DYNAMIC AND DISTRIBUTED TRUST FOR MOBILE AD-HOC NETWORKS[1, 2]

John S. Baras and Tao Jiang
Electrical and Computer Engineering Department
and the Institute for Systems Research
University of Maryland College Park
College Park, MD 20742

ABSTRACT

Future battlefield networks will involve thousands of heterogeneous nodes operating under rapidly changing connectivity, and resource (bandwidth, energy, computation, etc.) constraints. Mobile Ad-hoc networks (MANET) form the basis for current and future military networks. Trust and trust establishment among communicating nodes (soldiers, vehicles, UAVs, satellites) and sensor nodes is the absolutely starting point for establishing any such network. The network management system needs to frequently validate trust, frequently defend against attacks, quickly isolate compromised nodes, and quickly establish trust in dynamically collaborating group (topology changes). In this paper we provide our solution to the problem of establishing and maintaining trust relations within a MANET, in a manner that satisfies both the dynamic and distributed constraints of the problem.

1. INTRODUCTION

Due to the absence of infrastructure, vulnerability of wireless links and changes in topology, MANET poses several formidable challenges for networking control, monitoring and management. The essential and unique properties of trust management in this new paradigm of wireless networking, as opposed to traditional centralized approaches are: (1) Uncertainty of trust value. Trust value is represented as subject probability ranging from 0 to 1; (2) Locality in trust information exchange; (3) Distributed computation.

The main ingredients of our innovative solution are: (i) An efficient, resilient, distributed scheme for distributing trust evidence documents; (ii) A distributed scheme for "spreading" trust to validated nodes; (iii) A new concept of topology control that helps trust propagation (speed) and minimizes resources (number of links and bandwidth); (iv) Fundamental analytical results, backing experimental evidence of performance, based on techniques from mathematical physics of spin glasses and phase transitions and on the mathematics of dynamic cooperative games on graphs. Within (i), our earlier work on swarm-intelligence based trust document distribution schemes (Jiang et al., 2004), shows its major advantages and performance in MANETs. This paper is focused on our results within (ii)-(iv). Our goal is to build a trust computation model based only on local interactions, and to investigate the global effects of these interactions. 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. The cooperative game framework we develop is useful for investigating other emergent properties of MANET: route connectivity, security, resource allocation.

[1] Prepared through collaborative participation in the Communications and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance (CTA) Program, Cooperative Agreement DAAD19-01-2-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.

[2] The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied of the Army Research Laboratory or the U.S. Government

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **00 DEC 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Dynamic And Distributed Trust For Mobile Ad-Hoc Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Electrical and Computer Engineering Department and the Institute for Systems Research University of Maryland College Park College Park, MD 20742

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM001736, Proceedings for the Army Science Conference (24th) Held on 29 November - 2 December 2005 in Orlando, Florida.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	17. LIMITATION OF ABSTRACT **UU**	18. NUMBER OF PAGES **2**	19a. NAME OF RESPONSIBLE PERSON

2. GAME-BASED MODEL

The network is modeled as an undirected graph $G(V, E)$, where V is the set of nodes, and E is the set of links. This is the physical model of the network. We are primarily interested in the logical model of the network that models the *logical relation* of trust. Thus we also consider the *Trust Graph*: $G_T(V_T, E_T)$, where V_T is the set of "trusted" nodes, a subset of V. G_T is the induced (by V_T) subgraph of $G(V, E)$. Here $E_T = \{e \mid e \text{ in } E, \text{ both ends of } e \text{ in } V_T\}$. Our distributed trust computation model is based on local policies (i.e. extensions of voting methods), which are rules that govern the collective decision of legitimate neighbors of a node regarding the trustworthiness (i.e. trust value) of the node. Agents are self-interested, and usually face a frustrated interaction. Normally outcomes without cooperation are worse than those with cooperation. Thus, it is desirable to analyze rules that force all entities to cooperate. These aspects are analogous to the statistical mechanics of complex systems with game theoretic interpretations.

Inspiration for our analytical methods comes from the Ising model in physics (Kindermann et al., 1998). The Ising model describes the interaction of magnetic moments or spins, where some spins seek to align (ferromagnetism), while others try to anti-align (antiferromagnetism). Each spin is either in position "up" or "down". In the Ising model, spins aim to minimize the Hamiltonian by only local alignment interactions. Inspired by the Ising model, we develop an interesting cooperative game, where nodes in the network correspond to spins and all nodes only interact with their neighbors. Let us assume nodes can only choose their strategies from two candidates which are denoted by $s_i \in \{-1,1\}$, and define the payoff matrix $\mathrm{Y} \in \mathbb{R}^{n\times n}$ and $y_{ij} = (J_{ij}/T)s_i s_j$. Then the payoff matrix Y defines the characteristic function of co-operative games $v : 2^N \to \mathbb{R}$, and $\forall$ coalition $S \subset N$,

$$v(S) = \sum_{\substack{i\in S\\ j\in S}} y_{ij} - \sum_{\substack{i\in S\\ k\notin S}} y_{ik}.$$

Then we get a formal cooperative game $\Gamma = (N, v)$, where each player aims to maximize their payoffs. We investigate coalition construction and the dynamics of coalition formation. We also find the conditions for the existence of a nonempty core for this trust cooperative game; i.e. which forces all the agents to cooperate to form a grand coalition. One interesting phenomenon in the Ising model is phase transitions. We find that phase transitions occur in the distributed trust models proposed here and analyze the scheme parameters controlling these phase transitions.

3. ANALYSIS

We analyze the effects of local interactions on global features and dynamics of the system. One of the most important properties is the existence of trusted paths (i.e. paths where all nodes are trusted) between trusted sources and destinations (Capkun et al., 2003). We analyze trust dynamics within a MANET, i.e. how trust spreads and/or is revoked between nodes. Trust dynamics are caused in MANET by node mobility, faulty nodes, compromised nodes, membership changes, topology changes, trusted path changes, changes in the referees for a node, changes in trust evidence for a node. We investigate and answer questions such as: Does trust spread to a *maximum* set of nodes? What parameters speed up or slow down this transition? We analyze performance as measured by metrics such as: the percentage of nodes that become trusted correctly as a function of time; the number of trusted paths generated; the probability of existence of at least one trusted path between any two trusted nodes; the smallest number of initial trusted nodes that can "spread" trust correctly to the entire network.

REFERENCE

Jiang, T. and Baras, J. S., 2004: Ant-based Adaptive Trust Evidence Distribution in MANET, in *Proc. of 2nd Intl. Workshop on Mobile Distributed Computing*, Tokyo, Japan, 588-593

Kindermann, R and Snell, J. L., 1980: *Markov Random Fields and their Applications*, American Mathematical Society, Providence, Rhode Island

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