

# Managing Trust in Self-organized Mobile Ad Hoc Networks \*

(Extended Abstract)

John S. Baras      Tao Jiang  
Institute for Systems Research and  
Electrical and Computer Engineering Department  
University of Maryland, College Park, MD 20742  
baras, tjiang @isr.umd.edu  
tel: 301-405-6606

As an important concept in network security, trust is interpreted as a set of relations among agents participating in the network activities. Trust relations are based on previous behaviors of agents. Trust management in distributed and resource-constraint networks, such as mobile ad hoc networks (MANETs) and sensor networks, is much more difficult but more crucial than in traditional hierarchical architectures, such as the Internet and base station- or access point-centered wireless LANs. Generally, this type of distributed networks have neither pre-established infrastructure, nor centralized control servers or trusted third parties (TTPs). The trust information or evidence used to evaluate trustworthiness is provided by peers, i.e. the agents that form the network. The dynamically changing topology and connectivity of MANETs establish trust management more as a dynamic systems problem. Furthermore, resources (power, bandwidth, computation etc.) are normally limited because of the wireless and ad hoc environment, so the trust evaluation procedure should only rely on local information. Schemes that depend only on local interaction also have the desired emergent property that enables fast reaction to network membership changes, topology changes and security changes that frequently happen in mobile networks. Therefore, the essential and unique properties of trust management in this new paradigm of wireless networking, as opposed to traditional centralized approaches, are: **uncertainty and incompleteness** of trust evidence, for instance, trust values can lie continuously between  $-1$  and  $1$ ; **locality** in trust information exchange; **distributed computation**, trust evaluation is employed individually .

In our work, local interaction requires that the control law for each agent should not require state information from all other agents, but rather from their neighbors. The neighbor set of an agent can represent the set of agents with which it is allowed to communicate (giving rise to a logical interconnection network), or the set of agents which it can sense, transit or receive information (physical wireless communication links). In order to decide the trustworthiness of agents based on their neighbors' opinion, the most straightforward scheme is to ask all their neighbors to "vote" for them. The value of each vote represents the opinion of the voter on the target agent. There have been several works that evaluate trustworthiness of neighboring agents in wireless environments, such as network traffic monitoring and distributed intrusion detection systems. Our vote values can be computed based on the observations from such systems. More general (than voting) policies can be accommodated in our analysis.

Trust management is a multifunctional control mechanism, in which the most important aspect is to establish trust from a small set of agents who are known to be trustworthy. These pre-trusted agents, for instance, can be the first few peers to join a network. Then the objective of the trust establishment is to evaluate the trustworthiness of the majority who are neutral initially (i.e. with trust value 0). They are evaluated by agents who have direct interaction with them. Those evaluating agents are either the physical or the logical neighbors of target agents. Based on their observations and evidence, they are able to provide opinions on the target agent and evaluate the trust value of the target agent. The whole network therefore evolves as the local interaction iterates from "isolated trust islands" to "a connected trust graph". Our interest is to discover rules and policies that establish trust-connected networks using

---

\*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.

only local interactions, to understand the impact of local interactions on the whole network and also to find the conditions under which trust spreads to a maximum set, as well as the parameters (e.g. topology type) that speed up or slow down this transition.

Another important aspect in trust management is trust revocation, which reverses previous trust opinions of agents based on newly obtained evidence with regard to those agents. Trust revocation is especially essential in mobile ad hoc environment because of the inherent properties of self-organized wireless communications. Rapid membership and topology changes due to node mobility and the existence of faulty or compromised nodes due to the vulnerability of networks require fast response and update on already established trust structure. In particular, if a previously trusted agent has been compromised or not in contact any more, how to revoke this agent and propagate the revocation to other peers in the network are crucial.

There have been several works on trust computation based on interactions with one-hop physical neighbors, such as [4] and [2]. However, most of the results in previous works are based on simulations. In our work, we analyze our local interaction rule using graph theory and percolation theory, and provide a theoretical justification for network management that facilitates trust propagation ([3]). Furthermore, in self-organized networks, agents are not under the control of any central authority, in other words, each agent is its own authority and adopts a selfish behavior. We model the interactions among agents as cooperative games, as opposed to non-cooperative games that are mostly used in the literature, and provide rules that encourage agents to collaborate with others and thus achieve the feasible Pareto optima in the context of cooperative games.

As discussed, 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 provide the framework for modeling individual interactions. This circle of ideas has a lot in common with randomized optimization methods from statistical physics, and especially from the theory of spin-glass materials.

One of the simplest local interaction models is the Ising model that describes the interaction of spins. This model provides the inspiration for our approach, as it can be directly used for distributed trust computation by relating the trust value of each node to the alignment of a spin. In the Ising model and more complex models of spin glasses, an important characteristic is the *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 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 changes in some global (macroscopic) parameters as the local parameters have varied. As the number of nodes in the network becomes large, phase transition is inevitable in both trust establishment and revocation. Therefore the parameters in the interaction rules are very crucial. For instance, in our trust establishment model ([1]), if the threshold is set just above the critical value, the network is separated into small groups of trusted nodes, while if the threshold is right below the critical value, the whole network emerges as a trusted giant component. We explain this rather surprising observation based on percolation theory and random graph theory.

## References

- [1] John S. Baras and Tao Jiang. Cooperative games, phase transition on graphs and distributed trust in manet. In *Proceedings of 43rd Control and Decision Conference (CDC'04)*, pages 93–98, Atlantis, Bahamas, December 2004.
- [2] Sonja Buchegger and Jean-Yves Le Boudec. The effect of rumor spreading in reputation systems for mobile ad-hoc networks. In *Proceedings of Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, Sophia-Antipolis, France, 2003.
- [3] Tao Jiang and John S. Baras. Autonomous trust establishment. In *Proceedings of 2nd International Network Optimization Conference*, March 2005.
- [4] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the Twelfth International World Wide Web Conference*, pages 640–651, Budapest, Hungary, 2003.