communication, information, social, and cognitive networks in order to assess the trustworthiness of a node. The four trust components are:

- **Communication trust** is based on a node's capability to process data measured by the *delay* incurred in forwarding or processing a packet. It could be affected by queue length, congestion at downstream nodes, and quality of outgoing links. This trust component can be computed from the number of packets received by the node.
- **Information trust** is based on *data integrity*, whether or not a node modifies or forges received messages or lies (e.g., lying about its trust status). This property can be computed by examining the integrity of the packets sent by the node.
- **Social trust** is assessed from the degree of *cooperativeness* of a node, and can be estimated from the frequency of packet forwarding or dropping by the node.
- **Cognitive trust** is a measure of *rationality* which is defined as the degree of willingness to follow a given protocol. This information is assumed to be known to the CN based on prior knowledge about the node population.

Recall that this work defines rationality as the willingness to comply with a common protocol. Note that rationality is represented as a static value that stays constant for the entire mission execution, based on the conjecture that disposition of human beings will only change very gradually, assuming that the mission duration is relatively short, less than a day. We relate a node's rationality with the willingness to improve the other three trust components. That is, a node with high rationality will change its behavior more aggressively to improve cooperativeness or data integrity. This relationship (rationality versus cooperativeness or data integrity) is justified in that each entity desires to reduce the possibility of failure by improving its behaviors with the goal of reaching the given trust threshold. Thus, the "rationality" component will indirectly affect the overall trust by influencing the attitude to improve cooperativeness and data integrity behaviors, as shown in Equation 2.

A node's self-reported trust value to the CN is based on three trust components, cooperativeness, data integrity, and processing delay where cooperativeness and data integrity are updated based on its rationality. The self-reported trust value of node i at time t is given as:

$$T_i(t) = w_1 P_i^{\text{cooperativeness}}(t) + w_2 P_i^{\text{data-integrity}}(t) + w_3 P_i^{\text{delay}}(t). \quad (1)$$

Each of the above three trust components is a real number in the range of [0, 1] and the weights sum to unity: $w_1 + w_2 + w_3 = 1$. A node will change its behaviors in terms of the cooperativeness and data integrity trust components, if and only if its projected trust value ($PT_i^X(t)$) is larger than its current trust value ($T_i(t - \Delta t)$) and either its current trust value is less than the trust threshold (T_{th}) or the current group trust (average trust of all member nodes) is less than the group trust threshold (T_{th}^{group}), as shown in Equation 2 below. Trust component X value of node i at time t is obtained by:

$$PT_i^X(t) = T_i^X(t-\Delta t) + f_{feedback}(t)P_{i,change}^X(t) \quad (2)$$

$$P_{i,change}^X(t) = c[P_i^{rationality}(1-P_i^X)]$$

$$f_{feedback}(t) = \begin{cases} 1 \text{ if } (T_i(t-\Delta t) < T_{th} \;||\; GT(t-\Delta t) < T_{th}^{group}) \\ 0 \text{ otherwise} \end{cases}$$

$$PT_i(t) = w_1 PT_i^{cooperativeness}(t) + w_2 PT_i^{data-integrity}(t) + w_3 PT_i^{delay}(t)$$

$$\text{if}((PT_i(t) - T_i(t-\Delta t)) > 0 \;\&\&\; (T_i(t-\Delta t) < T_{th} \;||\; GT(t-\Delta t) < T_{th}^{group}))$$

$$T_i(t) = PT_i(t);$$

$$\text{else } T_i(t) = T_i(t-\Delta t);$$

$$1 \geq T_{th}^{group} > T_{th} > 0, \qquad \Delta t = T_{update}$$

Here P_i^X is the original value of trust component X (cooperativeness or data integrity). $P_i^{rationality}$ represents node i's rationality initially given; $P_{i,change}^X(t)$ estimates how much node i can improve its behavior X upon each feedback and c is a constant. If the node's current trust level is below the trust threshold (T_{th}) or the current group trust level is below the group trust threshold (T_{th}^{group}), then the node accepts the feedback ($f_{feedback}(t) = 1$). Otherwise, the node stays in the previous trust at time t-Δt. As noted in Equation 2, we assume that the group trust threshold T_{th}^{group} is larger than the individual threshold T_{th}.

The processing delay trust component is based on the number of packets received by a node which is affected by the number of group members and their cooperative behaviors. This trust component value is estimated as:

$$P_i^{delay}(t) = \min\left[D/N_i^{packet}(t), 1\right] \quad (3)$$

where D is an allowed constant time delay. $N_i^{packet}(t)$ is computed based on the number of packets node i received for forwarding to other nodes or as a destination node related to all system activities (i.e., monitoring, beacon, public signal, group communication, and trust update). The expected number of packets received or forwarded by a node can be estimated via its path centrality. Note that $PT_i^{delay}(t)$ in Equation 2 is also computed based on Equation 3.

2.2 Failure Conditions

We define "system survivability" or "lifetime" as the time to first system or security failure: loss of system integrity or loss of service availability. Therefore, the system fails when either of the two conditions below is true.

• **Failure Condition 1 (FC1)**: The system fails when the fraction of member nodes that are malicious (i.e., modify or forge message, or lie) exceeds the system tolerance level ($TH_{malicious}$), leading to a security failure, *loss of system integrity*. FC1 is computed by:

$$M_{system}(t) = \sum_{i \in G(t)}^{all} (1 - P_i^{data-integrity}(t)) \quad (4)$$

$$FC1 = \begin{cases} 1 \text{ if } M_{system}(t) > TH_{malicious} \\ 0 \text{ otherwise} \end{cases}$$

Here G(t) is the set of member nodes at time t and $TH_{malicious}$ is the maximum number of malicious nodes that can be tolerated; and $M_{system}(t)$ is the average number of malicious nodes in the system.

• **Failure Condition 2 (FC2)**: The system fails if the total number of evicted nodes exceeds a threshold ($TH_{mission}$). Equivalently, failure occurs when too few member nodes are available for successful mission completion. This leads to system performance failure, called *loss of service availability*. FC2 is computed by:

$$FC2 = \begin{cases} 1 \text{ if } N_{evicted}(t) > TH_{mission} \\ 0 \text{ otherwise} \end{cases} \quad (5)$$

$N_{evicted}(t)$ is the number of nodes evicted by time t and $TH_{mission}$ is the minimum number of nodes required for successful mission completion.

2.3 Metrics

We use two metrics to measure performance: system survivability and overall group trust.

System Survivability Probability ($P_{survivability}(t)$): This metric indicates the probability that the system is alive at time t. This is defined by:

$$P_{survivability}(t) = \begin{cases} 0 \text{ if FC1 or FC2 is true;} \\ 1 \text{ otherwise;} \end{cases} \quad (6)$$

Overall Group Trust ($T_{group}(t)$): This metric refers to the average group trust. Trust value of each node, $T_i(t)$, is computed via Equation 1 and $T_{group}(t)$ is calculated as:

$$T_{group}(t) = \frac{\sum_{i \in G(t)}^{all} T_i(t)}{|G(t)|} \quad (7)$$

G (t) is the set of current members at time t.

3 Performance Model

We have developed a mathematical model using Stochastic Petri Nets (SPN) [5]. This section describes our SPN model of the proposed system and its lifecycle. Further, this section addresses how the metrics (system survivability and overall group trust) are computed in our SPN.

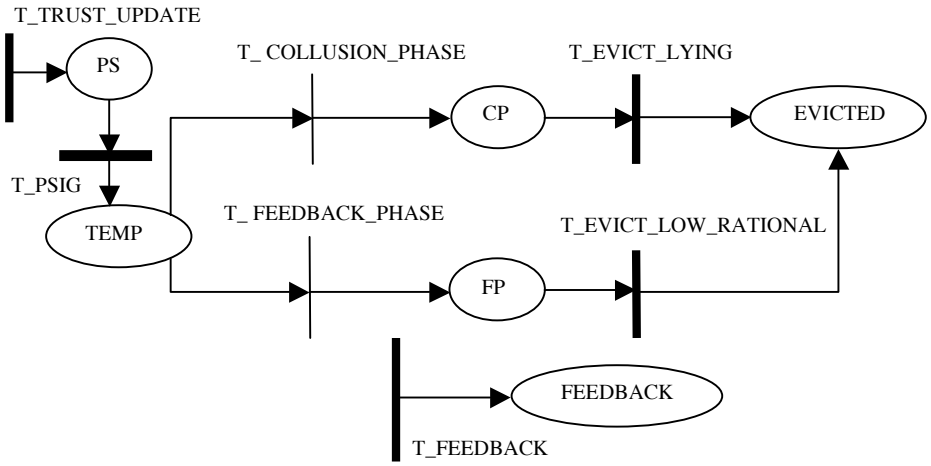

Fig. 1. SPN Model.

Fig. 1 describes our SPN model; Places (i.e., PS, TEMP, CP, FP, EVICTED, FEEDBACK in ovals) indicate token holders to indicate the status of the system. Transitions (e.g., T_TRUST_UPDATE, T_PSIG, etc.) refer to events that occur at a certain rate. A token in Place PS indicates that a new session for trust update is initiated. The public signals from the nodes are periodically disseminated to the CN with the transition rate T_PSIG, $1/T_{ps}$ where T_{ps} is the public signal interval. When the transition T_PSIG is triggered, a temporary place holder TEMP will obtain a token. When all nodes say "yes" indicating they observe the given trust threshold in their public signals, the immediate transition T_COLLUSION_PHASE is triggered and Place CP obtains a token. The immediate transition is triggered with only a probability without time given and indicated with a thin line distinguished from other transition rates in Fig. 1. The probability given in the immediate transition T_ COLLUSION_PHASE is computed by:

$$\text{probv}(\text{T\_COLLUSION\_PHASE}) = P_{\text{collusion}}(t) \tag{8}$$

$$P_{\text{collusion}}(t) = \prod_{i \in G(t)} P_i^{\text{collusion}}(t)$$

$$\text{where } P_i^{\text{collusion}}(t) = \begin{cases} (1 - P_i^{\text{data-integrity}}(t)) \text{ if } T_i(t) < T_{th} \\ 1 \text{ otherwise} \end{cases}$$

The probability in the immediate transition T_COLLUSION_PHASE is computed based on each node's lying probability based on the data integrity trust component. $G(t)$ represents the set of member nodes in the system at time t.

When Place CP has a token meaning all nodes say "yes," the CN also screens the public signals based on the information reported by neighboring nodes of each target node. When any lying nodes are detected by their neighboring nodes (either true negatives or false positives), they all will be evicted from the system with the rate $1/T_{\text{monitor}}$ in the transition T_EVICT_LYING. The number of nodes to be evicted

($N_{evicted}^{lying}$) by triggering the transition T_EVICT_LYING is computed by:

$$N_{evicted}^{lying} = N_{lie}(t)(1 - P_{fn}) + N_{good}(t)P_{fp} \tag{9}$$

$$N_{lie}(t) = \sum_{i \in S(t)}^{all} 1, \quad N_{good}(t) = G(t) - N_{lie}(t)$$

$S(t)$ is the set of member nodes whose trust value is below the trust threshold at time t. $N_{lie}(t)$ is the number of lying nodes having trust values below the trust threshold and $N_{good}(t)$ is the number of member nodes with trust values above the trust threshold at time t. $G(t)$ represents the set of member nodes in the system at time t. $P_{fn}$and P_{fp} are the false negative and false positive probabilities of a monitoring mechanism preinstalled on each node.

If any node honestly says "no" meaning it is not maintaining the given trust threshold, the immediate transition T_FEEDBACK_PHASE fires and accordingly Place FP has a token. The probability of the immediate transition T_ FEEDBACK_PHASE is computed by:

$$probv(T\_FEEDBACK\_PHASE) = 1 - P_{collusion}(t) \tag{10}$$

$P_{collusion}(t)$ and T_{ps} are explained as shown in Equation 8.

When Place FP has a token, the CN only identifies nodes that have trust values below the trust threshold and low rationality. Further, depending on the number of group members in the system, a certain fraction of nodes that are below the trust threshold with the lowest rationality will be evicted from the system with the rate $1/T_{monitor}$ in the transition T_EVICT_LOW_RATIONAL where $T_{monitor}$ is the monitoring interval. The nodes to be evicted here are computed as:

$$N_{evicted}^{low-rational} = \min\left[\sum_{i \in IR(t)}^{all} 1,\ G(t)P_{th}^{rationality}\right] \tag{11}$$

IR(t) is the set of member nodes with trust values below the trust threshold at time t and returns the lowest rational node first. $G(t)P_{th}^{rationality}$ is an upper bound to limit the number of nodes to be evicted and $P_{th}^{rationality}$ is a constant in the range of (0, 1).

When the transition T_FEEDBACK is triggered with the rate $1/T_{update}$ where T_{update} is the trust update interval, a token is taken to Place FEEDBACK which accumulates tokens over time. mark(FEEDBACK), meaning the number of tokens in Place FEEDBACK, represents the maximum feedback each node can accept for improving its trust value from its initially given trust value. Since each node's trust value is different, only some of member nodes will accept the feedback with the maximum of mark(FEEDBACK) depending on their trust status (discussed in Equation 2). The transition T_FEEDBACK only fires (returns 1) when the following conditions are met:

$$\text{If (mark(FEEDBACK)} < \text{MAX\_FEEDBACK} \quad (12)$$
$$\&\& \left(T_i(t-\Delta t) < T_{th} \;||\; GT(t-\Delta t) < T_{th}^{group}\right) \text{ return 1;}$$
$$\text{return 0 otherwise;}$$

MAX_FEEDBACK is a constant to limit the amount of feedback for the entire mission duration. Equation 12 explains that a feedback is issued when any member node does not reach the trust threshold or the current group trust does not reach the group trust threshold.

We made the states reaching FC1 or FC2 absorbing states such that all transitions are halted when either failure condition is met. Two metrics in Section 2.3 are computed using built-in functions of SPN Package version 6 [5] as follows.

System survivability probability is computed as:

$$P_{survivability}(t) = \sum_{i \in S}^{all} P_i(t) S_{alive}(t) \quad \text{where } S_{alive}(t) = \begin{cases} 0 \text{ if FC1 or FC2 is true;} \\ 1 \text{ otherwise;} \end{cases} \quad (13)$$

S is the set of allowable states of the system (e.g., possible states that are generated by SPN to represent the status of the system such as collusion phase or feedback phase at time t) and $P_i(t)$ is the probability of the system being in state i. $S_{alive}(t)$ returns a binary value where 0 represents system failure and 1 otherwise, representing a reward assignment to each state i defined in the system.

Overall group trust is calculated as:

$$T_{group}(t) = \sum_{i \in S}^{all} P_i(t) P_{group}(t) \quad \text{where } P_{group}(t) = \frac{\sum_{j \in G(t)}^{all} T_j(t)}{|G(t)|} \quad (14)$$

S and $P_i(t)$ are similarly defined as in Equation 13. G (t) is the set of current members at time t. $P_{group}(t)$ is used as a reward assignment to each state i.

In addition to the two metrics above, we also show the results using a combined metric, the so called "trust-survivability" metric. This metric indicates the overall group trust only when the system is alive. This metric is computed by:

$$T_{survivability}(t) = \sum_{i \in S}^{all} P_i(t)\, P_{trust-survivability}(t) \quad (15)$$

$$P_{trust-survivability}(t) = \begin{cases} 0 \text{ if FC1 or FC2 is true;} \\ P_{group}(t) \text{ otherwise;} \end{cases}$$

S and $P_i(t)$ are defined as in Equation 13. $P_{trust-survivability}(t)$ is used as a reward assignment to each state i. As we shall see in Section 4, this metric enables us to identify the optimal threshold based on the tradeoff between system survivability and group trust.

4 Numerical Results and Analysis

This section shows the results obtained from our analytical model and explains the physical meanings of the observed results. In particular, we identify the optimal trust threshold that maximizes overall group trust while meeting required system survivability. Table 1 summarizes the key default design parameter values used.

Table 1. Default design parameter values used.

Parameter	Meaning	Value
$T_{monitor} = T_{ps} = T_{update}$	Time interval used for disseminating message related to monitoring, public signal, or trust update	300 sec.
$P_{fp} = P_{fn}$	False positive or negative probability	0.05
T_{th}	Trust threshold	0.7
T_{th}^{group}	Group trust threshold	$T_{th} + 0.1$
Initial Trust Distribution	Initial trust values given to the node population in terms of cooperativeness, data integrity, and rationality based on uniform distribution	[0.6, 1]
N_{init}	Initial number of nodes	100 nodes
MAX_FEEDBACK	Maximum value of feedback	20
$TH_{mission}$	Minimum number of member nodes for mission execution; used in FC1	60
$TH_{malicious}$	Maximum number of malicious nodes out of the total member nodes; used in FC2	$N_{init}/3$
d	Allowed constant time delay in computing processing delay in Equation 3	600 sec.
c	A constant used in $P_{i,change}^{x}(t)$	1/20

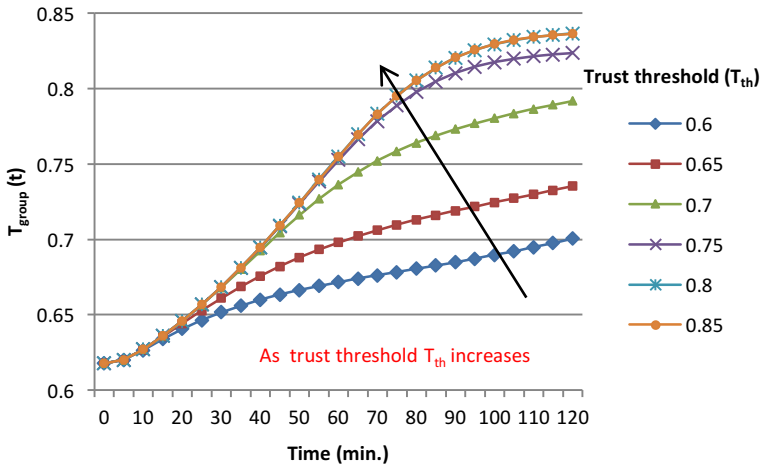

Fig. 2. Group trust metric over time for various trust thresholds (T_{th}).

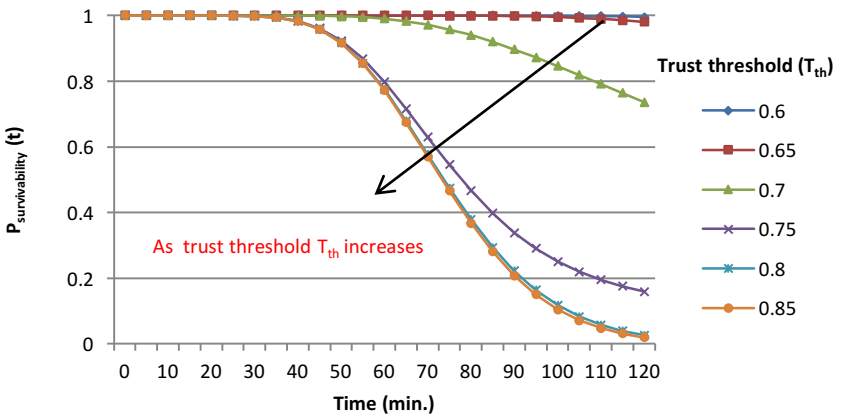

Fig. 3. System survivability metric over time for various trust thresholds (T_{th}).

Figs. 2 and 3 show the evolution of the two metrics over time as the trust threshold varies. Fig. 2 demonstrates that when higher trust threshold is used, higher overall group trust is observed. On the other hand, Fig. 3 shows that as higher trust threshold is used, system survivability is lowered. As previously pointed out, the tradeoff between trust and survivability can be clearly observed in Figs. 2 and 3. When higher trust threshold is used, a node fails more frequently to reach the trust threshold. This leads to more nodes being evicted and consequently lowers the system lifetime. This effect is more dominant in FC2. At the same time, using the higher trust threshold encourages nodes to reach higher standard in order to avoid penalty (eviction).

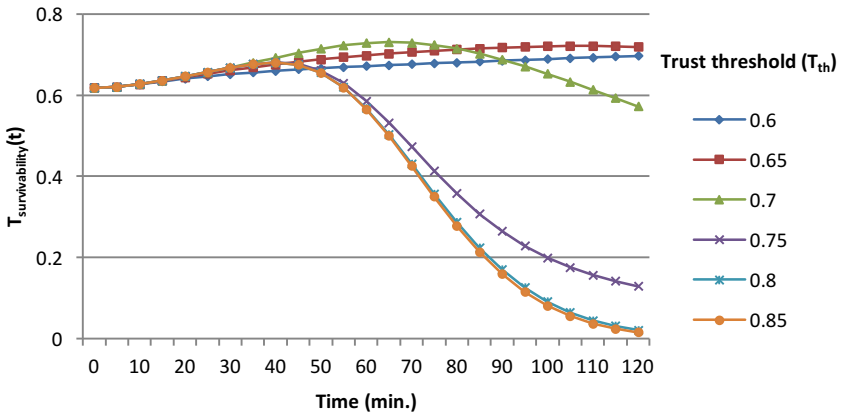

Fig. 4. Trust-survivability metric over time for various trust thresholds (T_{th}).

Fig. 4 shows the trust-survivability metric that identifies the optimal trust threshold (T_{th}) as the trust threshold varies. Notice that the optimal trust-survivability is observed at $T_{th} = 0.7$ when time < 80 min. Further, when $T_{th} = 0.6$ or 0.65, the metric increases monotonically within the 2 hour mission duration.

Next we study how sensitive the optimal trust threshold (T_{th}) is to different initial trust values (ITD: initial trust distribution) in the node population. Recall that the trust

components for cooperativeness, data integrity and rationality are drawn from a uniform distribution over [LB, 1]. In this example, we study the impact of varying LB. Fig. 5 shows the time-averaged group trust value for the 2 hour mission duration as LB varies. Each curve shows that higher group trust is observed at higher T_{th}. One noticeable observation is that even if LB is low, the node population with lower minimum trust (e.g., ITD = [0.5, 1]) performs better than the one with higher minimum trust (e.g., ITD = [0.55, 1] or [0.6, 1]) in some cases. For example, with T_{th} < 0.8, the node population with ITD = [0.5, 1] performs better than the one with ITD = [0.55, 1]. Further, with T_{th} < 0.7, the node population with ITD = [0.5, 1] even performs better than the one with ITD = [0.6, 1].

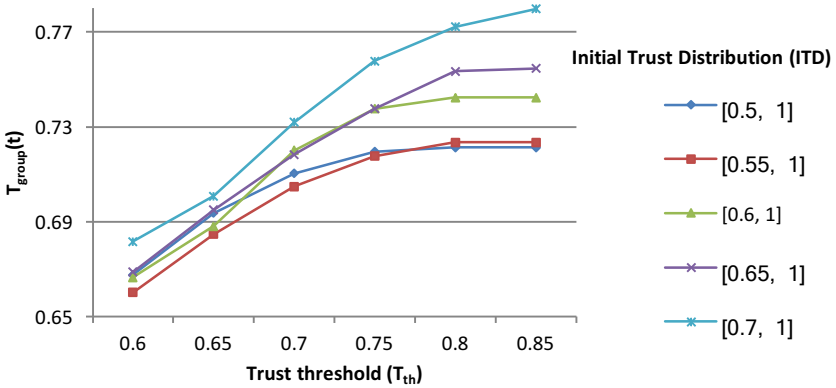

Fig. 5. Group trust metric versus trust threshold (T_{th}) for various ITD.

The mission group is penalized when any member node is below the trust threshold but the group trust may be above the group trust threshold. This encourages nodes to improve their behavior further. But if the trust threshold is low, nodes easily reach the threshold, and there is little incentive for them to improve their behaviors, since penalties are low in this scenario.

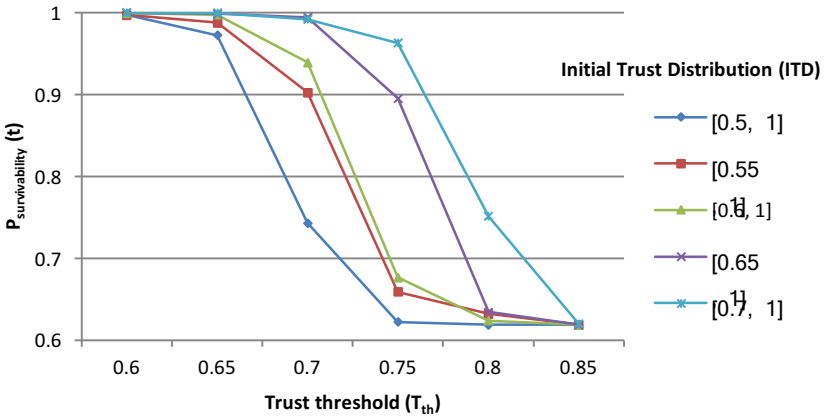

Fig. 6. System survivability metric versus trust threshold (T_{th}) for various ITD.

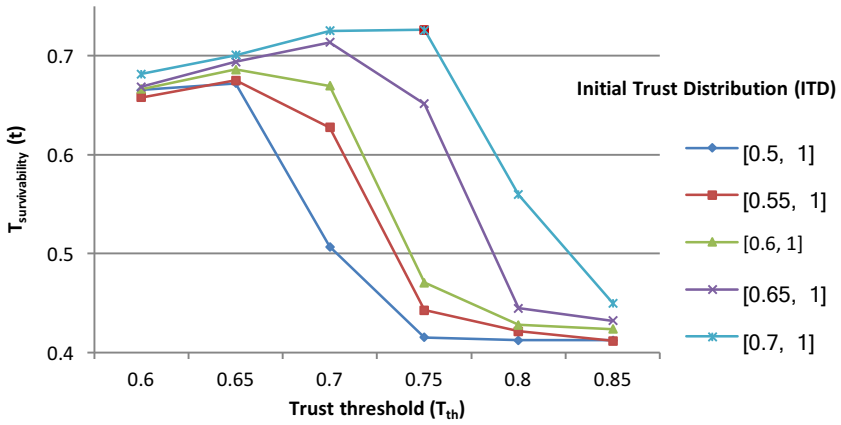

Fig. 7. Trust-survivability metric versus trust threshold (T_{th}) for various ITD.

Fig. 6 shows the time-averaged system survivability metric within the 2 hour mission duration when the trust threshold (T_{th}) varies under various ITD. Overall, the system survivability decreases as higher trust threshold is used and when the node population has lower initial trust values. Fig. 7 combines Figs. 5 and 6 in order to effectively identify the optimal trust threshold for various ITD. As expected, the trust-survivability metric improves as the initial trust quality improves. The identified optimal trust threshold shifts to the right as higher quality node population is used. For example, the optimal threshold is observed at $T_{th} = 0.65$ for ITD = [0.5, 1], [0.55, 1], and [0.6, 1], at $T_{th} = 0.7$ for ITD = [0.65, 1], and at $T_{th} = 0.75$ for ITD = [0.7, 1].

6 Conclusions and Future Work

We developed a composite trust metric considering various aspects of characteristics derived from communication, information, social, and cognitive networks. This work used *Aoyagi*'s game theory and aspiration concept in order to effectively stimulate participating nodes with the goal of maximizing their group trust level based on improved behaviors. We developed a mathematical model using SPN techniques to describe a trust network that maximizes overall group trust while meeting system survivability requirement. We identified the optimal trust threshold that maximizes group trust while maintaining required system survivability.

As future work, we plan to investigate (1) optimal trust update intervals that satisfy both trust and survivability requirements under various initial trust values over node population given; (2) dynamic trust thresholds to improve system survivability; (3) overall probability of success and failure based on an aspiration level that may induce risk-seeking behaviors; and (4) individual trust threshold considering each node's individual propensity for risk-aversion or risk-seeking [1, 7].

References

1. Atkinson, J.W.: Motivational determinants of risk-taking behavior. Psychological Review, vol. 64, no. 6, Part I, pp. 359-372 (Nov. 1957), available online 29 May 2007
2. Aoyagi, M.: Collusion in dynamic Bertrand oligopoly with correlated private signals and communication. Journal of Economic Theory, vol. 102, no. 1, pp. 229–248 (Jan. 2002)
3. Berman, Y.: Occupational aspirations of 545 female high school seniors. Journal of Vocational Behavior, vol. 2, no. 2, pp. 173-177 (April 1972), available online 27 July 2004
4. Bellosta, M., Brigui, I., Kornman, S., Vanderpooten, D.: A multi-criteria model for electronic auctions. In: Proc. 2004 ACM Symposium on Applied Computing, Nicosia, Cyprus, 14-17 (March 2004)
5. Ciardo, G., Fricks, R.M., Muppala, J.K., Trivedi, K.S.: SPNP Users Manual Version 6. Department Electrical Engineering, Duke University (1999)
6. Dash, R. K., Jennings, N. R., Parkes, D. C.: Computational-mechanism design: a call to arms. IEEE Intelligent Systems, vol. 18, no. 6, pp. 40-47 (Nov./Dec. 2003)
7. Diecidue, E., Ven, J.: Aspiration level, probability of success and failure, and expected utility. Int'l Economic Review, vol. 49, no. 2, pp. 683-700 (2008)
8. Festinger, L.: Wish, expectation, and group standards as factors in influencing level of aspiration. Journal of Abnormal and Social Psychology. vol. 37, no. 2, pp. 184-200 (April 1942), available online 15 May 2007
9. Han, Q., Arentze, T., Timmermans, H., Janssens, D., Wets, G.: An agent-based system for simulating dynamic choice-sets. In: Proc. 2008 Spring Simulation Multiconference. Ottawa, ON, Canada, 13-16, pp. 26-33 (April 2008)
10. Hoppe, F.: Success and failure. Field Theory as Human Science. De. Rivera (Editor), pp. 324-422, New York: Gardner Press (1976), originally work published in 1931
11. Klein, M., Moreno, G.A., Parkes, D. C., Plakosh, D., Seuken, S., Wallnau, K.C.: Handling interdependent values in an auction mechanism for bandwidth allocation in tactical data networks. In: Proc. 3rd Int'l Workshop on Economics of Networked Systems. pp. 73-78, Seattle, WA (August 2008)
12. Mainland, G., Parkes, D., Welsh, M.: Decentralized, adaptive resource allocation for sensor networks. In: Proc. 2nd Symposium on Networked Systems Design and Implementation. vol. 2, pp. 315-328, Boston, MA (May 2005)
13. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Pro. 6th Annual ACM/IEEE Mobile Computing and Networking, pp.255-265, Boston, MA (Aug. 2000)
14. Ng, S.K., Seah, W.K.G.: Game-theoretic approach for improving cooperation in wireless multihop networks. IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics. (2010) [Online] version available.
15. Perrig, A., Tygar, J.D.: Secure Broadcast Communication in Wired and Wireless Networks. Kluwer Academic Publishers (2002)
16. Quaglia, R.J., Cobb, C.D.: Toward a theory of student aspirations. Journal of Research in Rural Education. vol. 12, no. 3, pp. 127-132 (Winter 1996)
17. Rue, R., Pfleeger, S.L.: Making the best use of cyber-security economic models. IEEE Security and Privacy, vol. 7, no. 4, pp. 52-60 (2009)
18. Sahner, R.A., Trivedi, K.S., Puliafito A.: Performance and Reliability Analysis of Computer Systems, Kluwer Academic Publishers (1996)