# Uncertainty Modeling and Reduction in MANETs

Feng Li, *Member*, *IEEE*, and Jie Wu, *Fellow*, *IEEE*

**Abstract**—Evaluating and quantifying trust stimulates collaboration in mobile ad hoc networks (MANETs). Many existing reputation systems sharply divide the trust value into right or wrong, thus ignoring another core dimension of trust: uncertainty. As uncertainty deeply impacts a node's anticipation of others' behavior and decisions during interaction, we include uncertainty in the reputation system. Specifically, we define a new uncertainty model to directly reflect a node's confidence in the sufficiency of its past experience, and study how the collection of trust information affects uncertainty in nodes' opinions. After defining a way to reveal and compute the uncertainty in trust opinions, we exploit mobility, one of the important characteristics of MANETs, to efficiently reduce uncertainty and to speed up trust convergence. Two different categories of mobility-assisted uncertainty reduction schemes are provided: the proactive schemes exploit mobile nodes to collect and broadcast trust information to achieve trust convergence; the reactive schemes provide the mobile nodes methods to get authenticated and bring their reputation in the original region to the destination region. Both of the schemes offer a controllable trade-off between delay, cost, and uncertainty. Extensive analytical and simulation results are presented to support our uncertainty model and mobility-assisted reduction schemes.

**Index Terms**—Authentication, mobile ad hoc networks, mobility, proactive, reactive, reputation, trust, uncertainty, vouching.

## 1 Introduction

Mobile ad hoc networks (MANETs) aim to provide wireless network services without relying on any infrastructure. The main challenge in MANETs comes from their self-organized and distributed nature. There is an inherent reliance on collaboration between the participants of a MANET in order to achieve the aimed functionalities. Collaboration is productive only if all participants operate in an honest manner. Therefore, establishing and quantifying trust, which is the driving force for collaboration, is important for securing MANETs.

Trust can be defined as the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context. It represents a MANET participant's anticipation of other nodes' behavior when assessing the risk involved in future interactions. Here, the participant is usually called the trustor, and other nodes are called the trustee. The trust relationship usually builds on the basis of the trustor's past direct interaction experiences and others' recommendations related to the trustee. The abstracted value from past experiences and recommendations is defined as the trustee's reputation.

Many reputation systems have been proposed in literature. Most of them sharply divide the recorded behavioral information into right or wrong. For example, in the EigenTrust model [1], behavioral information is obtained by counting the number of "satisfactory" and "unsatisfactory" interactions, and the difference between these two values is stored as reputation. Besides lacking a precise semantic, this information has abstracted away any notion of time. In EigenTrust, value 0 may represent both "no past interaction" and "many unsatisfactory past interactions." Consequently, one cannot verify exact properties of past behavior based on this information alone.

To tackle this problem, we introduce the concept of uncertainty, expand the subjective logic [2], and design a certainty-oriented reputation system to rationally evaluate trust. Uncertainty refers to the degree to which an individual or organization cannot accurately predict the behavior of its mutual rival or the environment. Uncertainty originates from information asymmetry and opportunism. It reflects whether a trustor has collected enough information from past interactions with a trustee and its confidence in that information. After adding this core dimension of trust into our reputation system, we can clearly separate newcomers from misbehavers and make certainty-based decisions possible. A series of uncertainty deduction formulas is also provided to rationally combine the trustor's first-hand observation with the collected second-hand recommendations.

Uncertainty increases transaction cost and decreases acceptance of communication and cooperation. Our objective is to reduce the trustor's perceived uncertainty so that transaction cost is lowered and a long-term exchange relationship is sustained. One way to efficiently reduce uncertainty is to exploit one important property of MANETs: *mobility*. Node movement can increase the scope of direct interaction and recommendation propagation, thereby speeding up trust convergence. Two categories of schemes, which exploit mobility to assist uncertainty reduction, are presented in this paper.

The proactive schemes aim to disseminate local reputation information by nodes' movement and achieve a global

- *F. Li is with the School of Engineering and Technology, Indiana University—Purdue University Indianapolis, 799 W. Michigan St., ET 301, Indianapolis, IN 46202-5150. E-mail: fengli@iupui.edu.*
- *J. Wu is with the Department of Computer and Information Sciences, Temple University, 324 Wachman Hall, 1805 N. Broad St., Philadelphia, PA 19122. E-mail: jiewu@temple.edu.*

*Manuscript received 18 Sept. 2007; revised 6 Oct. 2008; accepted 6 May 2009; published online 9 Mar. 2010.*
*For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2007-09-0281.*
*Digital Object Identifier no. 10.1109/TMC.2010.44.*

1536-1233/10/$26.00 © 2010 IEEE Published by the IEEE CS, CASS, ComSoc, IES, & SPS

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

trust convergence. In these schemes, mobile nodes build up trust relationships, collect trust information, move, and disseminate the collected information through recommendation whenever they stop again. Nodes received the broadcast recommendation, discounted the trust opinion, and integrated the information with the stored value. This process is repeated infinitely. By doing so, nodes store reputation of nodes in remote regions for future interaction and keep updating to reduce uncertainty.

The reactive schemes focus on dispatching mobile ambassadors to authenticate moving nodes and forward the moving nodes' original reputation to the new destination through recommendation. When a node is expected to move into a destination region to perform a new task, it searches its local area and tries to find the *ambassador* which moves from and represents the destination region. If such an ambassador exists, a recommendation will be issued, which includes the node's current reputation and a signature verifiable to the destination region. The moving node will present this recommendation to get the more precise initial reputation in the destination region.

By proposing these proactive and reactive schemes, we aim to illustrate the positive impacts of mobility on uncertainty reduction. We also offer flexibility for users to achieve their application objectives from a range of trade-offs between delay, cost, and uncertainty provided by the proposed schemes. We study this effect under different mobility models and analyze several factors, which will strongly influence the convergence speed and cost.

The contributions of this paper are as follows:

1. We rigorously define the concept of uncertainty and its role in trust evaluation.
2. We propose a certainty-oriented reputation system.
3. We present various proactive and reactive mobility-assisted uncertainty reduction schemes.
4. We analyze the uncertainty reduction effects under various mobility scenarios.

## 2 Related Work

### 2.1 Trust Management Systems

Various frameworks [3] have been designed to model trust networks and have been used as trust management systems [4]. We can divide them into three main categories. The trust management system in the first category has a central authority, which is usually called the trusted third party (TTP). Entities cooperate on the basis of the trust values (e.g., the authorization certificates) assigned by the TTP. Introducing a TTP will violate the self-organized nature of MANETs, which makes these systems inapplicable in MANETs.

In the second category, one global trust value is drawn and published for each node, based on other nodes' opinions toward it. EigenTrust [1] is one mechanism in this category. The algorithm allows computation of global trust values in the distributed environment. EigenTrust presents the request to separate misbehavers from newcomers. But, it lacks the method to satisfy this request naturally. EigenTrust is just a representative and most existing trust evaluation systems have the same requirement, but omit uncertainty at the same time.

The third category includes the trust management systems that allow each node to have its own view of other nodes. These systems are more realistic as they are similar to the trust models in the social network. Each node builds its view based on the observation as well as the recommendations from others. Many recent reputation systems, such as CONFIDANT [5], CORE [6], and OCEAN [7], belong to this category. In the improved CONFIDANT [8], Buchegger and Boudec provided a modified Bayesian approach for reputation representation, updates, and view integration. When updating the reputation according to recommendations, only information that is compatible with the current reputation rating is accepted. This approach is objective and robust. But, this approach still leaves an opportunity for elaborate attackers to launch false accusation attacks since there is no constraint on update frequency. This approach also lacks the ability to separate newcomers from misbehavers.

Carbone et al. proposed a formal trust structure in [9]. One important contribution of the trust structure is that it allows for an interval between belief and disbelief in order to reflect the uncertainty. The narrower the interval, the lower the uncertainty. The trust domain so obtained in [9] is particularly interesting, as it allows for the expression of complex policies. However, the focus of the trust structure is not the specific definition of uncertainty. Our notion of uncertainty can also be integrated into formally defined trust structures and adopted in enriched policies.

Josang [2], [10], [11] developed an algebra for assessing trust relations, and it has been applied to set up certification chains. In this algebra, the focus is on modeling the uncertainty in the reputation. A triplet designating belief, disbelief, and uncertainty is assigned to each trust statement. Many operators are given for the manipulation of these opinions. This model's strength lies in its ability to reason about the opinions and its consensus, recommendation, and ordering operators. However, its major weakness is that every entity's opinion is based on its own subjective policy, and the system cannot guarantee that users will assign consistent values. It also lacks an operator to synthesize different recommendations.

### 2.2 Mobility Helps Security

Mobility is one of the important characteristics of MANETs [12], and trust evaluation is an important method to stimulate nodes in MANETs to cooperate. However, to the best of our knowledge, there is no literature that fully addresses mobility's influence on trust convergence.

In [13], [14], Wu and coauthors raised the question of whether mobility should be treated as a foe (undesirable) or a friend (desirable). In security-related research, this question also attracted a significant amount of research interest [15], [16], [17], [18]. Some researchers argue that mobility is a hurdle to security, as it makes the authentication and identification process more difficult. Some new mechanisms, such as [17], have been proposed to tackle the problems caused by node mobility in MANETs. Others argue that far from being a hurdle, mobility can be exploited to set up security associations among users. By revising the traditional connection-based models and designing protocols that take mobility into consideration at the beginning, several recent research works show that mobility can be exploited to improve routing capability [19], increase network capacity [20], enlarge sensor coverage [21], and enhance security [16].

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

Movement-assisted models can be classified based on random (uncontrolled) movements, such as epidemic routing [22], and controlled movements, such as message ferrying [19], [23]. Although the mobility pattern of most nodes in MANETs is determined by their own tasks and considered to be random, the controlled-movement-based schemes in MANETs usually assign the specific task to a selected small portion of nodes to enhance the performance.

### 2.3 Vouching-Based Authentication

User authentication [24] in computing systems traditionally depends on three factors: something you have (e.g., a hardware token), something you are (e.g., a fingerprint), and something you know (e.g., a password). In [25], Brainard et al. explored a fourth factor: the social network (somebody you know).

In [25], Brainard et al. introduce the concept of vouching as a tool for online authentication. Vouching directly leverages human relationships, and this work can be seen as part of a broad exploration of the interplay between social networks and user authentication. We extend the fourth factor authentication mechanism. In our reactive schemes, the moving node depends on someone it knows and encounters in the movement to get authenticated and obtain a corresponding certificate.

## 3 Certainty-Oriented Reputation System

### 3.1 Motivations and Assumptions

Uncertainty is an important factor in trust evaluation. How to fully address and model uncertainty, and make it a direct metric is a key problem in trust evaluation system design and implementation. Another problem is to efficiently reduce uncertainty once we know how to evaluate it. In social life, if people want to raise their confidence in the evaluation of someone, they just get closer to that person and create chances for direct contact, or take the recommendations from someone they trust who knows the subject better. In MANETs, mobility increases the chance that two separated nodes meet and directly contact each other. It also allows each node to have more evidence to verify future recommendation. Intuitively, we consider mobility to be a good method of reducing uncertainty.

In this paper, the following assumptions were made: Each node has one unique ID and it cannot be spoofed; a node can only monitor the behavior of its 1 hop neighbor. When two nodes directly contact each other in 1 hop, they have a way to decide whether the result is satisfactory; nodes' behaviors are consistent. A node's general behavior can be deduced from its past actions; nodes are independent from each other, with no collusion. Our reputation system can accommodate independent false praise and false accusation.

### 3.2 Reputation Representation

The representation of reputation reflects the focus of a trust evaluation system. Reputation is the opinion of one entity toward another based on past experiences. In most of the existing systems, reputation is represented as two variables: belief and disbelief. However, dividing trust into only belief or disbelief is not always appropriate. One reputation value based on 10 contact experiences, and another based on 100 contact experiences, have totally different meanings. An ordering between no knowledge and total certainty is needed to reflect the degree of confidence in trust information.

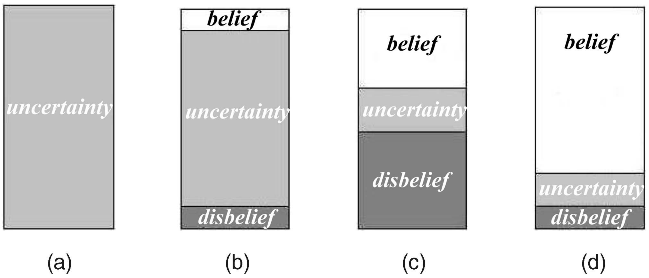


Fig. 1. Reputation representation in CORS. (a) $(1,1)$. (b) $(10,10)$. (c) $(50,50)$. (d) $(90,10)$.

In this system, a one-dimensional representation of belief, disbelief, and uncertainty is extended from the subjective logic [2]. Each node keeps a belief and disbelief value toward other nodes as a prediction of their future behavior. As these two values are only predictions, uncertainty always exists. We use a triplet to represent a node's opinion $(b,d,u) \in [0,1]^3$: $b+d+u=1$. $b$, $d$, and $u$ designate belief, disbelief, and uncertainty, respectively. Fig. 1 illustrates examples of the reputation representation under four different cases.

### 3.3 First-Hand Information Gathering

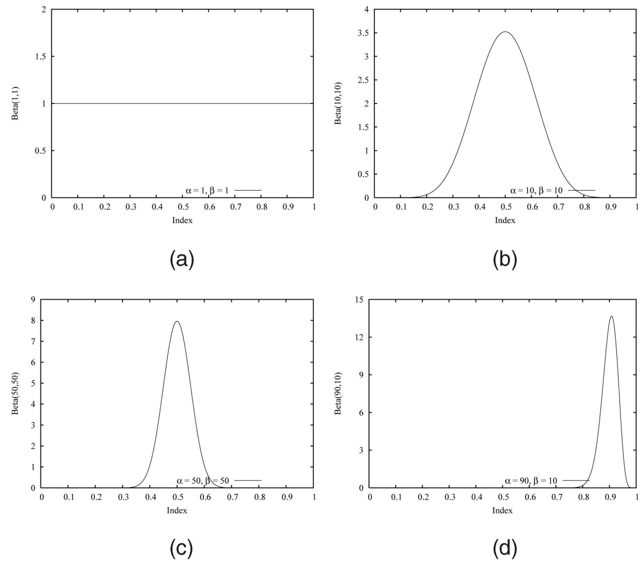
The reputation of a node computed from first-hand information is the reputation based on one's own experience. It is calculated directly from a node's observation. Each node will also propagate this information so that other nodes can use it as second-hand information. Each node estimates its neighbor's reliability based on its accumulated observations using Bayesian inference.

Bayesian inference is a statistical inference in which evidence or observations are used to update or to newly infer the probability that a hypothesis may be true. Beta distributions, $Beta(\alpha,\beta)$, are used here in the Bayesian inference, since it only needs two parameters that are continuously updated, as observations are made. To start, each node in the network has the prior $Beta(1,1)$ for all its neighbors. The prior $Beta(1,1)$ implies that the distribution of the reliability metric $p$ complies with the uniform distribution on $[0,1]$, which indicates complete uncertainty as there are no observations. When a new observation is made, if it is a successful forwarding, then $\alpha$ is updated. Otherwise, $\beta$ is updated. The prior is then updated as $Beta(\alpha,\beta)$ when needed. The triplet $(b,d,u)$ representing the node's opinion is derived from $Beta(\alpha,\beta)$. Fig. 2 shows that different $\alpha+\beta$ influence the density of the distribution.

We believe that uncertainty should include two aspects: one is the total amount of evidence, which is more straightforward. When the total amount of evidence, reflected in $\alpha+\beta$, is larger, the uncertainty is lower. The other aspect deals with whether $\alpha$ or $\beta$ dominates. This aspect actually captures the entropy type of uncertainty. An example is shown in Figs. 2c and 2d. The total number of evidence $\alpha+\beta=100$ in both cases. However, the distribution of the case in Fig. 2d is more concentrated then the case in Fig. 2c, which indicates less uncertainty. Therefore, the uncertainty in Figs. 2c and 2d is actually different although the total amount of evidence is the seem in these two cases.

An everyday example further illustrates this aspect of uncertainty. A fair coin has an entropy of one. However, if

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.



(a) (b)

(c) (d)

Fig. 2. Beta distribution corresponding to cases in Fig. 1. (a) $Beta(1,1)$. (b) $Beta(10,10)$. (c) $Beta(50,50)$. (d) $Beta(90,10)$.

the coin is not fair, then the uncertainty is lower (if asked to bet on the next outcome, we would bet preferentially on the most frequent result), and thus, the Shannon entropy [26] is lower. Similarly, in our environment, with the same total amount of evidence, a node would be most uncertain as to whether its neighbor under observation will behave good or bad in the next round when $\alpha = \beta$. If $\alpha$ ($\beta$) dominates, the neighbors will be more likely to bet on the fact that the node under observation is good (bad).

In order to capture both aspects in the design of the uncertainty notion, we define uncertainty $u$ as the normalized variance of $Beta(\alpha, \beta)$ as follows:

**Definition 1 (Uncertainty computation).** *The uncertainty should be calculated as follows:*

$$u = \frac{12 \cdot \alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)}. \tag{1}$$

There are two attributes for this uncertainty definition. First, when $(\alpha + \beta)$ is higher, it implies that there is more evidence, which consequently lowers uncertainty $u$ according to the above definition. Second, when the evidence for success or failure dominates, there will be less uncertainty when compared to the situation in which there is equal evidence for both success and failure. This property is reflected by the fact that uncertainty $u$ will be at its peak when $\alpha = \beta$ for any given $(\alpha + \beta)$. The numerator and denominator in Formula 1 guarantee the latter and the former attributes, respectively.

The total certainty is $(1 - u)$, which can be divided into $b$ and $d$ according to their proportion of supporting evidence. Since the proportion of supporting evidence for the statement that the transmission between two nodes is reliable is $\frac{\alpha}{(\alpha+\beta)}$, $b$ can be calculated as follows: $b = \frac{\alpha}{(\alpha+\beta)} \cdot (1 - u)$. Therefore, $d = (1 - u) - b = \frac{\beta}{(\alpha+\beta)} \cdot (1 - u)$.

### 3.4 Second-Hand Information Integration

Using first-hand information alone is not cost effective. Reputation exclusively based on direct contact increases the detection time when compared to an approach that also uses reports from others. The more information each node considers, the faster the trust evaluation achieves convergence.

Second-hand information is the information that a node gets from the first-hand information published by other nodes. It is a kind of trust transitivity. Node A first gathers other nodes' first-hand observations (in $\alpha, \beta$) toward node C. Node A converts the information (in $\alpha, \beta$) into an opinion (in $b, d, u$) and discounts it by node A's opinion toward the node reporting the observation. We call this the recommendation calculation. After gathering all the recommendations, node A will synthesize them and integrate the second-hand information with the first-hand observation and make a final anticipation and decision.

**Definition 2 (Recommendation calculation).** *Let* $R_C^B = \{b_C^B, d_C^B, u_C^B\}$ *represent node B's opinion toward C, and* $R_B^A = \{b_B^A, d_B^A, u_B^A\}$ *represent node A's opinion toward B. Then, node A will take node B's recommendation toward node C as* $R_C^{A:B} = \{b_C^{A:B}, d_C^{A:B}, u_C^{A:B}\}$, *where*

$$b_C^{A:B} = b_B^A \cdot b_C^B; \quad d_C^{A:B} = b_B^A \cdot d_C^B,$$
$$u_C^{A:B} = b_B^A \cdot u_C^B + d_B^A + u_B^A.$$

Definition 2 presents how node A computes the recommendation given by node B toward node C. The same formulas are used as the subjective logic [2] because they are both uncertainty centric and comply to common sense. Thus, A's belief toward B's opinion is directly converted into A's belief, disbelief, and uncertainty. Node A's disbelief in B's opinion becomes uncertainty toward C rather than becoming disbelief toward C. A's uncertainty in B also becomes part of the uncertainty in C. Notice that when node A's belief in B is high ($b_B^A \rightarrow 1$), the calculated recommendation will remain the same as B's opinion. The trust decay is low in this case as A trusts B.

Most existing research papers [6], [8], [7], [5] related to reputation systems use one integrated trust value to depict the overall trustworthiness of a node, which includes the recommendation trust. This actually simplifies nodes' behavioral model and utilizes the underlining assumption that a node's behavior will be consistent in all aspects, including forwarding behavior in MANETs and recommendations. This also complies with our daily experience: We give more weight to the recommendations from our intimate friends, although our friendship is usually based on the overall behavior.

We adopted a single integrated reputation in this paper to make it focus on the uncertainty. However, we also developed a trust system that separates behavioral trustworthiness with recommendation competency in our previous paper [27]. We considered it as applicable to the MANETs, and can calculate two distinct sets of belief, disbelief, and uncertainty for behavior trustworthiness and recommendation competency distinctively. But it also requires a significantly higher amount of evidence to reduce uncertainty to a the same level as the schemes using one set of trust values.

**Definition 3 (Recommendation synthesization).** *Let* $R_C^{A:B_i} = \{b_C^{A:B_i}, d_C^{A:B_i}, u_C^{A:B_i}\}$ *represent node* $B_i$*'s recommendation toward node C computed by node A, for* $1 \leq i \leq n$. *Then, node A will synthesize these recommendations as*

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

$$R_C^{A:\{B_1,\ldots,B_n\}} = \{(b_C^{A:B_1} + \cdots + b_C^{A:B_n})/n, (d_C^{A:B_1} + \cdots + d_C^{A:B_n})/n, (u_C^{A:B_1} + \cdots + u_C^{A:B_n})/n\}.$$

A simple method to calculate the average is used to synthesize the recommendations from different nodes toward one particular node. As shown in the following example, this weighted average process makes the model resilient to false praise and accusation. When a misbehaving node's recommendation is highly different from other nodes, it will raise the trustor's uncertainty.

**Definition 4 (Opinion combination).** *Let $\gamma$ be a node's character factor. Each node A will combine its first-hand and second-hand opinion toward B as:*

$$x_B^{A_f} = \phi_1 \cdot x_B^{A^{1st}} + \phi_2 \cdot x_B^{A^{2nd}},$$

*where $x \in \{b, d\}$, $u_B^{A_f} = 1 - b_B^{A_f} - d_B^{A_f}$ and*

$$\phi_1 = \frac{\gamma \cdot u_B^{A^{2nd}}}{(1-\gamma) \cdot u_B^{A^{1st}} + \gamma \cdot u_B^{A^{2nd}} - 0.5 \cdot u_B^{A^{1st}} \cdot u_B^{A^{2nd}}},$$

$$\phi_2 = \frac{(1-\gamma) \cdot u_B^{A^{1st}}}{(1-\gamma) \cdot u_B^{A^{1st}} + \gamma \cdot u_B^{A^{2nd}} - 0.5 \cdot u_B^{A^{1st}} \cdot u_B^{A^{2nd}}}.$$

If $\gamma$ is greater than 0.5, it means that a node tends to trust its own experience. If $\gamma$ is less than 0.5, it means that a node tends to trust others' recommendations. In this equation, $u_B^{A^{1st}}$ and $u_B^{A^{2nd}}$ are also two important factors. When the trustor is uncertain about one thing, it tends to learn from others' opinions with less uncertainty. Otherwise, its belief tends to be firm and others' opinions are less influential. $\phi_1$ and $\phi_2$ are composite factors which reflect the combined final weight.

## 4 Mobility-Assisted Uncertainty Reduction

Node movement increases the chance for potential contactors to gather more trust information and evidence, thus enlarging the scope of reputation qualified candidate nodes for future tasks. We present a detailed discussion on the effect of mobility on uncertainty reduction in this section.

Assume that trust events happen at a uniform rate $\rho$ between each pair of 1 hop neighbors. Each node's actual behavior is consistent and can be described as $\theta$ as in [5], which is the probability that a node will be honest in the trust events. A node's average moving speed is $v$. The moving cost per unit of distance is $c_m$. The unit cost of the trust event (such as one message exchange) is $c_e$. We use the total cost and delay (convergence time) to study the uncertainty reduction efficiency of each scheme.

### 4.1 Trust Information Dissemination: The Proactive Schemes

The first category of schemes exploits mobile nodes in an effort to disseminate local reputation values and collects reputations from other areas through recommendations. The goal of these schemes is to collect enough trust information from the interested areas, form stable trust opinions, and reduce the uncertainty in the trust opinion to a required degree. The reputation for remote nodes is integrated and stored for possible future interactions. Different mobility schemes lead to different convergence speeds and costs. These schemes are considered to be proactive as the trust information is disseminated before needed.

Here, a theorem is established to continue the research. $U_{max}$ is an uncertainty threshold that nodes are required to satisfy before we begin any trust-based MANET application.

**Theorem 1 (Pause time).** *In each step, a pair of nodes should interact at least $\frac{3}{U_{max}} - 1$ times to satisfy the uncertainty threshold requirement.*

**Proof.** We require: $u \leq U_{max}$ and compute $u$ as in Definition 1. We use $x = \alpha + \beta$ to represent total number of interactions. For a given $x$, when $\alpha = \beta = \frac{x}{2}$, $u$ achieves maximality. So, $x \geq \frac{3}{U_{max}} - 1$ guarantees that $u \leq U_{max}$. □

We first analyze the effect of mobility without controlling any nodes' movement. Using the random waypoint model, nodes will have a new neighborhood during each pause time. A node can contact and observe its new neighbors directly. The results of these direct contacts increase the $\alpha$ or $\beta$ in both nodes' first-hand opinion, therefore reducing uncertainty. However, the randomness also restricts the use of second-hand information. In each pause time, the disbelief and uncertainty between the newly encountered nodes are uncontrollable. In most cases, recommendations from new neighbors have a high level of uncertainty. Therefore, the efficiency of the uncertainty reduction is relatively lower than in other schemes. We will further investigate the uncertainty reduction effect under the random mobility models in the simulation.

Although the moving patterns of most nodes in the MANET are considered to be naturally random and independent of each other, controlling the moving trajectory and rendezvous points of a small portion of nodes to achieve better performance is considered to be possible in many recent research papers, such as [19], [14]. Therefore, we also analyze the proactive uncertainty reduction schemes while controlling the moving trajectory and rendezvous points of a very small portion of nodes. These selected nodes are regarded as being assigned the task of uncertainty reduction, and their movement should be considered as the cost of uncertainty reduction. This does not contradict with the motive and properties of MANETs. We first analyze two straightforward controlled movement models for comparison purposes. We then propose a hierarchical scheme which can provide flexible trade-offs with low cost.

#### 4.1.1 *Town Hall Scheme*

The first straightforward scheme is shown in Fig. 3a: All nodes in the network travel to one grid, pause for a sufficient time, build up trust, and reduce the uncertainty of other nodes to a required degree. After that, all nodes move back and will be able to perform tasks that demand remote nodes to cooperate and have trust requirements. We can approximate this model as all nodes start moving from the center of their grid, to the center of the network, pause for some time, and move back. The town hall model will lead to a relatively short convergence time with an extremely high cost.

#### 4.1.2 *Traveling Preacher Scheme*

Another straightforward scheme is to select one common trusted node to travel around all the grids through a Hamiltonian path, as shown in Fig. 3b. That node's movement can be divided into two rounds. In the first round, it pauses in each grid for a sufficient time to collect trust information. In the second round, it travels to each

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

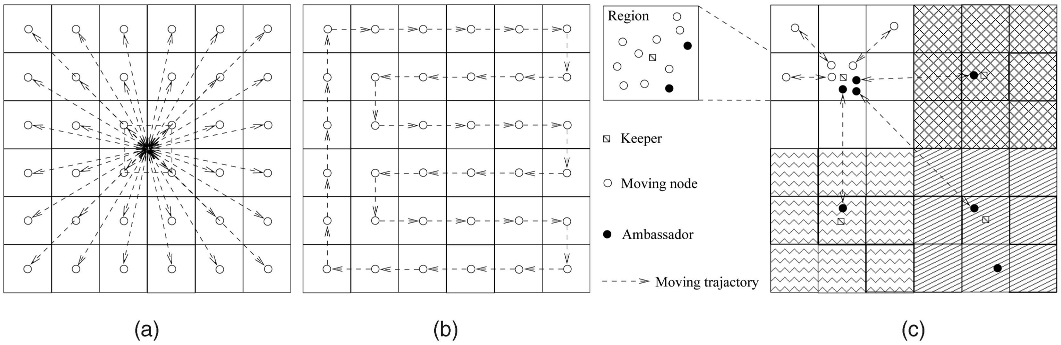


Fig. 3. Proactive mobility-assisted uncertainty reduction schemes. (a) Town hall. (b) Traveling preacher. (c) Hierarchical.

grid again to disseminate all the gathered trust information about other grids using the recommendation mechanism.

An important issue in this model is deciding the traveling preacher. One possible method is to let the system assign one node to be the preacher, and all other nodes should assign $b = 1$ to that moving node. But, this violates the self-organized rule of MANETs. Another option is to let the nodes elect one node that satisfies some condition to travel around. We will discuss the detailed election scheme later. Traveling preacher model shows a long convergence time but with an extremely low cost.

### 4.1.3 Hierarchical Scheme

When the requirement is a short convergence time to quickly start a trust-based application, or a controllable cost, the above two mobility models will offer extreme options. However, these two methods are not flexible enough and we lack a way to find a trade-off between convergence time and cost to satisfy different application objectives. Here, we present a two-level controlled mobility model, which is called hierarchical scheme. In hierarchical scheme, we divide the whole network into several regions, allowing each region to contain a specified number of grids, and choose mobility models for inter- and intraregion movement. Hierarchical scheme combines the advantages of the above two models and offers more options for MANET implementation. Various kinds of clustering mechanisms have been proposed in the MANETs [28], [29]. After using one of the existing clustering mechanisms, this hierarchical scheme can be applied on top of the clusters. The design of the hierarchical scheme consists of the following three parts:

**Moving node election.** After the cluster has been set up, all the nodes in the cluster will contact each other locally, build up trust, and compute reputation according to the previously discussed reputation system. After a sufficient pause time, each node will vote for the node with the largest belief and smallest uncertainty to move. The voting process can be described as Algorithm 1. Here, $B_{min}$ is the belief threshold. $\lambda$ is the required proportion of votes to win an election. $U_{max}$, $B_{min}$, and $\lambda$ should be regulated in the clusters' voting policy and represent the reputation requirements for a moving node. Each node sets a pause timer and will cast only one vote after time-out.

**Algorithm 1.** VoteForMove

```
while the timer lasts do
    Get first-hand observation and change $\alpha, \beta$
    accordingly when an event occurs;
    Update second-hand opinion accordingly when a
    recommendation comes;
end while
Compute combined opinion $b, d, u$ for each node;
if the largest $b$ in all the opinions satisfy $b \geq B_{min}$
then
    Vote the node with the largest $b$;
    Wait for the confirmation from elected moving
    node;
else
    Continue trust information collection;
end if;
```

As described in Algorithm 2, a node should wait until it gathers enough votes to move. It will go through a defined trajectory to collect the trust information for its home cluster. Nodes have already been organized into clusters based on which grid they belong to. The network is then divided into a number of regions. Each region selects one grid to be its *capital*. All of the elected moving nodes move to the capital of the region.

**Algorithm 2.** VoteGathering

```
Vote counter+1 when a vote comes;
if vote counter $\geq \lambda$ proportion of the nodes in the
cluster then
    Node broadcasts an elected confirmation and starts
    to move;
end if;
```

The moving nodes repeat the local contact process after they arrive in the capital. The pause time period in the capital allows them to build trust between each other and the local nodes of the capital. One node, which is commonly trusted by all moving nodes, will be elected to be the *keeper* of that region through a process similar to Algorithms 1 and 2. The keeper selects several nodes it trusts as *ambassadors*, which will travel between regions to collect information and feed it back to the keeper.

**Region partition.** The election process creates different roles to handle different trust information collection and dissemination tasks for intragrid, intraregion, and interregion. As we will use different methods to handle different classes of tasks, how to partition the region becomes an important design issue. The analysis of the town hall and traveling preacher models shows that the cost in the town hall model is positively proportional to the square of the

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

number of moving nodes, while the total pause time of the traveling preacher model is decided by the number of stops. To offer a more flexible uncertainty reduction-oriented mobility model, we can choose an optimal number of regions based on node density, network scale, and application-related cost and convergence time objectives. For a $2^k \times 2^k$ network, $2^0 \times 2^0, 2^1 \times 2^1$ until $2^k \times 2^k$ are possible region sizes. We can compute the convergence times and costs for each of these possible region sizes and select the optimal one as the scheme for region partition.

**Moving pattern control.** As we divide the network into regions consisting of grids, an optimal moving pattern for the inter- and intraregion levels must be selected.

For the intraregion level, we select an extension of the town hall method. Each grid elects a commonly trusted moving representative, and these nodes move to the capital to exchange intraregion trust information.

For the interregion level, a method will be chosen according to the number of regions and the distance between capitals. Possible moving patterns for the interregion level are town hall, traveling preacher, and another straightforward model, which we call *exchange ambassadors*. Using the town hall model will largely increase the uncertainty decay in recommendations from other regions. Considering a limited number of regions, an extension of the traveling preacher model can be applied and the time burden will be acceptable. In this extension, each region sends a moving node as the trusted representative to travel around the capitals and collect information only for its home region. Exchange ambassadors means that each pair of regions exchange trusted moving nodes which collect trust information for their home regions. It is a high-cost and low-convergence time method, and is especially suitable for a small number of regions. The main problem with this method is the ambassador selection. The keeper may not be able to find as many trustworthy ambassadors as it needs.

## 4.2 Authentication via Ambassadors: The Reactive Schemes

In reactive schemes, reputations are disseminated only when needed. The basic idea of these schemes is as follows: each region selects a number of mobile nodes that move out of the region and assigns them the role of *ambassador*. When a mobile node wants to move to any such region, it tries to get a start-up recommendation, which grants it a better initial reputation in the destination region. To do this, it needs to find an ambassador of the region and request a visa. The ambassador issues the visa and signs it by a verifiable key from the region it designates. The visa contains the collected local reputation toward the mobile node.

In the model, a node stays in its home region for a long period of time before it moves. After completing the tasks in that region, the node moves to the destination region in order to conduct a new task, which usually requires a long stay and cooperation from the other nodes in the destination region. After finishing it, the destination region becomes the new home region for the node's later movement.

Each node $i$ generates a private key $RK_i$ and public key $PK_i$ pair. $RK_i$ can be regarded as node $i$'s personal secret. $PK_i$ is distributed in the home region. Nodes in the home region can use direct contact to verify the identity when it receives the public key. They also monitor the behavior of $i$ and use a reputation system to draw trust opinions toward it.

Some nodes are selected to act as ambassadors of their home region. For these ambassadors, their home region will assign another kind of key for them, known as a *cachet* key $CK$. The ambassador uses $CK$ to represent its home region and provide authentication. The $CK$ is a pairwise secret key. In each region, a commonly trusted node is elected by using methods similar to Algorithm 1 and acts as the cluster head $CH$ in the region. It generates a key pool which contains a certain number of valid cachet keys: $CK^1$; $CK^2; \ldots; CK^n$. When an ambassador is about to move, the $CH$ assigns a key from the key pool.

We propose four reactive schemes which use different ambassador dispatching and seeking methods. The simple and history-based schemes are based on the random movement model, while the cross and metropolis schemes need to control ambassadors' movement. Each produces different probabilities of getting authentication for the incoming nodes.

### 4.2.1 Simple Scheme

In the simple selection scheme, when a node is about to move to a destination region, it will inform the $CH$ of its home region about its destination. The $CH$ checks the following conditions and decides whether to assign the outgoing node $i$ the duty of ambassador: 1) $Rep_i \geq T$, 2) the public key of $i$ is properly stored, and 3) no record indicates that a valid ambassador exists in the intended destination region of node $i$. Here, we use $Rep_i$ to represent node $i$'s reputation in the home region, and $T$ is the threshold of reputation which represents the $CH$'s requirement for its ambassadors. These conditions are the basic requirements for ambassadors, which are also adopted by the following three schemes.

When searching for the ambassadors, the moving node only investigates its home region for an ambassador of the destination region. If it cannot find the ambassador, it directly moves to the destination. If the moving node found an ambassador of the destination region in its home region, the ambassador generates a certificate as the visa. This process is illustrated in Fig. 5. In this visa, the ambassador should include node $i$'s public key $PK_i$, $i$'s reputation in the home region $Rep_i$, and signed by the cachet key $CK$ from the ambassador's home region $visa = E_{CK}\{PK_i|Rep_i\}$. Here, $E_{CK}$ means encrypting by $CK$.

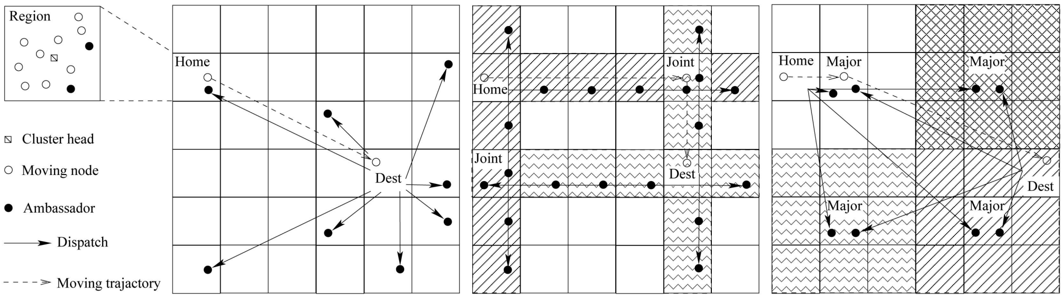
The moving node takes this visa to its destination region. Upon arrival, it presents the visa to the $CH$ in the destination region. The $CH$ verifies the visa, broadcasts the moving node's public key, and announces its reputation as the initial reputation of the moving node in the region.

### 4.2.2 History-Based Scheme

The nodes' movement is not always purely random, and the destination of an outgoing node could be vague before moving. If the destinations of outgoing nodes follow certain probability distribution, a history-based dispatching scheme is useful. This mobility model, denoted as the restricted random waypoint model in [16], is considered to be more realistic.

Using this model as the underlying mobility scheme, the outgoing node $i$ has the probability $p_i^j$ to go to region $R_j$.

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.



(a) (b) (c)

Fig. 4. Ambassador Dispatching Schemes. (a) General dispatching. (b) Cross dispatching. (c) Metropolis dispatching.

Each region $R_h$ also counts the incoming probability from another region $R_j$, which is the number of incoming nodes from $R_j$ divided by the total number of nodes coming to the $R_h$. We call this probability $q_h^j$.

When selecting ambassadors, a selection period is applied. The $CH$ will first record all the nodes that applied to move in the selection period. The $CH$ will deter the movement until the end of the selection period. Algorithm 3 is then applied to select $k$ nodes to be the ambassadors. The history-based scheme shares the same ambassador seeking and visa issuing rules as the simple scheme.

**Algorithm 3.** History-based selection

```
while the selection period timer lasts do
    if a node satisfies requirements and requests to move then
        Add possible destination regions into set $D$, and the node into ambassador candidate set $C$;
    end if;
end while;
Sort $D$ based on $q_h^j$;
Keep the first $k$ regions in $D$ and cut-off other regions;
for the region $R_j$ with largest $q_h^j$ in $D$ do
    Assign $CK$ to the node $i$ with largest $p_i^j$, and announce $i$ as the ambassador;
    Delete $R_j$ from $D$ and $i$ from $C$;
end for;
```

### 4.2.3 Cross-Dispatching Scheme

In the above two schemes, incoming nodes can be directly authenticated by an ambassador with certain probability. When the number of ambassadors is much smaller than the number of regions, the probability can be fairly low. In the cross-dispatching scheme, incoming nodes are guaranteed to be authenticated by an ambassador of the destination region. However, in this scheme, the movements of the ambassadors are not random, and indirect authentication should be allowed.

Assume that we have $n \times n$ regions, as shown in Fig. 4a. Each region sends one ambassador for each region in the same column and one ambassador for each region in the same row. For a moving node, there are two regions called *joint regions* in the network that have ambassadors from both its home region and destination region. Therefore, a trust transition chain can be formed if we require the moving nodes to move to a joint region before entering the destination region.

In the ambassador seeking phase, the moving node still searches its home region first. If it cannot find the ambassador of the destination region, it moves to the closest joint region to continue the searching.

When a moving node cannot find an ambassador for the destination region in its home region, it turns to ask the $CH$ to issue a visa that is verifiable to the ambassador of the home region. This visa is signed by the same cachet key as the ambassador's. This visa is in the form: $visa = E_{CK}\{PK_i|Rep_i\}$. When the moving node $i$ enters the joint region, it presents its visa to the ambassador of its home region. The ambassador of the home region $A_h$ then requests the public key of the ambassador of the destination region $A_d$ from the $CH$ of the joint or major region. The $A_h$ sends the request for a visa to $A_d$, which contains its recommendation to $i$. Let $Rep_i'$ denote $A_d$'s discounted opinion toward $i$, $A_d$ generates a new visa by using its cachet key $C\tilde{K}$ which is verifiable to the destination region: $visa' = E_{C\tilde{K}}\{PK_i|Rep_i'\}$.

### 4.2.4 Metropolis Scheme

To offer more flexibility, a hierarchical dispatching scheme is developed. We can organize regions into areas, as shown in Fig. 4b. In each area, a "major" region is selected. When a region decides to dispatch ambassadors, it will first send ambassadors to major regions. When a node decides to move, it obtains a visa that is verifiable to the ambassador of its home region. It then moves to the nearest major region.

As the ambassador of the home region and the destination region can be found in the same "major" region, the reputation (discounted by the trust between two ambassadors) of the moving node can be passed, and it will get a visa verifiable for the destination region.

The metropolis scheme shares similar ambassador seeking and visa issuing rules with the cross-dispatching scheme. The only difference is that it uses the closest major region instead of the joint region.

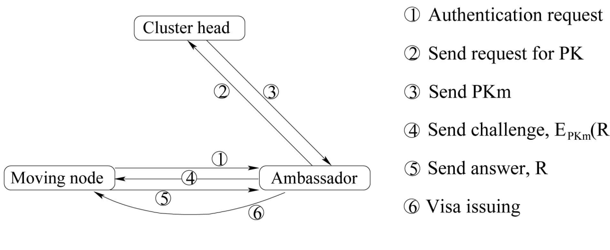


Fig. 5. Visa issuing process.

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

## 5 Analysis

Both proactive and reactive schemes offer many ways to adjust the trust convergence delay and cost related to a specific certainty goal. We analyze the trade-offs between delay, cost, and uncertainty in different mobility-assisted uncertainty reduction schemes, so as to provide flexible and controllable methods to support reputation-based applications in MANETs.

### 5.1 Proactive Schemes

Assume a grid-based model of size $2^k \times 2^k$. All the nodes in a $1 \times 1$ grid form a cluster. Although the basic model can be easily converted to other models, the grid-based model is chosen for its simplicity. Set the wireless communication range to 1 unit of distance. Each node in a cluster knows which grid it belongs to and the number of nodes in the same cluster. $N$ is used to represent the number of grids in the network $N = 2^k \times 2^k = 4^k$. Each grid has $n$ nodes.

#### 5.1.1 Trust Decay

Different from the town hall and traveling preacher scheme, the hierarchical scheme needs 2 hops of recommendation. Therefore, the trust decay in this process can be summarized as the followings:

**Theorem 2.** *In the hierarchical scheme, when the moving node goes back to its home cluster, the upper bound of uncertainty on the $\lambda$ portion of nodes that voted for the moving node is*

$$u \leq 1 - B_{min} + B_{min} \cdot \frac{3}{\rho \cdot T_p + 1}.$$

**Proof.** Based on Algorithms 1 and 2, the moving node is approved by at least $\lambda$ percentage nodes in the home cluster. For these nodes, the opinion $b, d, u$ toward the moving node should satisfy $b \geq B_{min}$ and $u \leq U_{max}$. The moving node broadcasts its first-hand observation $\alpha, \beta$ for the place of interest. $T_p$ represents the moving node's pause time in the place of interest, and we have $\alpha + \beta = \rho \cdot T_p$.

None of the nodes in the home cluster have any previous knowledge about the remote interest node, so for the ordinary nodes in the home cluster $u^{1^{st}} = 1$. From Definition 1, when $\alpha = \beta = 0.5 \cdot \rho \cdot T_p$, the uncertainty in the moving node's broadcast opinion will achieve a maximum. Using Definition 2 to compute the recommendation opinion from a moving node, $u^{2^{nd}} = b \cdot u_m^{1^{st}} + d + u$. As $b \geq B_{min}$ and $d + u = 1 - b$, for those nodes who vote for the moving nodes $u^{2^{nd}} = 1 - b \cdot (1 - u_m^{1^{st}})$. Because $u^{1^{max}} = 1$ and using Definition 4, we get $u \leq 1 - B_{min} + B_{min} \cdot \frac{3}{\rho \cdot T_p + 1}$ for all the nodes who vote for the moving node. □

It can be seen that the upper bound for the uncertainty of the remote interest node, after the moving node comes back and broadcasts its observation, is decided by two factors. The first one is a base uncertainty $1 - B_{min}$, which is decided by $B_{min}$, the threshold belief for moving. This $B_{min}$ is decided by the policy of the MANET. This requirement can be satisfied if nodes' actual behavior factor $\theta$ complies to normal distribution and the number of nodes $n$ in a cluster is large enough. For the second part of uncertainty $B_{min} \cdot \frac{3}{\rho \cdot T_p + 1}$, the longer the pause time of the moving node in a remote interest place, the smaller the uncertainty will be.

We now choose the town hall and exchange ambassador schemes for intra and interregion movement and select the number of regions as $4^i$. We can adjust some factors to achieve certain convergence time and cost objectives.

#### 5.1.2 Convergence Time

Given an uncertainty requirement $U_{max}$, the convergence time is $(\frac{3}{U_{max}} - 1)/\rho + \frac{2^k}{v}$ by using the town hall scheme; the convergence time of the traveling preacher scheme is $\frac{2 \cdot 4^k}{v} + (4^k \cdot \frac{3}{U_{max}})/\rho$, since the moving time is $\frac{2 \cdot 4^k}{v}$ and the pause time is $(4^k \cdot \frac{3}{U_{max}})/\rho$; the convergence time of the hierarchical scheme can be described as:

**Theorem 3.** *Given the threshold $U_{max}$, the convergence time of the hierarchical scheme is*

$$T = \frac{2^{k+2} \cdot (1 - 2^{-i})}{v} + \frac{9}{U_{max} \cdot p}.$$

**Proof.** The total convergence time will include three pause periods and two moving periods. The three pause periods include the local election period, moving nodes' pause time in the capital, and ambassadors' pause time in foreign capitals. The ambassadors will go back to the home capital and broadcast once. The moving nodes will do the same thing in their local grid. According to Theorem 1, all three pause periods should satisfy the $U_{max}$ requirement. The total pause time should be: $T_p = 3 \cdot \frac{3}{U_{max} \cdot p} = \frac{9}{U_{max} \cdot p}$.

The moving time includes the time for moving nodes to travel to the capital and back, and the time for ambassadors to travel to the foreign capitals and move back. We will compute the travel time for the farthermost grid/foreign capital. The travel time is $\frac{2 \cdot (2^{k-i} + 2 \cdot 2^k - 2 \cdot 2^{k-i})}{v} = \frac{2^{k+2} - 2^{k-i+2}}{v}$. □

#### 5.1.3 Cost

Applying the town hall scheme, the total moving distance is $8^k \cdot n$ and the number of interactions is $C^2_{4^k \cdot n} \cdot (\frac{3}{U_{max}} - 1)$. Therefore, the total cost is $8^k \cdot n \cdot c_m + C^2_{4^k \cdot n} \cdot (\frac{3}{U_{max}} - 1) \cdot c_e$; using the traveling preacher scheme, the total moving distance is $2 \cdot 4^k$ and the number of interactions is $4^k \cdot n \cdot \frac{3}{U_{max}}$. So, the total cost is $2 \cdot 4^k \cdot c_m + 4^k \cdot n \cdot \frac{3}{U_{max}} \cdot c_e$; the total cost of the hierarchical scheme can be described as:

**Theorem 4.** *Given the threshold $U_{max}$, the convergence time of the hierarchical scheme is*

$$C = 4^i \times \Bigg( (8^{k-i} + 2^{k-4}) \cdot c_m + \left( \frac{n \cdot (n-1) + 4^{k-i} \cdot (4^{k-i} - 1)}{2} + 4^k \right) \cdot \left( \frac{3}{U_{max}} - 1 \right) \cdot c_e \Bigg).$$

**Proof.** For each region, the cost of trust events happening during the moving node selection period of each grid should be $\frac{n \cdot (n-1)}{2} \cdot (\frac{3}{U_{max}} - 1) \cdot c_e$.

Each region contains $2^{k-i} \times 2^{k-i}$ grids, and $4^{k-i}$ elected moving nodes will move to the capital. Similarly, we can

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

get the cost of interactions between the moving nodes. The cost for intraregion movement is: $8^{k-i} \cdot c_m$. So, the total cost for the intraregion should be: $C_{intra} = 4^i \times (8^{k-i} \cdot c_m + (\frac{n \cdot (n-1) + 4^{k-i} \cdot (4^{k-i}-1)}{2}) \cdot (\frac{3}{U_{max}} - 1) \cdot c_e)$.

Each region will send out $4^i - 1$ ambassadors and one keeper. The cost of interregion movement should be: $C_{inter} = 2^{k+2i-4} \cdot c_m + 4^{k+i} \cdot (\frac{3}{U_{max}} - 1) \cdot c_e$. □

Theorems 3 and 4 illustrate that the way in which the network is partitioned decides the convergence time and cost. By adjusting $i$ in the above equations, a trade-off between the convergence time and cost can be found.

The trust opinion for nodes in the same region (except the home grid and the capital) will go through 3 hops. For nodes in different regions, the opinion will go through 4 hops. Whenever a trust opinion goes through one more hop, the uncertainty will at least increase $1 - B_{min}$, where $B_{min}$ can be different for each layer. If there are more than two layers in the hierarchical moving model, the uncertainty will be high.

## 5.2 Reactive Schemes

In the analysis, the following parameters are used: the network contains $n \times n$ regions, there exist $m$ major regions when applying the metropolis scheme, and each region selects $k$ nodes as ambassadors.

### 5.2.1 Trust Decay

The procedure can be considered a recommendation reasoning process. Using simple or history-based selection, the trust chain in this case is: 1) the ambassador authenticates and collects original reputation of the incoming node, 2) $CH$ receives recommendation from the ambassador, and 3) $CH$ broadcasts recommendation to nodes in the destination region.

The ambassador gets moving node $i$'s reputation from $i$'s home region. This reputation is considered to be the base with the original uncertainty. In step 2, as the ambassador is the selected delegate of $CH$, $CH$ should trust it. In step 3, nodes discount the reputation based on their trust. As the $CH$ is the commonly trusted node in the region, the uncertainty in the opinion should increase only a small amount.

When using the cross or metropolis dispatching scheme, the trust transition chain is more complicated:

1. the $CH$ of the home region authenticates and collects original reputation of the moving node,
2. $A_h$ receives recommendation from that $CH$,
3. $A_d$ receives recommendation from $A_h$,
4. $CH$ of the destination region receives recommendation from $A_d$, and
5. $CH$ broadcasts recommendation to nodes in the destination region.

In this case, since $A_h$ and $A_d$ are selected by their $CH$, respectively, before they move into the joint or major region, high disbelief or uncertainty may exist. Step 3 brings much higher uncertainty compared to the previous case.

However, there is still one more case to be examined. When a node cannot find an ambassador and moves to the destination region without getting authentication, the node will start with $u = 1$ in the new region, as the destination region has no information about the newcomer.

### 5.2.2 Cost

The analysis of the cost focuses primarily on the number of ambassadors and the movement model. If the cost is not considered, an extreme solution, in which each region sends ambassadors to cover all the other regions, will outperform the proposed schemes. However, it incurs a huge cost as the total number of ambassadors is $n^2 \cdot (n^2 - 1)$. Therefore, a parameter $k$, which is the designed number of ambassadors, can be used to achieve a trade-off between cost and authentication probability in the proposed schemes.

The ambassadors' movement model is also greatly related to the cost. For schemes like simple selection and the history-based scheme, to be an ambassador is only a "part-time" job. The costs for these schemes are relatively low.

The cross scheme requires the controlled movement of its ambassadors. The number of ambassadors is fixed to $2 \cdot n$. Its cost is relatively high compared to other schemes, but that is necessary to achieve the guaranteed authentication.

**Theorem 5.** *The total additional moving distance when using cross scheme is*

$$2 \cdot n \cdot \left( \sum_{i=1}^{n} ((i-1) \cdot i) + (n-i) \cdot (n-1+1) \right) = O(n^4).$$

The metropolis scheme is the most flexible one to achieve the cost trade-off. When the $k < m$, the cost and successful authentication trade-off can be achieved by adjusting $k$. When $k = m$, the guaranteed authentication is achieved.

### 5.2.3 Delay

We use relative moving delay, which is the time a moving node takes to find the ambassador, get authenticated, and move to the destination region compared to the time that the moving node needs to directly get to the destination region. For the simple or history-based selection scheme, the relative moving delay is 1, as the moving node will not change its trajectory to find an ambassador.

For the cross and metropolis schemes, the relative moving delay for the cross scheme varies from 1 to $\sqrt{2}$. The best possible delay is achieved when the home and the destination regions are in the same column or in the same row. The relative moving delay of the metropolis scheme depends on the number of predefined major regions $m$. If the major regions are uniformly distributed in the network, larger $m$ will lead to smaller relative moving delays. In this scheme, the worst case occurs when the home and destination region are adjacent to each other, while their distance to the closest major region is the maximum possible value. Therefore, the worst relative moving delay is $2\sqrt{2} \cdot \sqrt{\frac{n^2}{m}}$.

### 5.2.4 Authentication Probability

The probability of successfully getting authenticated depends on the parameter $k$. For the simple selection scheme, this probability is quite direct. As each region randomly selects ambassadors for $k$ other regions, the authentication probability is $\frac{k}{n^2-1}$.

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

For the history-based scheme, a region $R_h$ records the history sources of the incoming nodes and ranks these source regions according to the incoming probability $q_h^j$. The outgoing nodes with higher probability to go to those higher ranking regions will have higher priority to be selected as the ambassador. Suppose the first $k$ ranked source regions are $R_1, \ldots, R_k$, and the incoming probability is $q_h^1, \ldots, q_h^k$. The probability that an incoming node comes from the rest of the $n^2 - k - 1$ regions is $q = 1 - q_h^1 - \cdots - q_h^k$. The authentication probability in this case is

$$\sum_{j=1}^{k} \left(p_i^j \cdot q_h^j\right) + \frac{\sum_{j=1}^{k} \left(\left(1 - p_i^j\right) \cdot q\right)}{n^2 - k - 1}. \qquad (2)$$

This probability can be significantly higher than that for simple selection if most incoming nodes are from fewer then $k$ regions.

The cross scheme guarantees that the moving node meets an ambassador from the destination region and gets authenticated. The probability of authentication is 100 percent.

The metropolis scheme is relatively flexible. When $k \geq m$, the successful authentication probability is 100 percent as the moving node can always find ambassadors from its home and destination regions in the closest major region. When $k < m$, the probability is equal to the probability that both ambassadors from the home and destination region existing in the closest major region, which is $(\frac{k}{m})^2$.

# 6 Simulation Evaluation

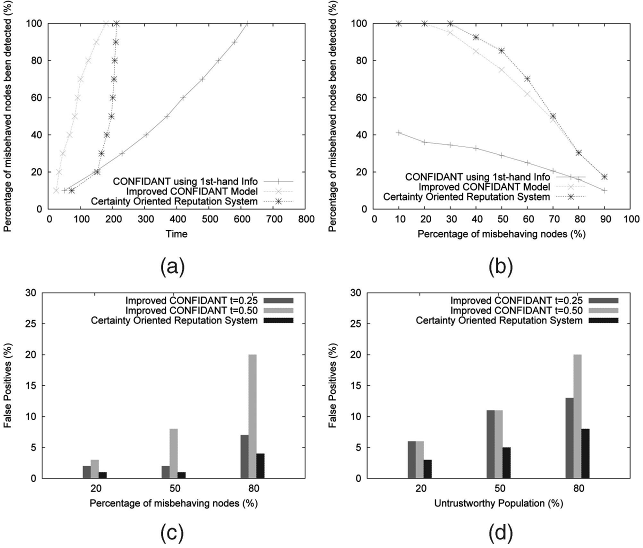
In the simulation, we aim to investigate the robustness of our certainty-oriented reputation system, and the uncertainty reduction effects of different mobility schemes.

## 6.1 Simulation Environment

We use a discrete event simulator for the simulation study. All protocols are evaluated in a network with both static nodes and mobile nodes randomly deployed in a $1{,}000 \text{ m} \times 1{,}000 \text{ m}$ area. The normal transmission range is $100 \text{ m}$. The area is uniformly divided into regions, and each region has 40 nodes, including 30 possible mobile nodes.

Nodes actual behaviors comply to the Bernoulli trial, which means that the probability that a node acts good is predetermined. If a node acts good for less than 40 percent of the interactions, we consider it a misbehaving node. The default percentage of misbehaving nodes in the network is 20 percent. Each node monitors other nodes in the same region and records the number of good or bad activities in $\alpha$ or $\beta$ toward each node. All nodes remain static and build up reputations in their home region in the initialization period. The $CH$, which is the static node with the highest reputation, is elected in each region. When the initialization period ends, moving nodes are allowed to move. All simulations are repeated 1,000 times to get reliable results. The following metrics are compared:

1. average delay or convergence time,
2. cost,
3. authentication probability, and
4. average uncertainty.



(a)

(b)

(c)

(d)

Fig. 6. Detection efficiency (a) over time, (b) with increasing percentage of misbehaving nodes; false positives when misbehaving nodes adopt (c) honest recommendation, and (d) bad mouthing and false praise.

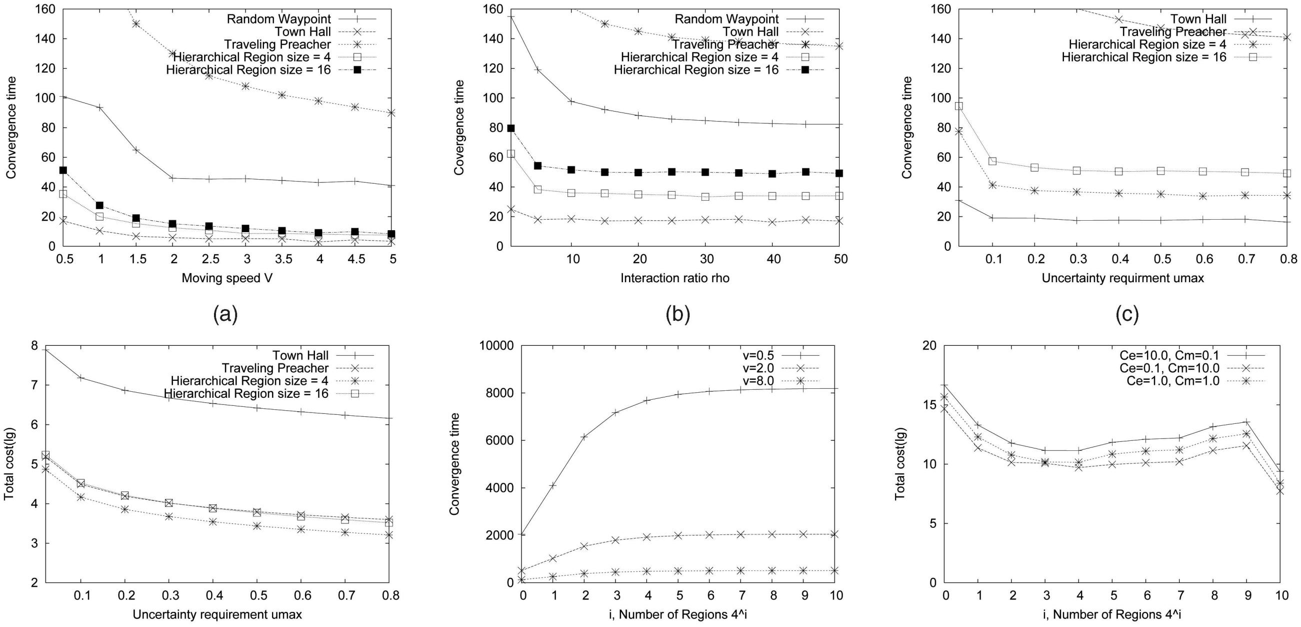
## 6.2 Simulation Results

For the first experiment, we deploy 100 nodes in a $1 \times 1$ grid. The performance metrics are the detection efficiency and the number of false positives. We compare three reputation systems. In these systems, *detected* means that a node is classified as a misbehaving node ($d \geq 0.4$) by all normal nodes. From Fig. 6a, we can see that improved CONFIDANT [5] (update threshold $t = 0.25$) is more efficient than using CONFIDANT with only first-hand information. Our reputation system (character factor $\gamma = 0.6$) is less efficient than the other two methods in the initialization time period, as the uncertainty is high and the disbelief cannot reach the threshold. But, when uncertainty is reduced and with the efficient use of second-hand information, the detection ratio goes up quickly. If we also take the number of false positives into account, as [5] produces more false positives when $t = 0.25$ in Fig. 6c, the certainty-oriented reputation system is certainly a good choice.

In Fig. 6b, the detection rate in all three reputation systems deteriorates as the percentage of misbehaving nodes increases (data are collected at time 250). That is because the faithful second recommendations in the networks decrease. However, we can also see that our certainty-oriented reputation system is more resilient toward the increasing percentage of misbehaving nodes.

Figs. 6c and 6d illustrate that the false positive will also increase in the certainty-oriented reputation system, when the percentage of misbehaving nodes increases. By comparing the two cases, we can see that the false positive will be much higher in the case that misbehaving nodes always give fake recommendations, either bad mouthing or false praise toward other nodes. Since nodes will discount others' recommendations using the $d$ and $u$ toward recommender, the certainty-oriented reputation system produces significantly less false positives compared to the CONFIDANT scheme.

Several factors strongly influence the uncertainty reduction efficiency in the proactive schemes. We use different mobility schemes and adjust the parameters in the



(a) (b) (c)

(d) (e) (f)

Fig. 7. Convergence time with different (a) moving speed $v$, (b) interaction ratio $\rho$, (c) uncertainty requirement $U_{max}$, and (d) total cost with different uncertainty requirement $U_{max}$; with different number of regions $4^i$: (e) convergence time and (f) total cost.

simulation. These parameters include: network size ($2^k \times 2^k$ grids, each grid has $n$ nodes); threshold for belief (default: $b_{min} = 0.6$), threshold for uncertainty (default: $u_{max} = 0.3$), required proportion of votes to win an election (default: $\lambda = 0.7$), interaction ratio (default: $\rho = 10$), nodes' moving speed (default: $v = 0.5$), unit cost for moving (default: $c_m = 1.0$), and unit cost for one interaction (default: $c_e = 1.0$). The observation values of this simulation are the convergence time and total cost.

For Figs. 7a, 7b, 7c, and 7d, we set up $2^3 \times 2^3$ grids, each with $n = 16$ nodes. We compare four different mobility models: the town hall model, traveling preacher model, and hierarchical scheme with region sizes 4 and 16. Random waypoint model is also considered and compared under different moving speed and interaction ratio. We draw the following conclusions from Figs. 7a, 7b, 7c, and 7d:

1. The town hall and traveling preacher models are two extreme cases. Town hall scheme has the smallest convergence time and the largest total cost, while traveling preacher scheme causes huge convergence time and has the lowest total cost.
2. Hierarchical scheme leads to shorter convergence time than under the random waypoint model in most of the simulation cases.
3. The hierarchical scheme offers a good trade-off between total cost and trust convergence time. In all the cases, the curve of the hierarchical scheme is close to the best extreme case.
4. Different region size leads to different performance in hierarchical scheme.

In this simulation experiment, hierarchical scheme with region size 4 outperforms hierarchical scheme with region size 16 in both convergence time and total cost.

We use a network size $2^{10} \times 2^{10}$ grids in Figs. 7e and 7f and vary the number of regions from $4^0$ to $4^{10}$, where $i = 0$ represents the extension of the town hall model. The environmental variable $v$ and the weight between $c_e/c_m$ have a strong influence on the slope of each curve. Therefore, the application objectives (cost or time sensitive) together with $v$ and $c_e/c_m$ decide the optimal number of regions.

In Figs. 8a, 8b, and 8c, the reputation threshold for the ambassador is $b \geq 0.7$ and the number of ambassadors is fixed to $k = 15$. We adjust $n$ which decides the number of regions ($n \times n$) to compare the schemes, $n$ varies in $[5, 15]$. In Fig. 8a, the cost is defined as the total travel distance of the ambassadors from a single region. In the metropolis and cross scheme, ambassadors need to move to designated regions, which makes the cost higher. The cost in the cross scheme appears to increase linearly since the ambassadors' average moving distance remains the same and the number of ambassadors from each region is $2 \cdot n$. Comparatively, the metropolis scheme is preferable as the cost of this scheme only depends on the number of major regions $m$. In Fig. 8b, the speed $v$ of moving node equals $1.0\ \mathrm{m/s}$. One thousand source and destination pairs are randomly generated, and the sum of the moving and waiting delay is collected. The delay of the cross and metropolis schemes are higher since the moving nodes move to the closet joint or major regions instead of directly to the destination.

In Fig. 8c, the probability of authentication is much higher in the case of cross or metropolis scheme. It makes these schemes preferable in applications where additional cost and delay aren't the major concern, and lower uncertainty for newly incoming nodes is one of the main goals. Considering the results in Fig. 8 synthetically, the metropolis scheme seems to be more flexible in terms of the trade-off among delay, cost, authentication probability, and uncertainty.

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

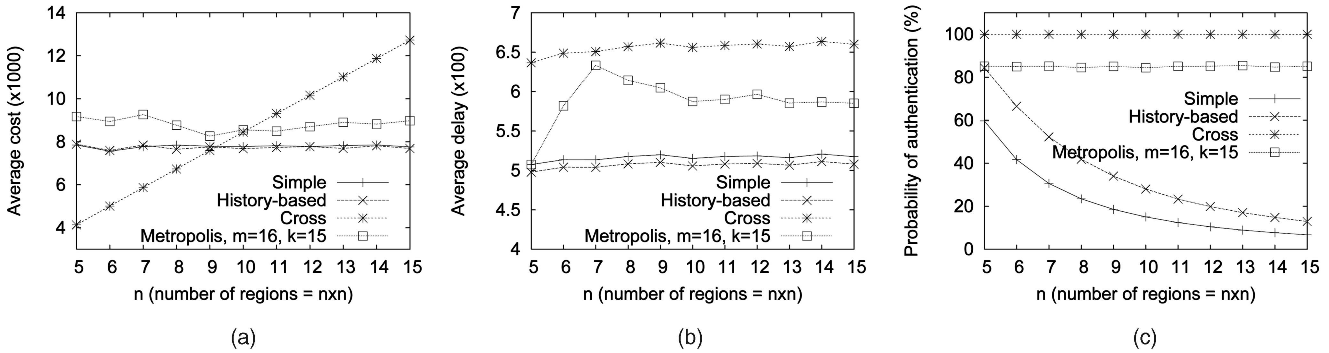


Fig. 8. Reactive schemes comparison with different region sizes. (a) Cost. (b) Delay. (c) Authentication probability.

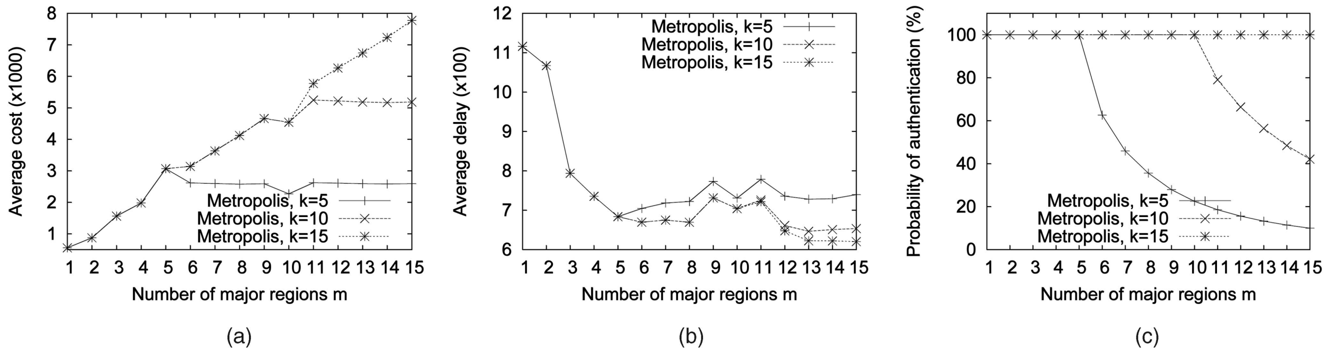


Fig. 9. Metropolis scheme comparison with different number of major regions. (a) Cost. (b) Delay. (c) Authentication probability.

Therefore, the simulations in Fig. 9 use similar settings as in Fig. 8. We then adjust $m$ and show the results of different combinations of $k$ and $m$. The number of regions is fixed to $n^2 = 100$. The results in Fig. 9 can be summarized as: 1) Increasing $m$ can significantly reduce delay when the number of regions $n^2 >> m$. 2) $k$ can be adjusted to achieve fine-grained trade-off between cost, delay, and authentication probability. 3) $k$ should be selected closer to $m$. Otherwise, the probability of authentication drops very fast as $m$ increases.

In Figs. 10a and 10b, the average uncertainty $u$ is calculated between each pair of source and destination nodes. Network size is $8 \times 8$. Each node's behavior is consistent in the simulations, including the misbehaving nodes. The average uncertainty increases due to the increasing percentage of misbehaving nodes under all mobility schemes. The uncertainty reduction effects of the mobility schemes deteriorate. However, the average uncertainty increases because a regular node will consider a misbehaving node's recommendation as highly uncertain, which indicates that the false-praise and bad-mouthing attacks are restricted.

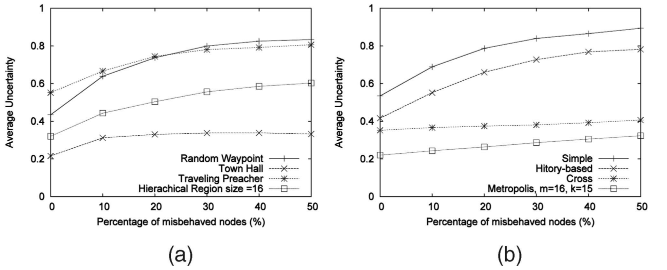


Fig. 10. Uncertainty comparison among (a) proactive schemes and (b) reactive schemes with a different percentage of misbehaving nodes.

Simulation results can be summarized as follows:

1. Uncertainty is one important metric in MANETs. Certainty-oriented reputation systems can achieve good detection rates while keeping the false positive rate at a low level.
2. With proactive or reactive schemes, we can efficiently disseminate trust and reduce uncertainty by exploiting nodes' movement. All the schemes illustrate the uncertainty reduction effect with the assistance of mobility.
3. Different mobility schemes provide different tradeoffs between delay, cost, and uncertainty. The controlled mobility-based schemes appear to offer better performance in terms of uncertainty reduction.
4. The performance of the certainty-oriented reputation system deteriorates and the average uncertainty increases as the percentage of misbehaving nodes increasing. However, our reputation system still appears to be more resilient than CONFIDANT.

## 7 Conclusion

Uncertainty is a core dimension of trust that reflects a node's confidence in the sufficiency of past experiences. It deeply impacts nodes' anticipations and decisions. In this paper, we present a certainty-oriented reputation system that emphasizes the relationship among uncertainty, observation, and recommendation. We propose schemes based on the reputation system, which use mobility as an asset to reduce uncertainty in far-flung nodes and reduce the overall

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.

uncertainty in the network proactively. We provide methods to allow mobile nodes to carry and disseminate their reputations reactively. We also design one proactive scheme and one reactive scheme that can offer flexibility for users to achieve application specific goals. By selecting different mobility patterns and adjusting controlled parameters, different trade-offs between delay, cost, and uncertainty can be realized. We give both theoretical proof and simulation results to illustrate that our approach strikes an acceptable balance between the cost and convergence time. In the future, we will further study the impact of nodes' behavior inconsistency on our reputation system and conduct simulation and analytical research to study the effect of the aging factor under different mobility schemes.

## ACKNOWLEDGMENTS

This work was supported in part by US National Science Foundation grants CNS 0422762, CNS 0434533, CNS 0531410, and CNS 0626240.

## REFERENCES

[1] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," *Proc. Int'l Conf. World Wide Web,* 2003.

[2] A. Josang, "An Algebra for Assessing Trust in Certification Chains," *Proc. Network and Distributed Systems Security Symp. (NDSS '99),* 1999.

[3] A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems,* vol. 43, no. 2, pp. 618-644, 2007.

[4] W. Zhang, S. Das, and Y. Liu, "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks," *Proc. Ann. IEEE Comm. Soc. Sensor and Ad Hoc Comm. and Networks,* 2006.

[5] S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," *Proc. Int'l Symp. Mobile Ad Hoc Networking and Computing,* 2002.

[6] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security,* 2002.

[7] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Technical Report cs.NI/0307012, Stanford Univ., 2003.

[8] S. Buchegger and J. Boudec, "A Robust Reputation System for P2P and Mobile Ad-Hoc Networks," *Proc. Workshop Economics of Peer-to-Peer Systems (P2PEcon),* 2004.

[9] M. Carbone, M. Nielsen, and V. Sassone, "A Formal Model for Trust in Dynamic Networks," *Proc. IEEE Int'l Conf. Software Eng. and Formal Methods (SEFM '03),* 2003.

[10] A. Josang, S. Marsh, and S. Pope, "Exploring Different Types of Trust Propagation," *Proc. Int'l Conf. Trust Management,* 2006.

[11] A. Josang and S. Pope, "Normalising the Consensus Operator for Belief Fusion," *Proc. Int'l Conf. Information Processing and Management of Uncertainty,* July 2006.

[12] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *Wireless Comm. and Mobile Computing,* vol. 2, no. 5, pp. 483-502, 2002.

[13] J. Wu and F. Dai, "Mobility Management and Its Applications in Efficient Broadcasting in Mobile Ad Hoc Networks," *Proc. IEEE INFOCOM,* 2004.

[14] J. Wu, S. Yang, and F. Dai, "Logarithmic Store-Carry-Forward Routing in Mobile Ad Hoc Networks," *IEEE Trans. Parallel and Distributed Systems,* vol. 18, no. 6, pp. 735-748, June 2007.

[15] S. Capkun, M. Cagalj, and M. Srivastava, "Securing Localization with Hidden and Mobile Base Stations," *Proc. IEEE INFOCOM,* 2006.

[16] S. Capkun, J. Hubaux, and L. Buttyán, "Mobility Helps Security in Ad Hoc Networks," *Proc. ACM MobiHoc,* June 2003.

[17] W. Zhang, H. Song, S. Zhu, and G. Cao, "Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks," *Proc. ACM MobiHoc,* 2005.

[18] F. Li and J. Wu, "Mobility Reduces Uncertainty in MANETs," *Proc. IEEE INFOCOM,* 2007.

[19] W. Zhao, M. Ammar, and E. Zegura, "A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks," *Proc. MobiHoc,* 2004.

[20] M. Grossglauser and D. Tse, "Mobility Increases the Capacity of Ad-Hoc Wireless Networks," *Proc. IEEE INFOCOM,* 2001.

[21] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility Improves Coverage of Sensor Networks," *Proc. Int'l Symp. Mobile Ad Hoc Networking and Computing,* 2005.

[22] A. Vahdat and D. Becker, "Epidemic Routing for Partially-Connected Ad Hoc Networks," technical report, Duke Univ., 2000.

[23] W. Zhao, M. Ammar, and E. Zegura, "Controlling the Mobility of Multiple Data Transport Ferries in a Delay-Tolerant Network," *Proc. IEEE INFOCOM,* 2005.

[24] J. Newsome, E. Shi, D.X. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," *Proc. Int'l Symp. Information Processing in Sensor Networks,* 2004.

[25] J. Brainard, A. Juels, R. Rivest, M. Szydlo, and M. Yung, "Fourth Factor Authentication: Somebody You Know," *Proc. Conf. Computer and Comm. Security,* 2006.

[26] T. Cover and J. Thomas, *Elements of Information Theory.* Wiley Interscience, 1991.

[27] D. Zhou and J. Wu, "Survivable Multi-Level Ad-Hoc Group Operations," *Proc. Int'l Workshop Mobile and Wireless Networks,* 2003.

[28] J. Yu and P. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks," *IEEE Comm. Surveys and Tutorials,* vol. 7, no. 1, pp. 32-48, 2005.

[29] J. Wu, F. Dai, M. Gao, and I. Stojmenovic, "On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks," *J. Comm. and Networks,* vol. 4, no. 1, pp. 59-70, 2002.

**Feng Li** received the PhD degree in computer science from Florida Atlantic University in August 2009. His PhD advisor was Professor Jie Wu. He joined the Department of Computer, Information, and Leadership Technology at Indiana University-Purdue University Indianapolis (IUPUI) as an assistant professor in August 2009. His research interests include the areas of wireless networks and mobile computing, security, and trust management. He has published more than 20 papers in conferences and journals. He is a member of the IEEE. More information about his research can be found at http://www.engr.iupui.edu/~fengli/contact.html.

**Jie Wu** is the chairman and a professor in the Department of Computer and Information Sciences, Temple University. He was a program director at the US National Science Foundation. His research interests include the areas of wireless networks and mobile computing, routing protocols, fault-tolerant computing, and interconnection networks. He has published more than 500 papers in various journals and conference proceedings. He serves on the editorial board of the *IEEE Transactions on Mobile Computing*. He was also the general cochair for IEEE MASS 2006, IEEE IPDPS 2008, and DCOSS 2009. He has served as an IEEE Computer Society distinguished visitor and is the chairman of the IEEE Technical Committee on Distributed Processing (TCDP). He is a fellow of the IEEE. More information about his research can be found at http://www.cis.temple.edu/~wu.

▷ **For more information on this or any other computing topic, please visit our Digital Library at** www.computer.org/publications/dlib.

Authorized licensed use limited to: Temple University. Downloaded on August 11,2010 at 15:45:59 UTC from IEEE Xplore. Restrictions apply.