Reputation Propagation and Agreement in Mobile Ad-Hoc Networks

Yanbin Liu
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712
Email: ybliu@cs.utexas.edu

Yang Richard Yang
Computer Science Department
Yale University
New Haven, CT 06520
Email: yry@cs.yale.edu

Abstract— **Several reputation systems have been proposed for mobile ad-hoc networks in order to stimulate cooperation among mobile nodes. However, whether or not the mobile nodes will agree on the reputation of other nodes is not studied. In this paper, we present a formal specification and analysis of a general class of mechanisms to locally update the reputation of mobile nodes. Given an initial assessment of the reputation of other mobile nodes, we formally show that under mild conditions, the mobile nodes will achieve reputation agreement. Our analysis captures reputation propagation using graph connectivity and makes use of a recent theoretical result [1]. We also evaluate the convergence speed of two reputation propagation mechanisms through simulations. Our simulations show that the speed of reputation propagation is an important factor for the convergence speed of reputation agreement.**

I. Introduction

In recent years, mobile ad-hoc networks have received much attention due to their potential applications and the proliferation of mobile devices [2], [3]. Specifically, mobile ad-hoc networks refer to wireless multi-hop networks formed by a set of mobile nodes without relying on a preexisting infrastructure. In order to make an ad-hoc network functional, the nodes are assumed to follow a self-organizing protocol, and the intermediate nodes are expected to relay messages between two distant nodes. Recent evaluations have shown that ad-hoc networks not only are flexible and robust, but also can have good performance in terms of throughput, delay and power efficiency [4].

So far, applications of mobile ad-hoc networks have been envisioned mainly for emergency and military situations. In such applications, all of the nodes in the network belong to a single authority and therefore have a common objective. As a result, cooperation among the nodes can be assumed. However, as observed by several authors [5], [6], [7], [8], [9], [10], [11], it may soon be possible to deploy ad-hoc networks for civilian applications as well. In such emerging civilian applications, the nodes typically do not belong to a single authority. Consequently, cooperation behaviors such as forwarding each other's messages cannot be directly assumed.

One possibility to stimulate cooperation is to use credit (or virtual currency). Buttyan and Hubaux proposed a nice solution of this type in [6], and then presented an improved result based on credit counters in [7]. For both proposals, a node receives one unit of credit for forwarding a message of another node, and such credits are deducted from the sender (or the destination). One potential drawback of these two approaches, however, is that they require a tamper-proof hardware at each node so that the correct amount of credit is added or deducted from the node. As a result of this requirement, although both proposals are interesting, they may not find wide-spread acceptance. In [12], applying game-theoretic design, we proposed Sprite, a simple, cheat-proof, credit-based system for mobile ad-hoc networks with selfish nodes. One feature of this system is that it does not need any tamper-proof hardware at any node. One potential limitation of this approach, however, is that it requires a credit clearance system; therefore, the system may not be applicable in some scenarios.

Another possibility to stimulate cooperation is to use a reputation system [5], [8], [9], [11], [13]. For example, in [5], Marti et al. proposed a reputation system for ad-hoc networks. In their system, a node monitors the transmission of a neighbor to make sure that the neighbor forwards others' traffic. If the neighbor does not forward others' traffic, it is considered as uncooperative, and this uncooperative reputation is propagated throughout the network. In [8], [9], Buchegger and Le Boudec proposed and evaluated their CONFIDENT protocol, which detects and isolates misbehaving nodes. In [11], [13], Michiardi and Molva specified a mechanism to maintain the reputation of mobile nodes. Although empirical evaluations have shown that the above systems can identify misbehaving nodes and improve the performance of an ad-hoc network, one important missing component is a formal analysis of the properties of the reputation systems.

The major objective of this paper, therefore, is a first attempt to formally analyze the properties of the mechanisms that mobile nodes use to update and agree on the reputation of other mobile nodes. In general, mobile nodes will evaluate the reputation of other nodes through both direct observations and reputation propagation among the nodes. As a first step, the focus of this paper is on reputation propagation, which is one of the key components; the investigation of both direct observations and reputation propagation will be presented in another paper under preparation.

Specifically, the problem we study in this paper is the following: given an initial assessment of the reputation of other mobile nodes, can the mobile nodes agree on the reputation of other mobile nodes using only local propagation, without any special nodes?

For a general class of mechanisms, where two mobile nodes exchange their states when they become neighbors and then

0-7803-7700-1/03/$17.00 (C) 2003 IEEE

each updates its state as a weighted average of the received state and its own state, we show that the mobile nodes can agree on the reputation of other nodes, if the reputation can propagate throughout the network often enough. Our analysis captures reputation propagation as graph connectivity and uses a recent nice theoretical result by Jadbabaie, Lin, and Morse [1]. As far as we know, this is the first formal approach to evaluate the properties of reputation propagation.

We also use simulations to investigate the convergence speed of two reputation propagation mechanisms. Our simulations show that the speed of reputation propagation is an important factor for the convergence speed of reputation agreement. Generally, the higher the propagation speed, the faster the convergence.

The rest of this paper is organized as follows. In Section II, we discuss related work. In Section III, we model reputation propagation as graph connectivities and prove properties. In Section IV, we present simulation evaluations. Our conclusion and future work are in Section V.

II. Related Work

Two classes of work are closely related to this paper: previous proposals of reputation systems, and previous studies on the emerging behavior of dynamics systems.

A. Reputation systems

Reputation systems are proposed as a mechanism to deal with misbehaving mobile nodes. For an overview on how to deal with uncooperative nodes, we refer the readers to [10]. So far, three reputation systems have been proposed. In [5], Marti et al. considered uncooperative nodes in general, including selfish and malicious nodes. In order to cope with this problem, they proposed two tools: a watchdog, which identifies misbehaving nodes, and a pathrater, which selects routes that avoid the identified nodes. Their simulations showed that by using these two tools, their system can maintain the total throughput of an ad hoc network at an acceptable level even with a large percentage of misbehaving nodes. As part of the Terminodes project [14], [15], [8], [9], Buchegger and Le Boudec proposed and evaluated their CONFIDENT protocol, which detects and isolates misbehaving nodes. In [11], [13], Michiardi and Molva specified their reputation system. They considered several functions such as routing and packet forwarding.

Some distributed trust management systems can also be considered as general reputation propagation systems [16]. For example, in PGP [17], the trust level (a.k.a. reputation) of a public key will depend on the trust levels of the other keys that sign the key.

Reputation systems have also been proposed in other contexts, *e.g.*, [18], [19], [20]. For example, Zacharia et al. [18], [19] considered reputation systems in the context of on-line communities. However, as we discussed in Section I, although there are some studies on the reputation systems using game theory (*e.g.*, [11], [20]), these previous approaches do not formally analyze the convergence properties of their systems.

B. Emerging behavior of dynamic systems

Emerging behavior such as motion coordination of dynamic systems is an active research area. The formalization and proof techniques of this paper are from [1], which is inspired by [21], in the context of distributed motion coordination. The solution techniques of [1] is based on previous well-known results [22] in non-negative matrices [23].

III. Modeling Reputation Propagation

Formally, we consider whether or not mobile nodes will agree on the reputation of other nodes, given their initial assessment of others' reputation, using local update rules. We call this problem the reputation agreement problem (RAP).

A. Model of reputation propagation

We assume that there is a total of n mobile nodes. Each node has an assessment of the reputation of another node. Note that it is straightforward to extend this paper to the case where each node has an assessment of the reputation of just a subset or even a different set of other nodes.

We assume that each node i uses a number to represent the reputation of another node. For example, the reputation may represent the cooperative level of the node. Node i can use the value of the reputation of a node to make its local decisions. For example, node i may only forward packets for a node with a reputation that is higher than a threshold; or node i may forward the packets of a node with a probability, where the forwarding probability is proportional to the reputation of the source. Since our objective is to study whether or not the nodes will achieve reputation agreement, in this paper, we consider the general framework and do not specify the exact meaning of the value of reputation.

To model reputation propagation, we adopt a discrete time model.[1] Let $r_{ji}(t)$ denote the current reputation of node j at node i at time t. To avoid self loop, we ignore r_{ii}, namely the reputation of node i at itself. Therefore, the local state of node i at time t will be the $n-1$ dimension vector $[r_{1,i}(t), \ldots, r_{i-1,i}(t), r_{i+1,i}(t), \ldots, r_{ni}(t)]$.

When mobile nodes i and j become close enough and therefore can communicate with each other, if node i *trusts* node j, it will send its state vector to node j. We call j a *neighbor* of i. In terms of implementation, node i can broadcast its state vector; therefore any node in its neighborhood can receive the vector. Privacy can be achieved by using a secure multicast scheme among those nodes who would share states with node i [24], [25]. Node i can also unicast the state vector to node j, using their individual secret channel. One advantage of the unicast scheme is that node i does not need to send to j its value of r_{ji}, which is the reputation of j at i.

Let $N_i(t)$ denote the neighbors of node i at time t. For ease of notation, assume that $i \in N_i(t)$. Consider a general class of distributed rules where node i updates $r_{ji}(t+1)$, namely the

[1] For techniques to map from a continuous system to discrete model, see [1].

new reputation of node j at node i, as a weighted sum of its own and its neighbors' states about j. Specifically, we have:

$$r_{ji}(t+1) = \sum_{k \in N_i(t)} w_{j,ik}(t) r_{jk}(t), \quad (1)$$

where $w_{j,ik}(t) > 0$ is the weight that node i gives to node k for its input on node j, if $k \in N_i(t)$. Note that for generality, $w_{j,ik}(t)$ can depend on both the state of and the inputs to node i. For consistency of notation, we let $w_{j,ik}(t) = 0$, if $k \notin N_i(t)$.

The model above is very general and allow for many possibilities. We consider three examples.

Example 1: Assume that node i receives the state vector of node k. Then node i can update the reputation of j, where $j \neq$ i or k. Node i updates the reputation of j as the average of the reputation of j at k and that at itself. For this example, we have that $w_{j,ii} = w_{j,ik} = \frac{1}{2}$, and 0 otherwise.

Example 2: Assume that node i has more memory and saves the state vectors received during a fixed time period. Then node i updates its state about j as the average of its own and those received from others. Suppose node i receives reputation about j from $n_{ij}(t)$ other nodes, we have that $w_{j,ik} = \frac{1}{n_{ij}(t)+1}$, where k is equal to i or is one of the $n_{ij}(t)$ neighbors that send i the reputation of j during the period.

Example 3: Extending Example 2 above, we can assume that node i saves the state vectors received during a fixed time period. When calculating its new state vector, node i can give the neighbor that has a higher reputation a higher weight. In particular, the state vector of neighbor k may have a relative weight that is proportional to $r_{ki}(t)$. That is, if neighbor k has a higher reputation at node i, its state vector will be weighted higher in node i's update. It is obvious that this update rule is more robust to selfish and malicious nodes.

Let $\mathbf{r_j}(t)$ denote the column vector that is the reputation of node j at the other $n-1$ nodes:

$$\mathbf{r_j}(t) \triangleq \begin{pmatrix} r_{j,1}(t) \\ \vdots \\ r_{j,j-1}(t) \\ r_{j,j+1}(t) \\ \vdots \\ r_{j,n}(t) \end{pmatrix}.$$

Let $\mathbf{w_j}(t)$ denote the weight matrix that others use to calculate the new reputation of j at time t. We have

$$\mathbf{w_j}(t) \triangleq \begin{pmatrix} w_{j,11} & \cdots & w_{j,1k} & \cdots & w_{j,1n} \\ \vdots & & & & \\ w_{j,i1} & \cdots & w_{j,ik} & \cdots & w_{j,in} \\ \vdots & & & & \\ w_{j,n1} & \cdots & w_{j,nk} & \cdots & w_{j,nn} \end{pmatrix}.$$

Writing in matrix form for how the nodes update the reputation of node j at the other nodes, we have

$$\mathbf{r_j}(t+1) = \mathbf{w_j}(t)\mathbf{r_j}(t). \quad (2)$$

Writing in matrix format for all nodes, we have

$$\mathbf{r}(t) \triangleq \begin{pmatrix} \mathbf{r_1}(t) \\ \vdots \\ \mathbf{r_j}(t) \\ \vdots \\ \mathbf{r_n}(t) \end{pmatrix},$$

and

$$\mathbf{w}(t) \triangleq \begin{pmatrix} \mathbf{w_1}(t) & \cdots & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & & & & \\ \mathbf{0} & \cdots & \mathbf{w_j}(t) & \cdots & \mathbf{0} \\ \vdots & & & & \\ \mathbf{0} & \cdots & \mathbf{0} & \cdots & \mathbf{w_n}(t) \end{pmatrix},$$

where $\mathbf{0}$ is an $(n-1) \times (n-1)$ matrix with 0 at all entries.

Given the above definitions, we can write the global system update as

$$\mathbf{r}(t+1) = \mathbf{w}(t)\mathbf{r}(t). \quad (3)$$

B. Reputation agreement

In order for the nodes to agree on the reputation of a node, we need to investigate the convergence of the global state vector. Specifically, we need to investigate whether or not the matrix product $\mathbf{w}(t)\mathbf{w}(t-1)\cdots\mathbf{w}(0)$ will converge.

Since the global update in Equation (3) can be decomposed as local update for each node as in Equation (2), in the sequel we only consider the convergence of the reputation of a given node j.

Formally, we need to verify whether or not

$$\lim_{t \to \infty} \mathbf{r_j}(t) = r_j^{ss} \mathbf{1}, \quad (4)$$

where r_j^{ss} is a number (the converged reputation of node j at the other nodes), and $\mathbf{1}$ is the all 1 vector $[1, 1, \cdots, 1]'$ of $n-1$ dimensions. In words, we need to investigate whether or not node j has the same reputation value at all other nodes.

Obviously, whether or not the nodes can achieve reputation agreement will depend on how each node updates its state and how states are propagated among the nodes.

We first consider how each node updates its state. From Equation (2), such update is captured by the relative weights. In this paper, we assume that $\sum_{k=1}^{n} w_{j,ik}(t) = 1$. Otherwise, if $\sum_{k=1}^{n} w_{j,ik}(t) > 1$, the system will diverge to infinity; if $\sum_{k=1}^{n} w_{j,ik}(t) < 1$, the system will goto 0. Since $\sum_{k=1}^{n} w_{j,ik}(t) = 1$, the matrix $\mathbf{w_j}(t)$ is called a stochastic matrix [26]. We also assume that each node i will always give its own entry a positive weight, *i.e.*, $w_{j,ii} > 0$ for any j. This requirement is intuitive. Furthermore, since $w_{j,ii} > 0$ for any j, the diagonal entries of the stochastic matrix $\mathbf{w_j}(t)$ are all positive, and therefore the matrix is aperiodic [27].

We next consider how reputation is propagated among the nodes. To model reputation propagation, we adopt a graph-theoretic approach.

Let $G_j(t)$ denote the directed graph representing information flow about node j at time t. The nodes of this graph are

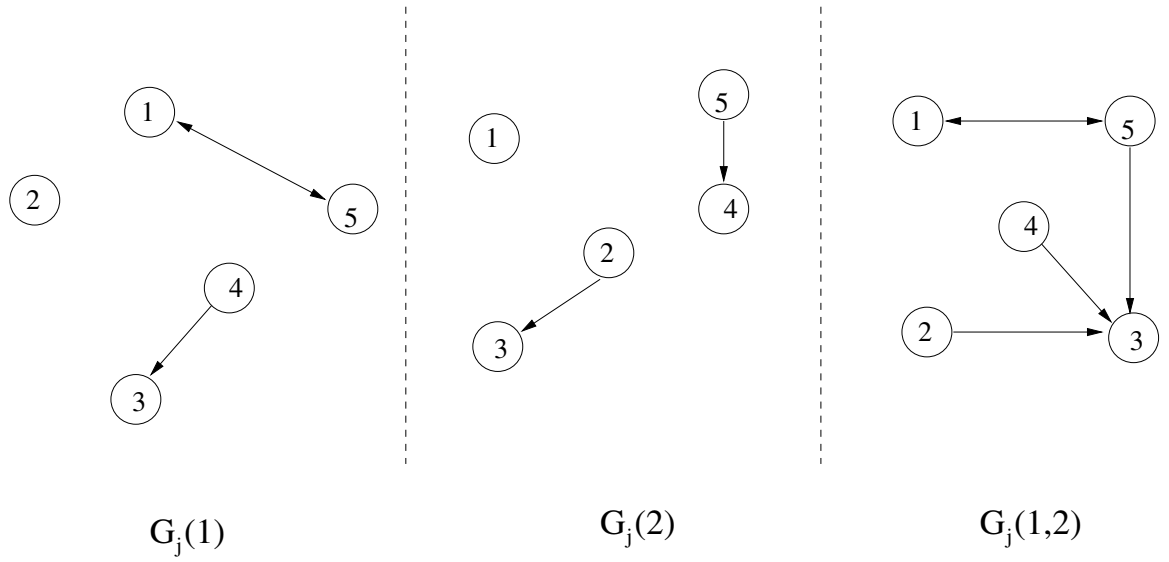

Fig. 1. Illustration of propagation graphs and super graphs.

the n mobile nodes. If node i uses the state of node k at time t to update its state about node j, we have a directed edge from node k to node i in graph $G_j(t)$, indicating that information flows from node k to node i.

Let $G_j(t_1, t_2)$ denote the super graph which is the union of graphs from $G_j(t_1)$ to $G_j(t_2)$, where $t_1 < t_2$. We say that $G_j(t_1, t_2)$ is strongly connected if there is a path from any node i to another node k. Figure 1 illustrates graphs and super graphs with an example.

Given the above formulation, we can prove the following theorem:

Theorem 1 (Reputation Agreement): Assume that there is finite number of possible values for each entry of $\mathbf{w_j}$, which can be achieved by quantization. If for any t_1, there is $t_2 \geq t_1$ so that the super graph $G_j(t_1, t_2)$ is strongly connected, then the system converges, *i.e.*,

$$\lim_{t\to\infty} \mathbf{r_j}(t) = r_j^{ss}\mathbf{1}.$$

The proof of Theorem 1 can be derived as that in [1], which is in the context of emerging behavior. The proof utilizes the following classic result by Wolfowitz [22].

Theorem 2 (Wolfowitz): Let $M_1, M_2, \ldots, M_m$ be a finite set of ergodic matrices with the property that for each sequence $M_{i_1}, M_{i_2}, \ldots, M_{i_j}$ of positive length, the matrix product $M_{i_j} M_{i_{j-1}} \cdots M_{i_1}$ is ergodic. Then for each infinite sequence $M_{i_1}, M_{i_2}, \ldots$, there exists a row vector $\mathbf{c}$ such that

$$\lim_{j\to\infty} M_{i_j} M_{i_{j-1}} \cdots M_{i_1} = \mathbf{1c}.$$

Intuitively, the condition of Theorem 1 is that if the states of the nodes are propagated to other nodes often enough, the nodes will achieve reputation agreement. The requirement for strong connectivity for a directed graph is intuitive because all of the nodes need to share information in order to achieve agreement. Furthermore, since each node will use its own state in its local update, the system will not be periodical. As a result, the reputation will spread out to all of the nodes.

IV. Simulation Evaluations

We have proved that the nodes will agree on the reputation of other nodes. In this section, we evaluate the convergence speed through simulations.

In all our simulations, the nodes are in an area of 400 by 400 units. The radius of communication neighborhood is 30 units. As for movement, a node randomly chooses a destination and moves in a straight line toward it at a speed uniformly distributed between 0 and some maximum speed. This is called the *random waypoint model*. We limit the maximum speed of a node to 2 units/second. During the movement of a node, if it moves into the communication range of another node, the two nodes may exchange state if they trust each other.

In our simulations, the initial assessments of a node about the reputation of other nodes are uniformly chosen from $[0, 1]$. To measure the convergence of reputation about a node j, we define

$$v_j(t) = \sum_{i\neq j} (r_{ji}(t) - m_j(t))^2,$$

where $m_j(t)$ is the average reputation of node j at time t, *i.e.*,

$$m_j(t) = \frac{1}{n-1} \sum_{i\neq j} (r_{ji}(t)).$$

Note that $v_j(t) = 0$ when node j has the same reputation at all the other nodes.

We first evaluate the convergence speed when the nodes use the rule of Example 1. Note that this is a very simple model and nodes do not need any memory.

Figure 2 shows the result. The x-axis of Figure 2 is time and the y-axis is the value of v at time t. We observe that regardless of the number of nodes, the system converges.

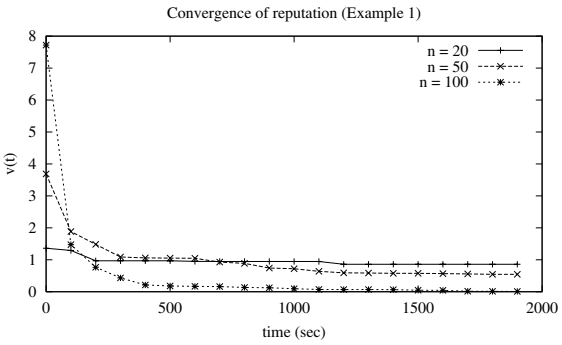

Fig. 2. Convergence of reputation when nodes use the rule in Example 1.

One further interesting observation is that although more nodes (*i.e.*, higher n) increase diversity at the beginning, as indicated by the high value of v at the beginning, the convergence of a network with more nodes is actually much faster. To understand the phenomenon, we can estimate the connectivity of the propagation graphs. Since each node has a coverage area of 2800 $(= 3.14 * 30 * 30)$ square units and the total area of the system is $160,000$ square units, when there are 20 nodes, if we assume that the nodes are randomly distributed in the area, there are about 0.35 nodes within the radius of each node; thus, the graph is not likely to be connected. When there are 50 nodes, there are about 0.88 nodes within the radius of each node; thus the connectivity of the graph increases. With 100 nodes, there are about 1.7 nodes within the radius of each node, and the graph is highly likely to be connected. In other words, although more nodes bring in more opinions, since the network are much more connected, the convergence is much faster. In fact, this phenomenon is similar to the question of connectivity in the context of wireless capacity [28], [29].

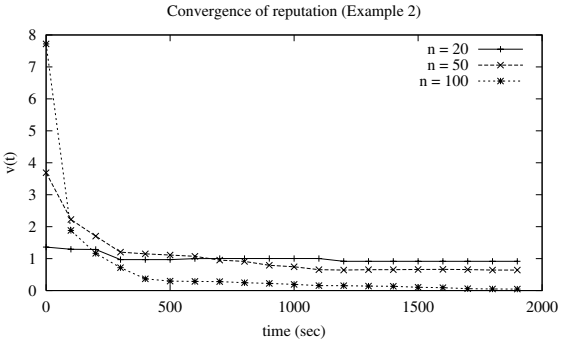

Fig. 3. Convergence of reputation when nodes use the rule in Example 2.

We next evaluate the convergence speed when the nodes use the rule as we discussed in Example 2. Note that in this case the nodes will keep track of received states and then do a batch update periodically.

Figure 3 shows the result. In this figure, each node will hold the received states for 10 seconds. Similar to Figure 2, we observe that regardless of the number of nodes, the system converges. Again, as the number of nodes increases, the convergence is faster.

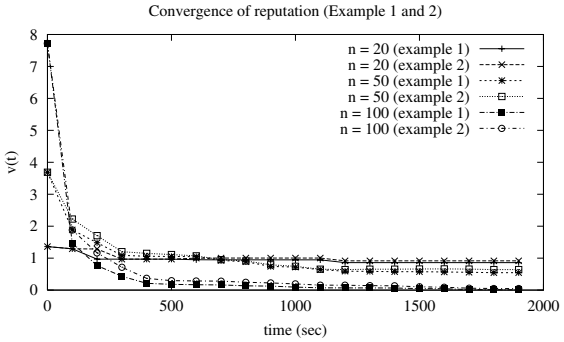

Fig. 4. Comparison of convergence speed when nodes use the rule in Example 1 and that in Example 2.

Figure 4 plots the results of previous two figures. We observe that although the rule in Example 2 uses more memory, it actually converges slower. This result may be somewhat counter intuitive at the beginning. The key to an understanding of this phenomenon is that by holding the update, the rule of Example 2 slows down the propagation of reputation and therefore slows down the system. In other words, the rule in Example 1 uses an update rule that is of the Gauss-Seidel type, and therefore can have a faster convergence speed [30].

V. Conclusion and Future Work

In this paper, we showed that if reputation propagates among mobile nodes often enough and the nodes always use their own states as part of system update, the mobile nodes will achieve reputation agreement through local reputation propagation, given an initial assessment of the reputation of other mobile nodes. Using the result of [1], our analysis models local updates as matrix operation and uses graph connectivity to model reputation propagation. Our simulations show that the speed of reputation propagation is an important factor for the convergence speed of reputation agreement. Generally, the higher the propagation speed, the faster the convergence.

We are currently extending the work in several directions. First, in this paper, for the proofs of convergence, we assume that the mobile nodes will send its state vector to other nodes truthfully. When a mobile node is malicious, the problem becomes the Byzantine Agreement Problem (*e.g.*, see [31], [32]), which has already been extensively studied in distributed computing. Our initial assessment shows that update rules such as those in Example 3 can also resist malicious attacks; we leave detailed security analysis as a future work.

Second, we will allow a node to update the reputation of a node through both reputation propagation and direct observations. Our preliminary results show that under a general class of update mechanisms, the reputation of a node can converge to its *inherent* property. The results of this investigation will be reported in a separate paper under preparation.

Third, although the reputation update mechanisms considered in this paper is already very general, what it provides

is only a sufficient condition. A necessary condition for convergence will be an interesting problem and we are currently investigating the issue.

Fourth, we are also considering to extend this analysis to other contexts where reputation agreement plays a role. For example, an interesting scenario will be the propagation of reputation in academia, where each researcher learns the reputation of another researcher.

ACKNOWLEDGMENTS

The idea of applying the results from [1] to reputation agreement was first suggested by Ali Jadbabaie, Steve Morse, and Edmund Yeh. The authors would like to thank Steve Morse, Ali Jadbabaie, Edmund Yeh, and Jie Archer Lin for helpful discussions. Yang Richard Yang was supported in part by NSF grant ANI-0207399.

REFERENCES

[1] A. Jadbabaie, J. Lin, and A. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," in *IEEE Control and Decision Conference*, 2001.

[2] C. Perkins, *Ad Hoc Networking*. Addison-Wesley, 2000.

[3] C.-K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems*. Prentice Hall PTR, 2001.

[4] J. Hershberger and S. Suri, "Vickrey prices and shortest paths: What is an edge worth?" in *Proceedings of the 42nd Annual Symposium on Foudations of Computer Science 2001*, Las Vegas, Nevada, Oct. 2001, pp. 129–140. [Online]. Available: http://www.cs.berkeley.edu/~christos/games/readings/vickreypaths.ps

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of The Sixth International Conference on Mobile Computing and Networking 2000*, Boston, MA, Aug. 2000. [Online]. Available: http://gunpowder.stanford.edu/~laik/projects/adhoc/mitigating.pdf

[6] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Boston, MA, August 2000. [Online]. Available: http://icawww.epfl.ch/Publications/Buttyan/ButtyanH00.ps

[7] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *ACM Journal for Mobile Networks (MONET), special issue on Mobile Ad Hoc Networks*, summer 2002. [Online]. Available: http://lcawww.epfl.ch/Publications/Buttyan/TR01"¨046.ps

[8] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, 2002.

[9] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks," in *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*. IEEE, June 2002. [Online]. Available: http://lcawww.epfl.ch/Publications/LeBoudec/BucheggerL02.pdf

[10] S. Buchegger and J. Y. L. Boudec, "Cooperative routing in mobile ad-hoc networks: Current efforts against malice and selfishness," in *Proceedings of Mobile Internet Workshop. Informatik 2002.*, Dortmund, Germany, October 2002. [Online]. Available: http://lcawww.epfl.ch/Publications/Buchegger/BucheggerL02C.pdf

[11] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc network," in *Communications and Multimedia Security Conference (CMS) 2002*, Portoroz, September 26-27 2002. [Online]. Available: http://www.eurecom.fr/~michiard/pub.html

[12] S. Zhong, Y. R. Yang, and J. Chen, "Sprite, a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proceedings of IEEE INFOCOM '03*, San Francisco, CA, Apr. 2003.

[13] P. Michiardi and R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks," in *European Wireless 2002 Conference*, Florence, Italy, Feburary 2002. [Online]. Available: http://www.eurecom.fr/%7Emichiard/pub/michiardi"¨adhoc"¨selfishness.pdf

[14] J. P. Hubaux, J. Y. L. Boudec, S. Giordano, M. Hamdi, L. Blazevic, L. Buttyan, and M. Vojnovic, "Towards mobile ad-hoc WANs: Terminodes," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, Chicago, IL, September 2000. [Online]. Available: http://www.terminodes.com/mics/getDoc.php?sessid=003b3dfc72e02704e92bee%31b2460643"&docid=32"&docnum=1

[15] J. P. Hubaux, T. Gross, J. Y. L. Boudec, and M. Vetterli, "Towards self-organized mobile ad hoc networks: the Terminodes project," *IEEE Communications Magazine,*, January 2001. [Online]. Available: http://www.terminodes.com/mics/getDoc.php?sessid=003b3dfc72e02704e92bee%31b2460643"&docid=31"&docnum=1

[16] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management, Tech. Rep. 96-17, 28, 1996. [Online]. Available: http://citeseer.nj.nec.com/blaze96decentralized.html

[17] P. Zimmermann, *PGP User's Guide*. Cambridge, MA: MIT Press, 1994.

[18] G. Zacharia, "Collaborative reputation mechanisms in online communities," Master's thesis, Massachusetts Institue of Technologys, 1999.

[19] G. Zacharia, A. Moukas, and P. Maes, "Collaborative reputation mechanisms in electronic marketplaces," in *Proceedings of the 32nd Hawaii International Conference on System Sciences*, 1999. [Online]. Available: http://citeseer.nj.nec.com/rd/78162331%2C324569%2C1%2C0.25%2CDownload/h%ttp%3AqSqqSqmas.cs.umass.eduqSq%7EaseltineqSq791SqSqzacharia.collaborative"¨re%putation.pdf

[20] M. J. Fischer and Z. Diamadi, "A simple game for the study of trust in distributed systems," *Wuhan University Journal of Natural Sciences*, vol. 6, no. 1-2, pp. 72–82, 2001.

[21] T. Vicsek, A. Czirok, E. B. Jacob, I. Cohen, and O. Schochet, "Novel type of phase transitions in a system of self-driven particles," *Physical Review Letters*, vol. 75, pp. 1226–1229, 1995.

[22] J. Wolfowitz, "Product of indecomposable, aperiodic, stochasic matrices," in *Proceedings of American Mathematical Society*, vol. 15, no. 733-737, 1963.

[23] E. Seneta, *Non-negative Matrices and Markov Chains*. New York, NY: Springer Verlag, 1981.

[24] C. K. Wong, M. G. Gouda, and S. S. Lam, "Secure group communications using key graphs," in *Proceedings of ACM SIGCOMM '98*, Vancouver, B.C., Sept. 1998. [Online]. Available: http://www.acm.org/pubs/contents/proceedings/comm/285237/

[25] Y. R. Yang, X. S. Li, X. B. Zhang, and S. S. Lam, "Reliable group rekeying: A performance analysis," in *Proceedings of ACM SIGCOMM '01*, San Diego, CA, Aug. 2001. [Online]. Available: http://www.acm.org/sigs/sigcomm/sigcomm2001/

[26] R. Horn and C. R. Johnson, *Matrix Analysis*. New York. NY: Cambridge University Press, 1995.

[27] S. Karlin and H. M. Taylor, *A First Course in Stochastic Processes*, second edition ed. Academic Press, 1975.

[28] L. Kleinrock and J. Sylvester, "Optimum transmission radii for packet radio networks or why six is a magic number," in *IEEE National Telecommunications Conference*, Birmingham, AL, December 1978, pp. 4.3.1–4.3.5. [Online]. Available: http://citeseer.nj.nec.com/ncontextsummary/158232/0

[29] F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," April 2002. [Online]. Available: http://citeseer.nj.nec.com/509785.html

[30] D. Bertsekas and J. N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Athena Scientific, 1997.

[31] L. Lamport, R. Shostack, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Proggramming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[32] N. Lynch, *Distributed Algorithms*. San Mateo, CA: Morgan Kaufmann Publishers, 1996. [Online]. Available: http://theory.lcs.mit.edu/tds/distalgs.html