Cooperative Games, Phase Transitions on Graphs and Distributed Trust in MANET

John S. Baras and Tao Jiang

Abstract— **Mobile Adhoc Networks (MANET) provide a relative new paradigm of wireless networking, which poses several formidable challenges for control, monitoring and management, due to the basically "infrastructureless" nature of these networks. Security is viewed in this paper as part of the control-operations-management functionality of MANET. An important and critical part of security is trust establishment and maintenance. We provide a description of distributed trust within the MANET framework that consists of two major components: (a) trust document distribution; and (b) distributed trust computation. Within (a) we summarize our earlier work on swarm-intelligence based trust document distribution schemes, including their major advantages as compared to other schemes as well as their performance. This paper is primarily addressing our new results within (b). Here we show that under a variety of schemes for distributed trust computation and establishment we have established strong connections with various components of the theory of random graphs. In this context we demonstrate how phase transitions (in this case they mean node transitions from non-trusted to trusted) can appear within a MANET. We link the existence and analysis of such phase transitions to dynamic cooperative games. We demonstrate that dynamic cooperative games provide a natural framework for analyzing several problems for MANET. We also demonstrate the fundamental influence of the topology of the MANET on these phase transitions. Finally we conclude with a preliminary description of results that describe the effects of mobility and topology change on these trust establishment schemes.**

I. Introduction

Due to the absence of infrastructure, vulnerability of wireless links and changes in topology, MANET poses several formidable challenges for network control, monitoring and management. Securing such a network as part of the control-operations-management functionality is much more difficult than in traditional hierarchical architectures, but crucial in both military and commercial applications.

An important and critical part of security is trust establishment and maintenance, which is foundation for later-on securing mechanisms, such as key management and secure transmission. In MANET, existence of CA or KDC could not be assumed, so any notion of authentication or trust certificates issued by trusted third party(TTP), which is widely used in nowaday Internet and cellular networks, is no more suitable. Thus we consider **local information exchange** and **distributed computation** as the essential and unique characteristics of trust management in this new paradigm of wireless networking, as opposed to traditional centralized approaches.

Several models have been proposed in the literature for trust computation in large-scale open systems, such as [1], [2], [3], [4] and [5]. Previous research results avoided dependence on any centralized servers and provided trust computation mechanisms in a distributed way. However, almost all the methods assume the existence of certain trust relationships between communicating nodes. In distributed and autonomous systems, obtaining evidence for these trust relationships is not an easy job. One of the previous works ([6]) on trust evidence distribution is based on a P2P File-sharing system – Freenet [7]. The problem in distributed P2P systems is that mobility is not taken into account. Therefore the Freenet-based scheme is not able to easily handle transmission failures and routing table updates. In our previous work [8], we proposed a new approach: ant-based evidence distribution (ABED), which preserves all the advantages of P2P file-sharing systems and in addition is suitable for mobile environments.

In ABED, interacting with each other using information - "pheromone" deposited - in nodes they pass, mobile artificial agents, called "ants", are able to find the optimal path toward their food, i.e. trust evidence in the present context. The pheromone regulation process, especially *reinforcement mechanism*, enables the exploration of new paths, which makes it particularly suitable for dynamically changing environments, such as MANET.

We simulated ABED using ns-2. We compared ABED with the Freenet based scheme proposed in [6]. The results show that ABED outperforms Freenet based schemes in all the metrics including hopcount needed to retrieve trust evidence, rate of successfully obtaining evidence and request delay. Especially, ABED shows fast convergence properties at the beginning of the process, which is highly desired for mobile wireless networks.

The main topic of this paper will focus on the second part of our scheme: distributed trust computation. Our goal is to build a trust computation model based only on local interactions, and we investigate the global effects of these interactions both by simulation and theoretical analysis. Our

Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011. Research also supported by the U.S. Army Research Office under grant No DAAD19-01-1-0494. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

J. S. Baras and T. Jiang are with the Institute for Systems Research and the Department of Electrical & Computer Engineering, University of Maryland, College Park, MD 20742 USA. Email: {baras, tjiang}@isr.umd.edu

focus is the analysis of dynamic and emergent behaviors from local inference in terms of trust computation.

II. Graphs, cooperative games and phase transitions

A. Graph model

In this paper, the wireless MANET is modeled as an undirected graph $G(V, E)$. Notice that edges of G represent coonections in the context of trust information exchange, which do not necessarily require two end nodes to be neighbors in geometrical distance. In other words, we are primarily interested in the logical model of the network that models the **logical relation** of trust rather than the spatial graph. We distinguish two different types of links: links between neighboring nodes (nodes within wireless communication range) and links between pre-trusted nodes (nodes trust each other from the very beginning). Both types of links are bound to certain cryptographic keys, thus authentication, integrity and confidentiality are considered to be guaranteed. Those keys are established either by secure physical channels (for neighboring nodes) or offline key exchanges (for pre-trusted nodes). Let $N_i = \{\text{node}j | e_{ij} \in E\}$ be the 'trust' neighborhood of vertex i.

We will investigate the behavior of our trust computation model on different logical graph topologies. In particular, we will investigate three kinds of graph:

- *Physical graph*: with only links between neighboring nodes.
- *Random graph*: with only links between pre-trusted nodes. We assume pre-trusted nodes are randomly chosen from nodes pairs and they are independent of node positions, therefore it forms a random graph. The theory of random graphs was founded by Paul Erdös and Alfréd Rényi [9].
- *Small-world graph*: a set of models that lie between the aforementioned physical graph and random graph. Small-world phenomena were first theoretically modeled and studied by Watts and Strogatz in their groundbreaking paper [10], where shortcuts are created by rewiring links in a regular lattice. The most prominent properties of the small-world graph model are short average path length and large clustering coeffiecient, given a very small number of shortcuts. We will demonstrate the advantages offered by these properites in trust establishment.

We will elaborately describe and define the three models in Section IV.

B. Cooperative games

As we discussed in Section I, trust computation is distributed and restricted to only local interactions in a MANET. Each node, as an autonomous agent, makes the decision on trust evaluation individually. The decision is based on information it has obtained by itself or from its neighbors. Those aspects are analogous to situations in statistical mechanics of complex systems with game theoretic interactions. Game theory and more specifically the theory of evolutionary games provides the framework for modeling individual interactions. We first probe into two basic cooperative game models and their relation to our approach to trust computation.

1) Ising model : One of the simplest local interaction models is the Ising model, that describes the interaction of magnetic moments or spins, where some spins seek to align with one another (ferromagnetism), while others try to anti-align (antiferromagnetism). The Ising spin model consists of n spins. Each spin is either in position "up" or "down". Any configuration of spins is denoted as $\mathbf{s} = \{s_1, s_2, \ldots, s_n\}$, where $s_i = 1$ or -1 indicating spin i is up or down respectively. A Hamiltonian, or energy, for a configuration $\mathbf{s}$ is given by

$$H(\mathbf{s}) = -\frac{1}{T} \sum_{\forall i \in V, j \in N_i} J_{ij} s_i s_j - \frac{mH}{T} \sum_i s_i. \qquad (1)$$

where T is the temperature. The first term represents the interaction between spins. The second term represents the effect of the external (applied) magnetic field.

The problem of computing the ground states (global minimum of energy) for the Ising model is an NP-hard problem. There are 2^n possible configurations for the model, the computation becomes infeasible when n gets large. So we must use heuristic methods to find low energy configurations. As proposed in [11], we could imagine that the spins try to reduce their own *frustration* (or energy) individually, and come up with an interesting cooperative game. In game theoretic terms, the *payoff* for node i when the graph has a configuration $\mathbf{s} = \{s_1, s_2, \ldots, s_n\}$ is

$$\pi_i = \sum_{j \in N_i} J_{ij} s_i s_j \qquad (2)$$

When $J_{ij} = 1$, the agents are rewarded for aligning their states; when $J_{ij} = -1$ they want to take on opposite states in order to maximize their payoffs. Agents interact in order to maximize their own payoffs.

This model provides the inspiration for our approach, as it can be directly used for distributed trust computation. Let s_i be the trust value assigned to node i, where $s_i \in \{-1, 1\}$. Node i will be assigned a trust value according to the opinion of the majority of its neighbors. We set $J_{ij} = 1, \forall j \in N_i$. Then the payoff of i is $\pi_i = s_i \sum_{j \in N_i} s_j$. In order to maximize π_i, i will set s_i with the same sign as $\sum_{j \in N_i} s_j$, which is actually the same value as neighbor majority. Simulations using Simulated Annealing (SA) show that the average payoff of the whole network is a function of the temperature T in the Ising model. High temperatures, in the trust computation context, mean that the agents are very conservative and not willing to change their trust values, the payoffs are near 0, which is the expected payoff for a random set s_i from $\{-1, 1\}$. While, as the temperature decreases (aggressive agents), the algorithm becomes greedier and payoffs increase, most of the nodes will reach agreement.

2) Evolutionary prisoner's dilemma game: Another example of cooperative games is the prisoner's dilemma (PD) games. It provides a frustrated two-party interaction and has been extensively studied by physicists, economists, biologists and mathematicians. Evolutionary prisoner's dilemma (PD) games were introduced by Axelrod [12] to study the emergence of cooperation rather than exploitation among selfish individuals. Some recent works, such as [13] and [14], studied the stationary states of evolutionary PD games on square lattices and random graphs. The most interesting problem here is to find the payoff matrix that leads agents to cooperate instead of defecting. The payoff in trust computation will be the benefit of being trusted and of trusting neighbors. In our future work, we plan to find the conditions for the payoff matrix that force all agents to cooperate even with existing malicious nodes.

C. Phase transition

In the Ising model (section II-B.1), an important characteristic is *phase transition phenomena*. It is observed that when the temperature is high, all the spins behave nearly independently (no long-range correlation), whereas when temperature is below a *critical temperature* c_0, all the spins tend to stay the same (i.e., cooperative performance). Phase transitions are also studied in evolutionary PD games, such as in [13].

Phase transition is a common phenomenon that takes place in any combinatorial structure, where a large combinatorial structure can be modeled as a system consisting of many locally interacting components. A phase transition corresponds to a change in some global (macroscopic) parameter of the system as the local parameters are varied. Distributed trust computation is essentially a cooperative game where nodes interact with their neighbors locally. In the following section, we discuss a trust computation model based on local interactions and node cooperation. We will analyze the global parameters, especially emphasizing analogs of phase transition phenomena.

III. Distributed trust computation model

A. Model specification

Our distributed trust computation model is based on elementary voting methods. Only nodes in a node's neighborhood have the right to vote. For security concerns, nodes with key-identity binding certificates, which are signed by off-line authentication servers, are qualified to vote. Votes have to be digitally signed using voters' private keys and are sent to the owners of the votes with voters' certificates. Verification takes place when the owner of the votes wants to prove the trustworthiness of itself. The specification of our model is provided below.

- **Distribution of voters**: The distribution of valid voters depends on the application. Here we simply assume voters are uniformly distributed among nodes in the network, i.e. initially each node is qualified as a voter with probability P_v.
- **Voting rule**: Whether a voter votes or not depends on several conditions, such as the decision rule of voters, the accuracy of information, etc. However, in order to have a simple and general model, we assume that each voter votes for all its neighbors with the same probabilities. P_p is the probability that nodes provide a positive vote and they provide a negative one with probability P_n.
- **Decision rule**: Suppose node i gets $V_{p,i}$ positive votes and $V_{n,i}$ negative votes, the effective number of votes will count as $V_i = V_{p,i} - V_{n,i}$. Obviously, the more positive votes, the more the node is trusted. Let η be the threshold that determines the trustworthiness of a node. If $V_i \geq \eta \cdot |N_i|$, node i is trusted, otherwise node i is not trusted.

B. Model analysis

Given any $j \in N_i$, the probability that j provides a positive vote is $P_+ = P_v P_p$ and the probability of a negative vote is $P_- = P_v P_n$. Let the number of neighbors of node i be $K_i = |N_i|$, which is actually the degree of node i in the graph G. Let's order the elements in the set N_i, where N_{ij} is the j^{th} element in N_i. Let $T_{ij}, j = 1, 2, \ldots, K_i$ be the vote N_{ij} provides. $T_{ij} \in \{-1, 0, 1\}$, where -1 represents negative votes, 1 represents positive votes, 0 is the rest. Then the probability distribution of T_{ij} is:

$$P(T) = \begin{cases} P_- & if \quad T = -1 \\ 1 - P_+ - P_- & if \quad T = 0 \\ P_+ & if \quad T = 1 \end{cases} \tag{3}$$

Then the effective number of votes $V_i = \sum_{j=1}^{K_i} T_{ij}$.

Let P_{iT} be the probability that node i is voted as trusted. Then

$$P_{iT} = Pr\{V_i \geq \eta \cdot K_i\} = Pr\{\sum_{j=1}^{K_i} T_{ij} \geq \eta \cdot K_i\} \tag{4}$$

According to our voter model, voters are independent from each other and also their votes, $T_{ij}, \forall j \in \{1, 2, \ldots, K_i\}$ are independent from each other. Thus we have,

$$P_{iT} = \sum_{V_i \geq \lceil \eta \cdot K_i \rceil} \sum_{i=1}^{K_i} P(T_{ij}) \tag{5}$$

Note that even though the votes T_{ij} are independent, the trustworthiness of nodes are **not** independent. A simple example: suppose node i and node j share a common neighbor node k. Consider the extreme case, where a node is trusted only if all its neighbors vote positively for it. Then given that node i is trusted, which means its neighbor k is a voter with probability 1, the probability that node k votes for trusting j is P_p, instead of the *a priori* $P_v P_p$. However, in most of the present paper we assume that they are independent, which as will be shown later, under certain conditions, is a rather good approximation.

We are going to analyze the effects of local voting interactions on global features and dynamics of the entire

network. A main goal of trust establishment in MANET is to investigate if the network is *securely* connected, meaning if any pair of nodes can find at least one secure path between themselves in the netowrk [15]. A *secure path* in our context is a path consisting only of trusted nodes. We denote by θ the number of pairs of trusted nodes between which there exists a path in the network. Similarly, we define θ_s as the number of pairs of trusted nodes between which there exists a **secure** path in the network. Then the probability (percentage) for the existence of at least one secure path between trusted pairs P_{sp} is $P_{sp} = \frac{\theta_s}{\theta}$. Other metrics we considered include the percentage of trusted nodes in the network and the time taken to converge to a steady-state system.

Let V_T be the set of all trusted nodes in $G(V, T)$, i.e., $V_T = \{i | i \in V \text{ and } V_i \geq \eta\}$. Then we get a new graph $G_T(V_T, E_T)$ which is the **induced** subgraph of G by V_T. We call $G_T(V_T, E_T)$ the *trust graph* and $E_T = \{e | e \in E \text{ and both ends of e are in } V_T\}$. Therefore, we have $N_{trust} = |V_T|$ and NP_{secure} is the number of (path) connected pairs in G_T. The probability of the existence of secure paths P_{sp} is dependent on the cluster size and connectivity of G_T.

IV. Topology Effects

In this section we further investigate our distributed trust computation model on different network topologies: random graphs, physical graphs and small-world graph models. We'll show the significant influences of network topology on the dynamics of trust models.

A. Random Graphs

We take the random graph model defined by Erdös and Rényi in their classic article on random graphs [9]: every pair of nodes is connected with probability p. Such a random graph is denoted by $G(n, p)$, where $n = |V|$ is the total number of nodes, which is also called as the binomial model.

We say that the random graph $G(n, p)$ *evolves* as p increases from 0 to 1 [9]. The random graph starts with a set of n isolated vertices, eventually becomes a fully connected graph, with the maximum number of edges $\frac{n(n-1)}{2}$ for $p \to 1$. According to random graph theory, $p(n)$ satisfies the *Zero One Law* – at certain $p(n)$, a particular property of a graph most likely arises, and surprisingly appears quite suddenly. For instance, $p = \frac{1}{n}$ is the famous "double jump" of Erdös and Rényi, after which a giant component has emerged and connectivity is achieved at $p = \frac{\ln n}{n}$.

Now let us return to our trust model. Assume that 'trustworthinesses' of nodes are independent. Then we could let $P_T = P_{iT}, \forall i \in V$, which is a function of P_+, η and K_i. Therefore given the trust graph $G_T(V_T, E_T)$, the probability of obtaining G_T is

$$P[G_T] = P_T^{|V_T|}(1 - P_T)^{|V/V_T|}, \tag{6}$$

where $V/V_T = \{j | j \in V \text{ and } j \notin V_T\}$.

Consider the limiting properties of random graphs, i.e. for n large enough,

$$|V_T| \approx P_T \cdot |V|. \tag{7}$$

If $\eta \ll 1$, i.e. few nodes are needed to prove trustworthiness,

$$|V_T| = O(|V|) = O(n). \tag{8}$$

Then according to the *Zero One Law*, at $p = O(\frac{1}{n})$, a giant cluster emerges in the trust graph G_T, thus the probability of the existence of at least one secure path between trusted pairs P_{sp} starts to become significantly greater than 0. Once p reaches $O(\frac{\ln n}{n})$, G_V is connected, i.e. $P_{sp} \to 1$. Therefore, for $O(\frac{1}{n}) \leq p \leq O(\frac{\ln n}{n})$, the value of P_{sp} ranges from approximately 0 to 1. Increasing the threshold η results in decreasing P_T. By Eqn. (7), $|V_T|$ decreases accordingly. Therefore the number of trusted nodes is smaller, which means increasing the threshold η will reduce the percentage of secure path P_{sp}.

We simulate the trust computation models according to the algorithm in section III-A. The simulation parameters are listed in Table I below. Our numerical results support the above analysis. In Fig. 1, the x axis is the threshold value η, the y axis is P_{sp} and each curve corresponds to a different value of p. Notice that when η is small, specifically $\eta \leq 0.4$, all curves are relatively flat, where random graph properties dominate the trust graph G_T. As η grows, P_{sp} decreases. Especially, at around $\eta = 0.5$, phase transition is continuous and sharp.

TABLE I
SIMULATION PARAMETERS

Number of nodes n	100
Edge existing probability p	simulation variable
Probability of voters in the graph P_v	0.5
Probability voters provide positive votes P_p	0.9
Probability voters provide negative votes P_n	0
Trustworthiness threshold η	simulation variable

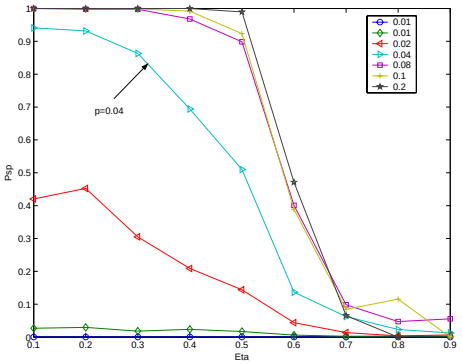

Fig. 1. P_{sp} vs. η in random graphs, each curve is with different edge probability p

Let's further investigate the *Zero One Law* for a given threshold. In our simulations, we fix $\eta = 0.3$ which is

considered to be fairly small according to Fig. 1 and with variable p changing. We can easily observe that the phase transition phenomenon happens when $p \in [0.01, 0.1]$, which is exactly the phase transition interval $[O(\frac{1}{n}), O(\frac{\ln n}{n})]$ of $n = 100$ derived in the theoretical analysis. Though the accurate equality in Fig 2 is a coincidence, the interval order justifies our analysis.

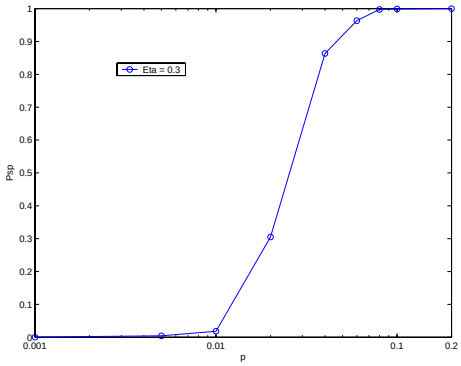

Fig. 2. P_{sp} vs. p in random graphs with η fixed at 0.3

B. Physical graph

For simplicity, our physical graph is modeled as a 2-D $L \times L$ lattice with periodic boundary, so the degree of each node is fixed to 4. Our trust path in a 2-D lattice is similar to "site percolation" in statistical mechanics, in which all the links are present and the nodes of the lattice are occupied with probability p . According to the results of percolation theory, especially of site percolation, for the 2-D lattice with probability p, there exists a critical probability $p_c = 0.5927$ as $L \to \infty$. Since trusted nodes are decided with probability P_T, as defined in subsection IV-A, P_T is actually the site presence probability p in G_T.

We could derive the accurate value of P_T for 2-D lattices. Referring to the parameters in Table I, using Eqn. (5), we have for $\eta_1 = (0.25, 0.5]$, $P_T^{(1)} = 0.609$. Similarly, for $\eta_2 \in (0, 0.25]$, $P_{T,2} = 0.1914$. Thus $P_T(2) < p_c < P_T(1)$, therefore phase transition happens as $\eta = 0.25 + \epsilon$, where ϵ is a small positive number. This is actually what we observed from numerical analysis as shown in Fig. 3.

C. Small-world graphs

The small-world model has its roots in social systems where most people are friends with their immediate neighbors. On the other hand, everybody has one or two friends who are far from him/her, which are represented by the long-range shortcuts. The first experiment on small-world networks was studied in [16], where mails were delivered using acquaintances. This experiments resulted in "six degree of separation". In the past five years, there has been substantial research on the small-world model in various complex networks, such as social networks, Internet and biological systems. As a social concept, distributed trust networks exhibit small-world properties too. In [17], it was

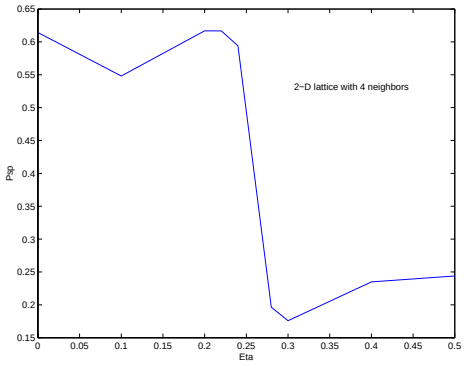

Fig. 3. P_{sp} vs. η in a 2-D lattice

shown that the PGP certificate graph is a small-world model. Therefore, to understand real trust systems in MANET, it is interesting to understand their behavior when the topology is small-world topology.

Several small-world models have been proposed so as to resemble actual networks. Scale-free networks in [18] present the growth and preferential attachments that appear to be the fundamental organizing principle for many complex networks. Most of the scale-free networks are small-world. Small-world concepts in the context of wireless ad hoc networks have also been discussed. Clustering in ad hoc networks generates naturally a small-work network, where clustering heads or hubs serve as nodes attaching with shortcuts. In another example, [19] creates a small world in large-scale wireless networks based on defining contacts for network nodes during resource discovery. In this paper, we use the first small-world model by Watts and Stragatz in [10](WS model), because it is relatively simple but retains the fundamental properties of practical networks.In the WS model, we start from a ring lattice with n vertices and $k = 4$ degree per vertex. Then each edge is rewired at random with probability p_{rw}, thus shortcuts are created. This construction models the graph between regularity ($p_{rw} = 0$) and chaos ($p_{rw} = 1$).

Our simulation results are shown in Fig. 4, where different curves represent different rewiring probabilities p_{rw}. We observe the obvious transition from regular lattices to random graphs in the simulations. In the middle of the transition, as $p_{rw} \approx 0.01$ both the property of high clustering in lattices and the property of short path in random graphs are present.

D. Trust Computation Continued ...

Our voting scheme can be performed for one or several rounds. Nodes, that have been voted as trusted nodes, become legitimate voters and vote for their neighbors along with other legitimate voters in following rounds. This dynamic voting process stops when the trust establishment reaches steady state, i.e., the trustworthiness of all nodes is not changing any more via voting. Thus the procedure starts from a small portion of pre-validated trusted nodes. Through

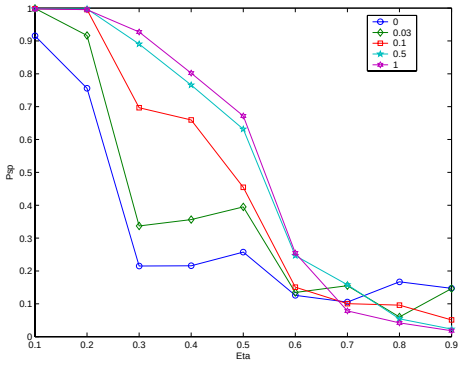

Fig. 4. P_{sp} vs. η in a WS small-world network

the iterations of local voting, the set of trusted nodes will grow from separated "trusted" isles to a connected trust graph throughout the network.

Figure 5 illustrates simuation results after several rounds of iterated voting on the same small-world model as in Figure 4. Comparing Figure 4 and 5, we could easily see the trust spreading process; for the same thereshold η, the latter has higher P_{sp} for all models. Figure 5 also shows that higher p_{rw} gives better performance (more secure paths). On the other hand, when the thereshold η is high, low p_{rw} value tends to resist deterioration, because trusted nodes are clustered together. The most significant curve is the one with $p_{rw} = 0.1$, which is a traditional small-world graph according to [10]. It not only achieves almost the same performance as a random graph, but also resists deterioration in high η. Apparently, with a relatively small portion of shortcuts, small-world networks facilitate the formation of secure paths.

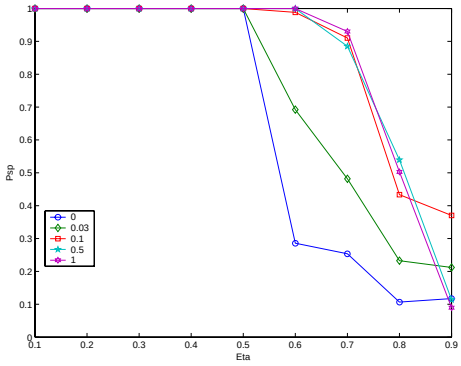

Fig. 5. P_{sp} vs. η in a WS small-world network at steady state

V. Conclusions and Future Work

In this paper, we provided a description of our distributed trust scheme within the MANET framework, that consists of two major components. One is trust evidence distribution. We summarize our earlier work on swarm-intelligence based trust evidence distribution schemes. We show that our schemes are especially suitable for distributed mobile networks, and provide better performance compared to previous methods. The other component, which is the main contribution of this paper, is distributed trust computation based on local interactions. We have demonstrated the connections of our model to random graph theory and cooperative game theory. We explain phase transition phenomena that appear in our trust computation model and describe the effect of topology on our scheme. Overall, our work is based on purely distributed mechanisms, which is desired in the context of MANET.

Our future work will combine the two components of our distributed trust management mechanism to find optimum and efficient solutions, theoretically analyze the iterated scheme on graphs, especially on small-world networks, and further investigate cooperative game theory for dynamic analysis of the computation part.

References

[1] M. K. Reiter and S. G. Stubblebine, "Toward acceptable metrics of authentication," in *Proceedings of IEEE Symposium on Security and Privacy*, 1997, p. 10.

[2] T. Beth, M. Borcherding, and B. Klein, "Valuation of trust in open networks," in *Proceedings of 3rd European Symposium on Research in Computer Security – ESORICS'94*, 1994, pp. 3–18.

[3] U. Maurer, "Modelling a public-key infrastructure," in *Proceedings of 1996 European Symposium on Research in Computer Security – ESORICS'96*, 1996, pp. 325–350.

[4] M. K. Reiter and S. G. Stubblebine, "Path independence for authentication in large-scale systems," in *ACM Conference on Computer and Communications Security*, 1997, pp. 57–66.

[5] P. Zimmermann, *PGP User's Guide*. MIT press, 1994.

[6] L. Eschenauer, "On trust establishment in mobile ad-hoc networks," M.S. Thesis, University of Maryland, College Park, 2002.

[7] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributed anonymous information storage and retrieval system," *Lecture Notes in Computer Science*, vol. 2009, p. 46, 2001.

[8] T. Jiang and J. S. Baras, "Ant-based adaptive trust evidence distribution in MANET," in *Proceedings of Second International Workshop on Mobile Distributed Computing*, Tokyo, Japan, March 2004, pp. 588–593.

[9] P. Erdös and A. Rényi, "On random graphs. I," *Publ. Math.*, pp. 290–297, Debrecen 1959.

[10] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, pp. 440–442, 1998.

[11] J. N. Bearden, "The spin galss bead game," Technical Report, L.L Thurstone Psychometric Laboratory, the University of North Carolina at Chapel Hill, 2001.

[12] R. Axelrod, *The Evolution of Cooperation*. New York: Basic Books, 1984.

[13] G. Szabo and C. Toke, "Evolutionary prisoner's dilemma game on a square lattice," *Physical Review E*, vol. 58, no. 1, p. 69, July 1998.

[14] H. Ebel and S. Bornholdt, "Coevolutionary games on networks," *Physical Review E*, vol. 66, no. 056118, 2002.

[15] S. Capkun and J. P. Hubaux, "BISS: Building secure routing out of an incomplete set of security associations," in *Proceedings of WiSe*, San Diego, USA, September 2003, p. 9.

[16] S. Milgram, "The small world problem," *Psychology Today*, vol. 1, no. 61, pp. 60–67, 1967.

[17] S. Capkun, L. Buttyán, and J. P. Hubaux, "Small worlds in security systems: an analysis of the PGP certificate graph," in *Proceedings of The ACM New Security Paradigms Workshop 2002*, Norfolk, Virginia Beach, USA, September 2002, p. 8.

[18] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 509512, pp. 509–512, 1999.

[19] A. Helmy, "Small worlds in wireless networks," *IEEE Communications Letters*, vol. 7, no. 10, pp. 490–492, October 2002.