Using Social Network Theory Towards Development of Wireless Ad hoc Network Trust *

Sameer Pai[1], Tanya Roosta[2], Stephen Wicker[1], Shankar Sastry[2]
[1]School of Electrical and Computer Engineering, Cornell University
[2]Department of Electrical Engineering and Computer Science, University of California, Berkeley

Abstract

The evolution and existence of stable trust relations have been studied extensively in the context of social theory. However, reputation systems or trust schemes have only been recently used in the domain of wireless ad hoc networks. It has been shown that these schemes provide positive results as a self-policing mechanism for the routing of data in wireless ad hoc network security. This paper develops a relationship between the trust concepts in the social network theory and wireless ad hoc networks. In addition, the paper maps existing trust schemes in wireless ad hoc networks to a long-standing theory in social networks. Most importantly, a refined model of trust evaluation in social networks is constructed and mapped to a new trust scheme for ad hoc networks. The new trust scheme is analyzed and shown to outperform existing schemes using scenario and simulation analysis.

1 Introduction

Wireless ad hoc networks are networks which lack a predefined infrastructure and which are capable of multihop communication. The nodes, in this type of network, act as hosts or routers and forward packets to other networked nodes. A recently emerging type of a wireless ad hoc network is a sensor network. A sensor network consists of some number of small wireless devices with sensors. A few applications of sensor networks are in providing health care, emergency disaster relief, surveillance, battlefield intelligence, and infrastructure monitoring. Much work has gone into the development of networks of these sensors. However, one serious fear that still exists is that of exposure, in a hostile environment, to misbehaving nodes[1]. The exposure of the wireless ad hoc network to misbehaving nodes could jeopardize the function of the network. Consequently, the data gathered by the network will be insufficient or even incorrect, which will result in the failure of the application and the network. In addition, misbehaving nodes can pose a threat to the privacy of the network users.

Reputation and trust relations have been extensively studied in the field of social sciences. Interestingly, the concept of trust as found in social science literature has analogues in wireless ad hoc network engineering literature. The main contributions of this paper are: to give an overview of the developing area of trust schemes for wireless ad hoc networks, and to incorporate theories of trust from social networks into these schemes to enhance their performance. More specifically, this paper examines trust in the context of routing and reliable forwarding of data in wireless ad hoc networks. The lack of a reliable infrastructure or a central authority in these networks means that nodes must collaborate to route data from point to point. When a source node transmits data, if the intermediary nodes fail to collaborate and route the data due to misbehavior, energy and other resources in the network are wasted. Moreover, if these misbehaving nodes fail to transmit the correct information or re-route the data to the wrong nodes, data integrity and/or confidentiality could be compromised. Therefore, nodes need a way to distinguish behaving nodes from those that misbehave.

Multiple distributed schemes, to compute trust values to help distinguish and route data around misbehaving nodes, have been proposed. In particular, an Information Theoretic Entropy Based Scheme and Cooperation of Nodes and Fairness In Dynamic Ad hoc NeTworks (CONFIDANT) are examined [11, 1]. These schemes, however, are slow to assess misbehavior in the network. Furthermore, these schemes

*This work was supported in part by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), Cisco, British Telecom, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia and United Technologies. The first author is also supported by a NSF IGERT Fellowship. The author emails are as follows: {skp27, sbw11}@cornell.edu, {roosta,sastry}@eecs.berkeley.edu

[1] Misbehaving nodes are defined to be those nodes that are incorrectly functioning or malicious.

are prone to eliminating behaving nodes in the presence of benign interaction failures, such as those that could occur in an error-prone wireless channel. This work reviews these existing schemes while mapping them to similar models for trust assessment in the social network theory. The paper uses aspects of social network theory to inform the design of a scheme that (i) is faster at detecting misbehaving nodes and (ii) preserves the network connectivity in the presence of the benign failures.

The rest of the paper is organized as follows: an overview of the literature discussing trust in social networks and wireless ad hoc networks are given in Section 2. Trust schemes for wireless ad hoc networks are algorithmically and quantitatively described in Section 3 and mapped to a theory of trust in social networks. The social network theory of structural balance is presented in Section 4. Trust scheme enhancements made by integrating insights from social theory are discussed in Section 5. The new trust scheme is explained in detail in Section 6. Different scenarios, where the new scheme could outperform existing schemes, are given in Section 7. Methodologies to test the performance of the new trust scheme and simulation results are also presented in Section 7.

2 Definitions of Trust

In this section a definition of trust used in social network analysis is given and compared with the definition of trust used in distributed wireless ad hoc networks.

The sociological concept of trust is rooted in multiple models. However, the most popular model defines trust as a means of measuring uncertainty [2, 7]. Behavior is judged through interactions among networked agents and trust measurements are made as a function of these interactions. One application of trust in a social network is for an agent (agent i) to tell if another agent (agent j), is acting in his or her best interest. If agent j is acting in the best interest of agent i, then future interactions are fostered, otherwise, future interactions are mitigated [9].

In [7], Krackhardt breaks down the prediction of trust into three *necessary and sufficient* component parts: interactions between agent pairs, affection meaning liking of one agent by another agent, and time or a history of past interactions between one agent with another agent. Two trust schemes developed in wireless ad hoc networks, which are in agreement with Krackhardt's theory, will be illustrated in the following subsections.

In wireless ad hoc network, trust can be defined as the reliance of a network node on the ability of other nodes in the network to pass necessary data from this node while preserving the integrity of the data. In this paper, the term *node* refers to the wireless ad hoc network entities and *agent* refers to social network entities. In contrast to social networks, trust can easily be quantified in an algorithmic way in ad hoc networks. For example, in [1] and [11] trust is defined as a *measure of uncertainty* and is measured by the information theoretic concept of *entropy*. Trust in wireless ad hoc networks is a way for one node (node i) in the network to measure the uncertainty of another node's (node j's) data forwarding actions. Node i uses this information and a trust threshold to make future decisions about its own actions (i.e. whether to continue to use node j as a possible node for forwarding data in the future or not). [2] Even though such a trust scheme could help preserve data integrity, it could drastically affect the network connectivity.

3 Trust Schemes in Ad hoc Networks

There are multiple trust schemes that have been proposed in wireless ad hoc networks. The basis of a trust scheme is as follows: node i observes the communication of a neighbor node j after passing data to it. These observations could be done at the data packet level or at the message level [1, 5, 10, 11]. However, in this paper we abstract away the level at which the observations are done. Node i observes if node j correctly relays the forwarded data towards the final destination, meaning the correct next hop for the data. If the data is correctly forwarded without errors, then the interaction between the node and its neighbor is considered to be successful; otherwise, it is deemed as being unsuccessful.

3.1 Trust Scheme Mappings

In this section we give a mapping between the social network trust model and trust in wireless ad hoc networks.

The observing node i keeps track of the total successful interactions as well as the unsuccessful interactions, with node j. These parameters are related to Krackhardt's components of *interaction* and *time*. These components are used to calculate a fraction directly proportional to the fraction of successful interactions, a belief, which is encompassed by Krackhardt's concept of *affection*. In the existing trust schemes for wireless ad hoc networks a fraction directly proportional to the fraction of successful interactions is used to form a trust value between the trustor and trustee. Therefore, in these schemes, a trust value is assigned by node i to node j as a function of the past successful and unsuccessful interactions with that node. This assignment of trust value is termed *a direct trust value*. Trust values are assigned by a node to non-neighbor nodes as a function of their direct trust value for a neighbor and the neighbor's trust value in the non-neighbor node. Trust values assigned to non-neighbor nodes are termed *indirect trust values*. Thus, indirect trust

[2] An implicit assumption that is made is that the source node uses a routing algorithm which allows it to make a choice of the entire source-destination path to be used by the data packets.

values are formed using properties of transitive relations. Only if the trust value is beyond a given threshold, H', is a node believed to be trustworthy and data routed through it. In the remainder of this section we examine two trust schemes widely discussed in ad hoc network literature.

3.2 Information Theoretic Scheme

The Information Theoretic trust scheme [11] is one of the newest trust schemes presented in literature.

Updates to the *direct trust* values are made as follows: let $T_{i,j} = T_{subject=i:agent=j,action}$ be the trust value of the relationship $subject = i : agent = j, action$, and $p = p_{subject=i:agent=j,action}$ be the probability that node j performs the *action* from the point of view of node i. This probability is not an absolute value; in contrast, it is a function of the interaction of a node with another node. Therefore, node j can have different probabilities assigned to it by different node i's based on each node i's interaction history with j. Node i update its trust value of node j after each interaction as follows:

$$T_{i,j} = \begin{cases} 1 - h_b(p) & \text{for } 0.5 \leq p \leq 1 \\ h_b(p) - 1 & \text{for } 0 \leq p < 0.5 \end{cases}$$
$$p = Pr(V(N+1) = 1|n(N) = s) = \frac{s+1}{N+2} \tag{1}$$

Note that h_b is the binary entropy function $-\sum_x p(x) logp(x)$. The trust value obtained using equation 1 is a continuous value in the interval $[-1, 1]$. $V(m)$ is a random variable defined to be 1 if node j performs the action successfully from the point of view of node i in their m^{th} interaction, and $V(m) = 0$ otherwise. The random variable $n(N)$, is defined to be $\sum_{m=1}^{N} V(m)$.

Node i calculates an *indirect trust* value for non-neighbor node j using information from neighbor node k if $T_{i,k} > 0$. For multiple indirect routing paths of node i to node j via neighbor nodes k we have, $T_{i,j} = \sum_{k\in\mathcal{N}} w_k T_{i,k} T_{k,j}$, where $\mathcal{N}$ is the set of all such neighbors of node i with $T_{i,k} > 0$. Each $T_{i,k}$ is calculated by the direct trust equations given in 1. Each term w_k is a weight associated with the linear opinion pool model. Using this model, the weight w_k for each node in $\mathcal{N}$ is calculated by dividing the trustor's trust value for the k^{th} trustee by the sum of the trust values for all trusters, namely, $w_k = \frac{T_{i,k}}{\sum_{k\in\mathcal{N}} T_{i,k}}$. This allows the overall trust value $T_{i,j}$ to remain bounded in $[-1, 1]$. In order for the information theoretic scheme to work, a threshold value for trust, $T_{i,j}(H') = \hat{H}$, is set by the network engineer. Note that the update equations for the Entropy Based Trust scheme, Equation 1, are in accordance with Krackhardt's theory presented above.

3.3 The CONFIDANT mechanism

The CONFIDANT scheme [1], is one of the most widely cited trust scheme in use in wireless ad hoc networks. In CONFIDANT, direct trust value updates are based on direct interactions initiated and observed by a node that sends data, and are updated using:

$$f(\theta) = Beta(\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \theta^{\alpha-1}(1-\theta)^{\beta-1}$$
$$\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} = \frac{(\alpha+\beta-1)!}{(\alpha-1)!(\beta-1)!} \tag{2}$$

where $Beta(\alpha, \beta)$ corresponds to a Beta distribution. In the Beta distribution, the parameter α keeps track of the total number of unsuccessful interactions over time and the parameter β the total number of successful interactions. To simplify the equations, CONFIDANT uses $F_{i,j}$ which is a two-tuple keeping track of these parameters of the Beta distribution over time. $F_{i,j} = (\alpha, \beta)$ is initialized to $(1, 1)$. Updates to the parameters of the Beta distribution are made using $\alpha = \alpha + s$ and $\beta = \beta + (1 - s)$, where s indicates an unsuccessful interaction. In order to best understand the reasoning behind using the Beta distribution, due to space limitations, we refer the interested reader to [6]. A node using CONFIDANT assigns a *complementary direct trust (CDT)* value $(1 - DirectTrust_{i,j})$ using these parameters. In order to find this value, the node takes the expectation of the Beta distribution, denoted as $\mathbb{E}$:

$$CDT_{i,j} = \mathbb{E}(Beta(F_{i,j})) = \frac{\alpha}{\alpha + \beta} \tag{3}$$

In CONFIDANT second-hand (indirect) trust values, are handled in a similar way as the direct trust values. However, for indirect trust values, a node i takes weighted information from each neighbor node k which has information about a non-neighbor node j in the network. To simplify the equations, let $R_{i,j}$ be a two-tuple which keeps track of the parameters of the Beta distribution over time and is initialized to be $(0, 0)$. Now, if there are multiple indirect relations of node i to node j via neighbor nodes k, node i updates the overall trust value using $R_{i,j} = R_{i,j} + w_k F_{k,j} = (\alpha^{'}, \beta^{'})$. w_k is a weight statically set by the network engineer for all. Note that indirect trust values are calculated as a function of direct trust values. Again, each node i can calculate a *complementary indirect trust (CIT)* value $(1 - InDirectTrust_{i,j})$ for node j. This value can be calculated for $R_{i,j} = (\alpha^{'} > 0, \beta^{'} > 0)$ as follows:

$$CIT_{i,j} = \mathbb{E}(Beta(R_{i,j})) = \frac{\alpha'}{\alpha' + \beta'} \tag{4}$$

In CONFIDANT, a threshold value for trust, H', is set by the network engineer. There is no prescribed way to find this value. However, choosing this threshold wisely has a great impact on the performance of the algorithm. Therefore, there is a need to develop rules to determine H' for a given network with specific parameters. Again, from the discussion above, it is obvious that CONFIDANT conforms to Krackhardt's model for building trust.

4 Structural Balance In Social Networks

In this section we give a brief overview of Heider's structural balance theory in the context of social networks [4]. Although this theory is not directly applicable to the paradigm of trust in wireless ad hoc networks, it will help clarify some connections between these networks and social networks.

Heider focused on three agents within a network, agent X, agent Y, and agent O. In this theory, these agents form a clique of possible bi-directional ties. Within the triadic clique, the emotional state of any one agent towards the other two influences this agent's relationship to the other two agents. Thus, these emotional states induce some structure to form between the agents. Positively tied agents have a link and a mutually-trustworthy relationship. Negatively tied agents have no link and a negative or mutually-untrustworthy relationship. These links represent the structure that has formed as a result of the agent's emotional states towards other agents.

Heider's main theory was that a balanced triadic relationship (i.e. one in which no agent wants to change its positive or negative relationship with the other two agents to facilitate a structural equilibrium) occurs in one of two cases: i) when all three ties between X,Y, and O are positive, or ii) when any two ties between X,Y, and O are are negative and the third is positive. Although each of the cases can be examined separately, we have eliminated this examination due to lack of space.

Heider's main idea in the development of balance theory are clear. Heider theorized that the affective processes occurring amongst directly tied individuals (agents) could assist in bringing about change in networks structure. This would cause a network structure that is not balanced, to quickly become balanced.

In wireless ad hoc networks, directly tied nodes are those within mutual communication range of each other. In the framework of trust values, Heider's ideas give the insight that direct trust value computation should be altered to incorporate observations of particular neighbor nodes. Furthermore, the ideas give insight about dynamically setting trust thresholds for nodes that are in some way dependent on the neighbors of a particular node. Beyond these thresholds, a node determines another node to be trustworthy.

5 Balance Theory: Trust Enhancements

The wireless ad hoc network trust schemes presented in this paper are similar to the model of trust developed by Krackhardt. In the previous sections Krackhardt's model was used to construct a map between trust as defined in wireless ad hoc networks and trust as defined in social networks. This section examines how to take advantage of this mapping using ideas stemming from Heider's theory.

As was seen in CONFIDANT and the Entropy based trust schemes, trust evaluation is dependent on interaction, affection, and time as in Krackhardt's model. However, in these schemes, direct trust is based on affection as perceived by one node from knowledge of that node's direct interaction with another node. Heider's theory offers a new perspective. In social networks, Heider believes that affection among agents is not only influenced by direct interaction among agents. Heider's theory implies that affection is also a function of direct ties with other individuals mutually connected to both agents. This insight maps to wireless ad hoc networks in the following way: some fraction which is directly proportional to the fraction of successful interactions is computed not only based on a trustor's direct observations of a trustee, but also based on the observations of the trustee by the mutual direct neighbors of the trustor and trustee. Affection has been linked with trust evaluation in Krackhardt's theory. In order to make a better evaluation of direct trust among nodes, it is beneficial to incorporate ideas from Heider's theory of how affection can be influenced by neighboring nodes.

Heider's structural balance theory predicts that ties are bi-directional. However, this need not be the case in the case of trust. Direct trust values are assigned to a node independent of that node's trust value in a node assigning the value. To account for this difference, we apply ideas from balance theory from the point of view of one node. Next, balance theory explores at most triadic relationships. However, for use in a trust scheme, it is necessary to generalize the theory. We apply insights from the theory to multiple directly tied nodes. In balance theory, a tie among agents is either positive or negative. Putting this in the context of a trust scheme, trustworthiness can be computed by setting a threshold, denoted by H', for trust values. Below this threshold, a node evaluates another node as being untrustworthy and forms a "negative" tie, resulting in data not being routed through the untrustworthy node.

Another aspect to consider when mapping Heider's theory from social networks to wireless ad hoc networks is the dependence of the threshold on the node's structural position. The insights garnered from structural balance theory and social network analysis help design a way to set the these thresholds for each networked node. Intuitively, it is beneficial to assign a higher threshold of trust for those nodes which are likely to have a higher quality direct trust evaluation of other nodes.

As discussed, the threshold for direct trust aids in determining if data is routed to neighbor nodes. A trust scheme which assigns as high a threshold of trust as possible to a node seems to be best to maximally mitigate misbehavior of networked nodes. However, there should be some dependence of the calculation of this threshold, for any node, on that node's structural position and the potential quality of the trust values to which it has access. The following offers one method to calculate this threshold for each node: all nodes in the wireless ad hoc network are assumed to have global[3] and local density information. Multiple ways to assess or approximate expected density can be found in literature [3]. Furthermore, the global density is governed by the communication radius of each node. [4] Those nodes within each others' communication radius have a possible tie or communication link within the network. Nodes are also assumed to be given information about the total number of nodes in the network or are assumed to be capable of estimating this given the area of network coverage (for communication) and the communication area of the node (based on the communication radius).

The local density measure is proportional to the number of mutually tied neighbor nodes. This is true because in a randomly distributed wireless ad hoc network, an average of 59% of a node's neighbors are also neighbors. This finding is a fundamental result in wireless ad hoc networks, the proof for which can be found in [8]. Therefore, there is a strong positive correlation between the number of direct neighbors a node has (local density) and the number of mutual local neighbors. It is possible for a new trust scheme to take advantage of this information. The trust scheme could set a higher threshold for direct trust for nodes with high local density, and a lower threshold for direct trust is set for nodes with low local density. In this case, the measure of high versus low local density is with respect to the global density.

The previous analysis suggests that trust value computation for a node should be based not only on its direct observation of another node, but also on the observations of the nodes that are mutual neighbors of both of these nodes. This implies that the existing trust schemes can be improved by incorporating particular types of indirect observations to calculate direct trust values.

In the next section, we propose a new trust scheme which incorporates indirect observations to calculate direct trust values as well as dynamic thresholds to improve upon the already existing trust schemes in the area of wireless ad hoc networks.

6 A New Trust Scheme

Every trust scheme that has been presented in Section 3 has been shown to follow the same general principles in design. However, there are fundamental changes that could be made to improve these trust schemes. The first improvement is to incorporate indirect observations of certain direct neighbors into the trust value computation. Let $T_{i,j} = (s, u)$ be a two-tuple which keeps track of two parameters to calculate a direct trust value and is initialized to $(1, 1)$. The set $\mathcal{N}$ contains direct mutual neighbors of node i and j, which have direct trust evaluations for node j. Updates to direct trust values when node i interacts with node j are performed using $u = u + e$, $s = s + (1 - e)$, and $T_{i,j} = (s, u) + \sum_{k \in \mathcal{N}} f(T_{i,k}) T'_{k,j}$. In these equations e indicates an unsuccessful interaction (i.e. unsuccessful forwarding of data). Therefore, $e = 1$ if node j performs action unsuccessfully in any particular interaction with node i, and $e = 0$ if node j successfully interacts with node i in any particular interaction. In addition to the update equations, we have;

$$T_{k,j} = (x, y) \Rightarrow T'_{k,j} = (x - 1, y - 1) \tag{5}$$

$$T_{i,j} = (x, y) \Rightarrow f(T_{i,j}) = \frac{x}{x + y} \tag{6}$$

where x and y are real numbers set by the values in the two-tuple $T_{i,j}$ and $DirectTrustValue_{i,j} = f(T_{i,j})$. The new trust scheme assigns a direct trust value as a function of $T_{i,j}$.

Updates to indirect trust values are done as a function of direct trust values. Let the set $\mathcal{M}$ contain neighbors of node i which have (direct or indirect) trust evaluations for node j. Let $I_{i,j} = (x, y) \Rightarrow f(I_{i,j}) = \frac{x}{x+y}$ where $I_{i,j}$ is initialized to $(0, 0)$. Here, x and y are real numbers set by the values in the two-tuple $I_{i,j}$, and $IndirectTrustValue_{i,j} = f(I_{i,j})$. Therefore, the equations for updating an indirect trust values are $I_{i,j} = I_{i,j} + \sum_{k \in \mathcal{M}} f(T_{i,k}) T_{k,j}$.

As in the other trust schemes, a threshold value for indirect trust, H_I is set by the network engineer. Nodes use this to gauge the trustworthiness of other nodes. If any node j has a trust value assigned by node i (indirect) greater than the threshold, then j is determined as being trustworthy by node i. Otherwise, i determines j is untrustworthy. Any node deemed untrustworthy by node i is not used by node i for routing data. Every node in the network is designed to run this local trust scheme. However, not every node in the network has the same number of direct neighbors. Of these direct neighbors, a subset of them have possible ties to nodes which can report information about mutually tied neighbors, and these subsets vary for each node. These differences can be roughly accounted for, if every node had expected global density information, the number of total networked nodes, and every node acquired local density information (local number of possible ties). Using this information a node is capable of setting its direct trust threshold H, autonomously, i.e, $H_{max} = 1$, $H_{min} = 0$, $H_{min} \leq H', H \leq H_{max}$, and $\eta \in [1, n]$. Therefore, we have:

$$H = \begin{cases} H' + (H_{max} - H') * \frac{n_l - n_g}{\eta} & \text{if } n_g \leq n_l \\ H' - (H' - H_{min}) * \frac{n_g - n_l}{\eta} & \text{if } n_g > n_l \end{cases} \tag{7}$$

[3] The global density is a measure of the expected number of communication links (possible ties) for any node in the network.

[4] The network engineer sets the transmission power and the physics of radio propagation governs the radius.

In the above equations, H_{max} is the maximum trust threshold, which is set to 1 for our case. The value of H_{min} is set as the minimum trust threshold value, which in our case is set to 0. We assume that the network engineer sets H' to be a value between H_{max} and H_{min}. A threshold for direct trust, H, is calculated as a function of these parameters, a global density value, n_g, a local density value, n_l, the total number of nodes in the network, n, and η is a parameter determined by the network engineer [5]. This setup allows for a node to account for the structural position.

7 Main Hypothesis and Methods

The trust schemes presented in Section 3 assume that direct trust values should only be based on direct observations of one node by another node, [1, 11], but without additional information about observations from a subset of neighbors, a lower quality assessment is made. In certain scenarios, this could cause a node to revoke a neighboring node too quickly, resulting in reduced connectivity. In other scenarios, it could lead to a node revoking a neighboring node too slowly, reducing data integrity. Examples of these scenarios will be given in the following subsection.

The main hypothesis that we test in this section is that there are scenarios in which the new trust scheme could be beneficial to the network in terms of preserving connectivity and data integrity. This hypothesis will be tested using scenario analysis and simulation methods. In particular we show that the use of additional information and dynamic thresholding, within the new trust scheme, aids in outperforming other schemes in terms of revoking malicious nodes quickly while preserving network connectivity in the presence of benign interaction failures. For the purpose of this paper, we will focus only on direct trust values with the simplifying assumption that there is no incentive for nodes to give malicious trust reports.

7.1 Scenario Analysis

There are a number of benefits to using the new trust scheme that are not present when using the other trust schemes. Particularly, the new trust scheme outputs higher quality direct trust values using information about observations from mutual neighbors. This can easily be seen in the following two scenarios: suppose there are three nodes in the network: node A, node B, and node C. Every node is within the communication range of every other node.

In the first scenario, node C always misbehaves and A and B behave. Both node A and node B communicate data with node C and each other independently. Therefore, nodes A and B always have unsuccessful interactions with node C but not with each other. We assume here that there are no false positive or negative observations. To gain a better insight, we need to consider what happens in this scenario in CONFIDANT and the Information Theoretic scheme. For every scheme and every node, the network engineer sets the same threshold for trust, $0 < H' < 1$, before the network is deployed. Thus, the trust threshold equals H' for CONFIDANT, $H = H'$ (calculated) for the new scheme and $T_{i,j}(H')$ in the Information Theoretic scheme. Suppose that the threshold is set very high. Then, for every scheme, unsuccessful interactions with node C will cause nodes A and B to revoke node C very quickly. However, suppose that the threshold is set low. In this case, if the nodes use the Information Theoretic scheme or CONFIDANT, node C is revoked very slowly. This is due to the fact that A and B independently assign a trust value to node C. The trust value in these schemes is very slow to breach the high threshold.

We further analyze this using the update equations for these two trust schemes. For CONFIDANT $1 - CDT_{i,j} = 1 - \mathbb{E}(Beta(F_{i,j})) = 1 - \frac{\alpha'}{\alpha'+\beta'}$ decreases slowly with every negative interaction. For the Information Theoretic scheme, the direct trust value, $h_b(\frac{s+1}{N+2}) - 1$ also decreases slowly with every negative interaction. In the new scheme, A uses information from B about B's observations of C in order to assign a direct trust value to C. Additionally, in the new trust scheme, B uses information from A about A's observations of C in order to assign a direct trust value to C. Therefore, the rate at which the value $DirectTrustValue_{i,j} = f((s,u) + \sum_{k \in \mathcal{N}} f(T_{i,k})T'_{k,j})$ drops, is at least as fast as the rate of increase of negative interactions (from unsuccessful direct interactions and unsuccessful interactions from mutual neighbor A or B). Thus, in the new scheme, the rate at which the direct trust value breaches the threshold is very fast. In fact, it is much faster than CONFIDANT or the Information Theoretic scheme (shown below using simulation). This is because the new scheme is able to make a higher quality trust assessment than the other two schemes. Therefore, regardless of how the threshold is initially set, the new scheme outperforms the older schemes in preserving data integrity for a longer period of time.

In the second scenario nodes A, B and C do not intentionally misbehave. However, in this scenario, node A experiences a small burst of (unintentional) failures when interacting with C but node B has successful interactions with C [6]. This could, for instance, be caused by errors introduced in the wireless channel. Both node A and node B communicate data with node C and each other independently. Once again, it is informative to see what occurs in this scenario in each trust scheme that has been presented. For every scheme and every node the network engineer sets the same

[5] The value of η changes the performance of the new scheme when compared with the older schemes already discussed, however the new scheme outperforms the older schemes at any value of $\eta \in [1, n]$

[6] Here, we make the assumption that the percentage of times C fails is close to, if not slightly greater than the trust threshold

threshold for trust, $0 < H' < 1$, before the network is deployed. Thus the trust threshold equals H' for CONFIDANT, $H = H'$ for the new scheme and $T_{i,j}(H')$ in the Information Theoretic scheme. Suppose that the threshold is set very low. In this case, C will not be revoked by B or A in any scheme. This is because the few negative interactions A experiences with C will have little impact in bringing the direct trust value below the threshold. However, suppose that the threshold is set high. In this case, CONFIDANT and the Information Theoretic scheme work differently than the new scheme. In the first two schemes, C will not be revoked by B, however, there is a high probability that A will revoke C. The few benign interaction failures that A has with C would allow the trust value to drop below the threshold quickly in these schemes. This is because in CONFIDANT and the Information Theoretic scheme, A and B make independent direct trust evaluations of C. Unfortunately, this could compromise network connectivity since when A revokes C, there is no longer any communication between A and C. In contrast, in the new scheme, A uses information from B about B's observations of C in order to assign a direct trust value to C, and visa versa.

This can be seen in the direct trust update equation for the new scheme: $DirectTrustValue_{i,j} = f((s,u) + \sum_{k \in \mathcal{N}} f(T_{i,k})T'_{k,j})$. The successes that B has with C are included in A's trust evaluation of C and counterbalance the unsuccessful interactions A had with C. As a result, the new scheme is able to preserve network connectivity in the presence of benign interaction failures, whereas the old schemes cannot.

In general there is a necessity in wireless ad hoc networks to revoke malicious nodes quickly to both preserve data integrity and network connectivity despite having benign interaction failures. The two scenarios presented above showed instances in which, unlike the old schemes, the new scheme fulfils this necessity. This is true despite having arbitrary thresholds set by the network engineer prior to the network being deployed. Therefore, we have shown through analysis that the hypothesis holds. However, we further explore the hypothesis using simulation in the following section.

7.2 Simulation Analysis

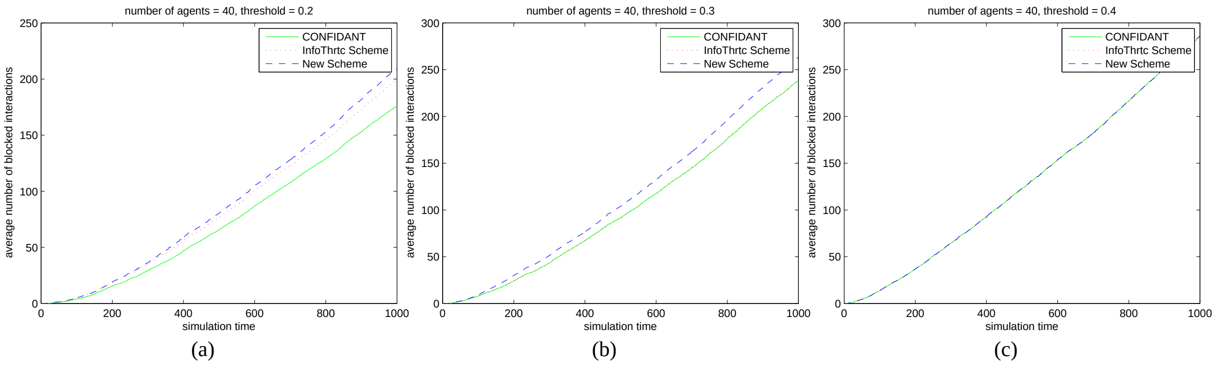
Although the two scenarios presented above seem to show that the new trust scheme can outperform the existing ones, the scenarios are not exhaustive. In order to test the scheme with more rigor, simulations are performed using the Trust Network Simulator (TNS), designed using MATLAB. Due to lack of space, we do not explain how a typical TNS simulation scenario runs, but rather present the results.

Essentially, the operation of TNS allows for Monte Carlo simulations of the trust schemes. These repeated trials give intuition about the general performance of the various trust scheme models under consideration. As a result, we can compare different trust schemes using various metrics of interest. There are multiple outputs provided by TNS. TNS outputs the number of interactions after which any node deems any other node to be untrustworthy. TNS also outputs the trust values of every node for every other networked node at the end of the simulation. Multiple other outputs from TNS are provided in the analysis and in figures 1 and table 1. Comparison of these outputs from the various trust schemes are also provided. In the simulation analysis that follows, the network is setup and tested using various topologies. In Figure 1 and Table 1, 40 nodes are simulated using a bidirectional chain topology. For the purposes of these experiments, η is set to $\frac{number of nodes}{2}$. In this network, half of the nodes always misbehave (as in Figure 1), or fail with a given probability at each time step (as in Table 1). The simulation is run for 1000 time steps and run over multiple iterations (3 to 100).

Table 1. Comparison of average number of revocations under varying probabilities of potentially benign node failure

Pr(Failure)	***Trust Threshold***	0.1	0.2	0.3	0.4
0.9	CONFIDANT	3.3	8.3	10.3	13
	Information Th.	3.3	9.3	10.3	13
	New Scheme	2.7	8	10.3	13
0.8	CONFIDANT	1.3	7.3	8.7	11
	Information Th.	1.3	7.7	9.7	11
	New Scheme	1	6.7	8	10
0.7	CONFIDANT	0.7	2.7	5.7	11
	Information Th.	0.7	3.3	6	11
	New Scheme	0	2.3	5	9
0.6	CONFIDANT	0	2	5	10
	Information Th.	0	2	5	10
	New Scheme	0	1.3	2.7	6

The graphs in Figure 1, show the tendency of the new trust scheme to outperform the CONFIDANT scheme as well as the Information Theoretic scheme in terms of revoking misbehaving nodes and blocking interactions with these nodes. At lower thresholds, ($0 < H' < 0.33$), this holds particularly true, since it is clear that the rate of increase of blocked interactions in time for the new scheme is greater than that for the other two schemes. However, at higher thresholds, $H' \geq 0.33$, and for a particular set of parameters, the new scheme behaves the same as the other schemes in terms of average number of blocked interactions. These results seem consistent with varying number of nodes, topologies, and values of η. Despite this caveat, as seen in Table 1, the new scheme does outperform the other two in terms of the number of node revocations (blocked misbehaving nodes) in the presence of benign interaction



(a) (b) (c)

Figure 1. Simulation results showing quick revocation of misbehaving nodes

failures, even at high trust thresholds. For low probability of node failures (unintentional node misbehavior) and as the threshold is increased between 0.1 and 0.4, Table 1 shows that the new scheme has fewer number of revocations than the other two schemes. As the probability of node failure is increased and if the trust threshold is set high, the new scheme has almost the same number of revocations as the other two schemes.

The new scheme has the added benefit of not quickly revoking nodes that have benign interaction failures. Given benign failures are highly likely to happen in the wireless ad hoc network setting (due to wireless channel errors), the trust scheme needs to ensure that nodes with random failures are not revoked too quickly.

8 Conclusion and Future Work

This paper reviewed definitions and examples of trust in social and wireless ad hoc networks. A general overview of trust scheme design was given. The existing trust schemes used for intelligent routing within wireless ad hoc networks, as presented in engineering literature, were shown to conform to this general design. In addition, a mapping between trust in social network theory and general design principles for trust schemes in wireless ad hoc networks was created. This paper examined and combined two social theories of trust formation. Using these combined theories and the mapping between the trust in social theory and wireless ad hoc networks, a new trust scheme was developed. We showed through simulation that the new trust scheme outperforms the existing trust schemes in certain scenarios. These performance boosts were seen in the ability of this new trust mechanism to revoke misbehaving nodes from the network quickly while preserving connectivity of the network in the presence of benign interaction failures.

Future work involves further simulation analysis with restrictions placed on the assumption of nodes not having incentive to give correct trust value information. Furthermore, different attack models, different ways to dynamically adjust trust thresholds, extended network topologies, and malicious trust reporting remain to be analyzed. The trust mechanisms described could be mathematically analyzed and improved upon using tools from Game Theory.

References

[1] S. Buchegger. Coping with misbehavior in mobile ad-hoc netoworks. *Thesis*, February 2004.

[2] D. Gambetta. Can we trust trust? *Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations*.

[3] B. Greenstein, E. Kohler, D. Culler, and D. Estrin. Distributed techniques for area computation in sensor networks. *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, 2004.

[4] F. Heider. Attitudes and cognitive organization. *Journal of Psychology, 21: 107-112*, 1946.

[5] D. B. Johnson, D. A. Maltz, and Y.-C. Hu. The dynamic source routing protocol for mobile ad hoc networks (dsr). Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt, 2004.

[6] A. Josang and R. Ismail. The beta reputation system. *Bled Electronic Commerce Conference Proceedings*, June 2002.

[7] D. Krackhardt. The strength of strong ties. *N. Nohria and R. Eccles (Eds.), Networks and organizations: Structure, form, and action,Harvard Business School Press*, 1994.

[8] S. Ni, Y. Tseng, Y. Chen, and J. Sheu. The broadcast storm problem in a mobile ad hoc network. *in Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking*, August 1999.

[9] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems. *Communications of the ACM, 43 (12) : 45-48*, 2000.

[10] T. Roosta, M. Meingast, and S. Sastry. Distributed reputation system for tracking applications in sensor networks. *Proceedings of tInternational Workshop on Advances in Sensor Networks (IWASN)*, 2006.

[11] Y. L. Sun, W. Yu, Z. Han, K.J., and R. Liu. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*.