Autonomous Trust Establishment[1]

Tao Jiang John S. Baras
Institute for Systems Research and Department of Electrical Engineering
University of Maryland, College Park, MD 20742 USA
Email: {tjiang, baras}@isr.umd.edu

Abstract

Trust establishment in networks is the essential foundation for follow-on security mechanisms, such as key management and secure transmission. In this paper, we concentrate on self-organized, distributed and resource-constraint networks which pose formidable challenges on trust establishment due to lack of infrastructure and centralized servers. We model our trust establishment strategy as a local voting scheme and discuss its long run behavior. More specifically, we investigate the dynamic evolution of trust within the network, i.e. how trust spreads among nodes, via analyzing its convergence behavior. By theoretical analysis based on graph theory, we also find the conditions under which trust spreads to a maximum set of nodes and parameters that speed up or slow down this transition.

keywords: Network, Trust Establishment, Security, Graph Theory

1 Introduction

As an important concept in network security, trust is interpreted as a set of relations among agents participating in network activities. Trust relations are based on the previous behavior of agents within a protocol. Trust establishment in distributed and resource-constraint networks, such as mobile ad hoc networks (MANETs), sensor networks and ubiquitous computing systems, is much more difficult but more crucial than in traditional hierarchical architectures, such as Internet and base station- or access point-centered wireless LANs. Generally, this type of distributed networks has 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. 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 member 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 value is between -1 and 1; **locality** in trust information exchange; **distributed computation**, trust evaluation is employed individually.

Trust establishment is a process starting from a small set of agents who are known to be trustworthy. For example, the first few peers to join a network are often known to be trustworthy. While the majority are neutral, i.e. with trust value 0. They are evaluated by agents who have direct interactions with them. Those agents are either the physical or logical neighbors of target agents. Based on their observations and evidence, they are able to provide opinions on the target agent, to build the trust value (also called reputation) of the target agent. The whole network therefore evolves as the local interactions iterate from "isolated trust island" to "a connected trust graph". Our interest is to discover the rules that establish trust-connected networks using only

[1]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.

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 parameters that speed up or slow down this transition.

There have been several works on trust computation based on interactions with one-hop physical neighbors. In [3], for instance, first-hand observations are exchanged between neighboring nodes, where node A adjusts his opinion for node B, based on how close B's evidence is to A's previous opinion about another node C. It provides an innovative model to link nodes' trustworthiness with the quality of the evidence they provide. While, our work emphasizes the inference of trust value rather than the methods to generate the direct trust. It is similar with [5] and [6], where weighted averages are used to aggregate multiple votes for trust evaluation and provided promising results on using this simple local interaction rule to correctly evaluate trust in distributed networks. Particularly in [5], different kinds of malicious behaviors have been simulated and their results showed that by ranking nodes according to the trust value, the network application (in their case, file downloading in p2p networks) doesn't get affected by malicious nodes. However, the results of both [5] and [6] are based on simulation. In this paper, we analyze our local interaction rule using graph theory and provide a theoretical justification for network management that facilitates trust propagation.

In addition to the above works, an extensive amount of research has focused on designing decentralized trust-inference protocols, such as [1] and [8]. These works categorize trust information into direct trust and recommendations (though they have different specific meanings), and trust evaluation is computed by aggregating along and across paths. Those schemes are applicable for networks that are easy to obtain routing and path information, but this requirement is not always true in our settings.

This paper is organized as follows. In Section 2 we discuss our framework based on the graph model. We formally define our trust evaluation rule and discuss some security issues. As our main contribution, Section 3 gives theoretical results and provides necessary conditions for establishing a trusted network. In Section 4, the topology impacts on our trust establishment procedure is provided and an important graphical parameter, the second largest eigenvalue of a graph, is discussed, which furthermore guides the network topology design.

2 Problem formulation

The network is modeled as an undirected graph $G(V, E)$. Throughout this paper, we use the terms *node* and *agent* interchangeably, where a node i is an element in the set V. From the discussion in Sect. 1, local interaction requires that the control law for each agent should not require state information from all other agents, but rather from a subset which we call neighbors: $\mathcal{N}_i \triangleq \{j|(i,j) \in E\} \subseteq \{1,\ldots,N\} \setminus \{i\}$. The neighbor set of agent i, $\mathcal{N}_i$, can represent the set of agents with which i is allowed to communicate (giving rise to a logical interconnection network), or the set of agents which i can sense, transit or receive information (physical wireless communication links).

In order to estimate 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 a particular voter on the target agent, which comes from observation of the voter. There have been several works that evaluate trustworthiness of agents in a distributed manner, such as network traffic monitoring and distributed intrusion detection systems [7, 12]. In this paper, we assume the voting values are provided by a certain scheme. Let's first introduce two notations. Let t_i be the trust value of node i and v_{ij} be the voting value from node i about node j, and $v_{ij} \in [-1, 1]$, where i fully trusts j with $v_{ij} = 1$ (absolutely positive vote), and $v_{ij} = -1$ when i totally distrusts j (absolutely negative vote). Our local voting rule for the trust value of node i

(t_i) could be interpreted as the following general rule:

$$t_i = f(v_{ij}, t_j, \forall j \in \mathcal{N}_i).$$

The function $f(\cdot)$ should satisfy the following properties:

- $-1 \leq f(\cdot) \leq 1$, since our trust value is in the range of $[-1, 1]$.
- Votes from the nodes with high trust value are more credible, so they should carry larger weights.

There are several choices for the voting rule, i.e. the function $f(\cdot)$. For instance, it can be the average, maximum or minimum of all votes. In this paper, the rule we use is the weighted average of all votes, where the efficient vote made by i is equal to the multiplication of v_{ij} and t_i, i.e., the trust value of node i is the weight applied to all votes taken by i. Therefore, we have the updating rule for the trust value of node i

$$t_i(n) = \frac{1}{d_i} \sum_{j \in \mathcal{N}_i} t_j(n-1) v_{ji}(n), \tag{1}$$

where n represents discrete time and $d_i = |\mathcal{N}_i|$ is the degree of node i. For the rest of the paper, we assume v_{ji} is a constant. Generally this assumption is not true, since agents are always willing to adjust their votes based on new information. However, what we are concerned within this paper is the convergence of the voting rule. By varying the voting values, the convergence time would be longer, but eventually trust value converges to the same steady state, given that voting values will be fixed finally. Therefore, we use v_{ij} instead of $v_{ij}(n)$ from now on. Let's define D to be the diagonal matrix whose ith diagonal element is d_i and the matrix V represents the values of all votes, $v_{ji} = 0$ if node j and i are not neighbors. Then Eqn. (1) is rewritten as

$$T(n) = D^{-1} V T(n-1), \tag{2}$$

where $T = [t_1 \ t_2 \ \dots \ t_N]'$ is the trust value vector. Obviously, Eqn.(1) satisfies the properties of the voting rule described above. Notice that this rule is quite conservative (or pessimistic), in the sense that nodes get fully trusted with value 1 only if all their neighbors are fully trusted and the votes by them are with 1. We consider that pessimism may be necessary in self-organized networks, since such networks are more vulnerable to malicious behaviors.

To determine the trustworthiness of nodes, we apply a threshold rule on the steady states of trust values, which are defined as $t_i = \lim_{n \to \infty} t_i(n)$. Our threshold rule is dependent on a system defined parameter η as follows:

$$\text{Node } i \text{ is } \begin{cases} \text{trusted}, & \text{if } t_i \geq \eta \\ \text{neutral}, & \text{if } t_i < \eta \end{cases}.$$

There are also concerns about the integrity, authenticity and availability of votes. We assume that nodes vote on all their neighbors, which can be forced by penalty, i.e. non-voting nodes are considered to be distrusted. The authenticity and integrity could be achieved by resorting to cryptography, such as digital signature. A more involved scheme is discussed in [4], where votes are used for key revocation. The difference is that our decision is based on collective values of all votes, while [4] considers the number of votes received for revocation. A different method is discussed in [5], where the weighted average is computed by another specific delegated node instead of the target node itself by using a distributed hash table (DHT); therefore nodes are not able to cheat on the votes for them. Hence, we assume that the voter of each vote is known and all votes cannot be modified.

Since our voting scheme is purely decentralized, any complete trust is not assured beforehand even when assuming that all agents are virtuous. The first and indispensable question to answer is how to build up a fully trusted or at least trust connected network in virtuous environments. Our theoretic analysis provides the necessary and sufficient condition for trust spreading through out the whole network, which is presented in the next section.

3 Trust spreading

In this section, we regard the trust establishment process as a dynamic system. We discuss the convergence property of the system and investigate the spreading of trust as the system reaches the steady state. First, we discuss the situation where voting starts without any intentional configuration, and we show that the condition to reach a fully trusted network is quite non-intuitive. Then we provide a mechanism that guarantees trust to be established in the whole network.

3.1 Simple voting

Since we assume no adversary in the network, i.e. all nodes behave rationally and all votes are "reasonable", which means we admit the uncertainty of the voting value but no one is voting maliciously, we have $v_{ij} \in [0, 1]$. Furthermore, nodes start with trust value no less than 0. Otherwise if a node has trust value less than 0 initially, it is excluded by others immediately. Therefore, $t_i(n) \geq 0,\ \forall i \in V$ and $n \geq 0$. Our goal is to show that as $n \to \infty$ the vector sequence $\{T(n)\}$ converges and to find the steady-state value T.

Define a matrix $F = D^{-1}V$, then the state equation (2) is written as $T(n) = F^n T(0)$. First, a very simple scenario is considered where all votes are all of the value 1, which means all nodes are able to correctly verify their neighbors as trusted. Therefore $V = A$, where A is the adjacency matrix of graph G, and F is the normalized adjacency matrix. It's trivial to verify that F is a *stochastic* matrix[2]. We show in the following that the convergence behavior of $T(n)$ depends on whether F is reducible or not, which represents the connectivity of the network.

- G is connected, i.e. F is irreducible.

  Since F is a stochastic matrix, the largest eigenvalue of F is 1. Let π be the right eigenvector corresponding to eigenvalue 1, which is an N-dimension normalized row vector[3], then $\pi F{=}\pi$. We could prove by ergodicity that [9],

  $$F^n = \begin{bmatrix} \pi \\ \pi \\ \vdots \\ \pi \end{bmatrix}.$$

  Thus $\forall i \in V$, $t_i \triangleq \lim_{n\to\infty} t_i(n) = \pi \times T(0) = \sum_{j=1}^{N} \pi_j t_j(0)$. Therefore, every node reaches the same trust value at the steady state. We can see that whether a node is trusted or not, purely depends on the initial configuration of $T(0)$. Obviously, if $\sum_{j=1}^{N} \pi_j t_j(0) \geq \eta$, all nodes are trusted, and none is trusted otherwise. Therefore the initial trust value is very crucial here. It is easier to establish a complete trusted network if a large number of nodes have high trust value initially, otherwise none will get trusted.

- G is not connected, i.e. F can be written (decomposed) as $F = \text{blockdiag}[F_1, F_2, \ldots, F_K]$, where $F_k, k = 1, \ldots, K$ are irreducible matrices of order N_k, $\sum_{k=1}^{K} N_k = N$. Thus the graph

[2] A matrix is called a stochastic matrix, if the sum of the elements of each row is 1.

[3] For a normalized vector, the sum of all elements is equal to 1.

G has K components, which are disconnected with each other. Let's use $\mathcal{C}_i, i = \{1, \ldots, K\}$ to denote those components, where $\mathcal{C}_i$ has normalized adjacency matrix F_i. Similarly, since F is irreducible, we can find the vector π_i which is the right eigenvector of F_i corresponding to eigenvalue 1, such that $t_i \triangleq \lim_{n\to\infty} t_i(n) = \sum_{j=\mathcal{C}_k} \pi_j t_j(0)$, if $i \in \mathcal{C}_k$. Therefore, the trustworthiness of a node is related to the initial configuration within its connected component. It's easy to extend the results of irreducible matrices to reducible ones by applying the method above. From then on, we will assume G is connected.

More generally, the voting value v_{ji} is less or equal to 1 instead of always being 1, i.e., uncertainty is considered. Then F is a semi-stochastic matrix. We can prove that $F^n \to 0$ as $n \to \infty$ (see Appendix), thus T also goes to 0. Therefore, trust **cannot** be established at all if there is uncertainty in votes.

We have shown that using the simple voting scheme, trust can only be established under certain strict conditions: all voting values are 1 and the initial configuration must satisfy $\sum_{j=1}^{N} \pi_j t_j(0) \geq \eta$. A single vote with value less than 1 will result in failure of trust establishment. This actually emphasizes the difficulties of designing algorithms in self-organized networks. However, we want to ensure fully established trust relations in virtuous network without depending on the initial states. Therefore we introduce the notion of headers, which are agents that are always trusted with trust value 1.

3.2 Voting with headers

As we just mentioned, headers are pre-trusted agents. For instance, they can be the leader of a cluster, or agents holding a certificate signed by authorities. To simplify the discussion, we also assume all headers only vote for nodes that they fully trust. Therefore, if a node i is trusted with b_i headers, it will get b_i more votes with value 1. So define b_i as the number of headers that fully trust node i. Let B be the diagonal matrix with ith diagonal element equal to b_i and $\mathbf{1} = [1 \ \ldots \ 1]'$. Then the updating rule in (2) changes to

$$T(n) = (D + B)^{-1}(VT(n-1) + B\mathbf{1}). \tag{3}$$

Again as we did in Sect. 3.1, first the situation with all 1-valued votes is considered, i.e., V=A. Define $\widetilde{T}(n) = \mathbf{1} - T(n)$. By Eqn.(3), we can deduce that $\widetilde{T}$ satisfies the equation

$$\widetilde{T}(n) = (D + B)^{-1}A\widetilde{T}(n-1) \triangleq \widetilde{F}\widetilde{T}(n-1), \tag{4}$$

where $\widetilde{F} = (D + B)^{-1}A$. Thus, $\widetilde{T}(n) = \widetilde{F}^n\widetilde{T}(0)$. It's easy to observe that if there is at least one node i such that $b_i > 0$, $\widetilde{F}$ is a semi-stochastic matrix. From Lemma 1 in the Appendix, we have $\widetilde{F}^n \to 0$, as $n \to \infty$. Therefore $T(n) \to 1$. It follows that

Corollary 1 *For a connected graph, all nodes get fully trusted in steady state given* 1*-valued votes, iff* $\exists$ *at least one node that connects to one or more headers.*

Thus adding just one header guarantees a fully trusted network. Now consider votes with uncertainty. The following theorem is the main result of this paper.

Theorem 1 *Given that the threshold of trustworthiness is* η*, the number of headers for each node must satisfy*

$$B\mathbf{1} \geq \frac{\eta}{1-\eta}(D - V)\mathbf{1}.$$

Proof Using a similar technique as above, let $\widetilde{T}(n) = \xi - T(n)$. Substituting it into Eqn.(3), we have

$$\widetilde{T}(n) = (D + B)^{-1}V\widetilde{T}(n-1) + (D + B)^{-1}\left((D + B - V)\xi - B\mathbf{1}\right). \tag{5}$$

Let the last term on the right hand side of Eqn. (5) be 0. Then $\widetilde{T}(n) \to 0$ as $n \to 0$, so $T(n) \to \xi$.

According to the decision rule, we want $T = \lim_{n\to\infty} T(n) \geq \eta\mathbf{1}$, therefore $\xi \geq \eta\mathbf{1}$. Consider the case $\xi = \eta\mathbf{1}$, since $(D+B)^{-1}\left((D+B-V)\xi - B\mathbf{1}\right) = 0$, we have

$$B\mathbf{1} = \frac{\eta}{1-\eta}(D-V)\mathbf{1}.$$

Notice that the function $f(x) = \frac{x}{1-x}$ is strictly increasing for $x \in [0,1)$. If we want $\xi \geq \eta\mathbf{1}$, then

$$B\mathbf{1} \geq \frac{\eta}{1-\eta}(D-V)\mathbf{1}.$$

■

Similarly, for graphs that are not connected, the theorem holds for each connected component separately.

Theorem 1 proves as well as provides a network design method to establish a fully trusted network by introducing certain number of headers. Moreover, this method only employs local interactions, and it converges to the desired result without dependence on any initial configuration.

4 Convergence rate and network topology

Having found a simple and light-weight trust establishment method, the next concern is the dynamics of the trust establishment procedure. In particular, we investigated the time it takes to reach the steady state, in other words how fast the trust values converge. We introduce an important theorem , the *Perron-Frobenius Theorem*[2], which states that for a stochastic matrix A, $A^n = \lambda_1^n v_1 u_1^T + O(n^{m_2-1}|\lambda_2|^n)$,where λ_1 is the largest eigenvalue with its left and right eigenvector u_1 and v_1 respectively[4], λ_2 is the second largest eigenvalue and m_2 is the algebraic multiplicity of λ_2. Thus the convergence rate of A^n is of order $n^{m_2-1}|\lambda_2|^n$. Normalized adjacency matrices are stochastic matrices, therefore those with smaller λ_2 converge faster.

Then the question becomes: what kind of networks or which network topology has smaller λ_2? Since the well-known small-world paper by Watts and Strogatz in 1998 ([11]), research on network topology has gained voluminous attention. The small world models have two prominent properties: high clustering coefficient and small average graphical distance between any pairs. The small average distance essentially indicates that nodes can communicate with other nodes in a few hops given a very large network.

In this paper, we consider one of many small-world models, the so-called ϕ-model ([10]), which is modeled by adding small number of new edges into a regular lattice. The network starts as a two-dimensional lattice with periodic boundary, and the neighbors are those one hop away. Then new edges are added by randomly choosing two unlinked nodes. In our simulations, a network is considered with 400 nodes on the lattice. For the original lattice, each node has 4 neighbors, and the total number of edges is 800. Each simulation includes several rounds. At each round, 2 new edges are added randomly into the network. The second largest eigenvalue and the convergence time are computed for each round. Figure 1 shows the second largest eigenvalue λ_2 as a function of the number of new edges added. It shows that with more edges added, the second largest eigenvalue of the graph decreases. So, generally speaking, small-world networks have smaller second largest eigenvalue than the original lattice. Figure 2 illustrates the substantial changes of the convergence time as new edges are added. Notice that given 8 new edges are added, which is just 1% of the total edges, the convergence time drops from 5000 rounds to 500 rounds. Thus trust is established much faster in a network with small-world property than a regular lattice. This conclusion also provides a direction for network management so as to achieve good performance.

[4]Notice that $\lambda_1 = 1$ for a stochastic matrix.

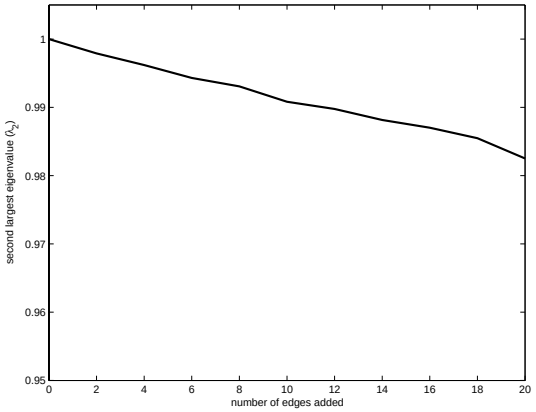

Figure 1: The second largest eigenvalue λ_2

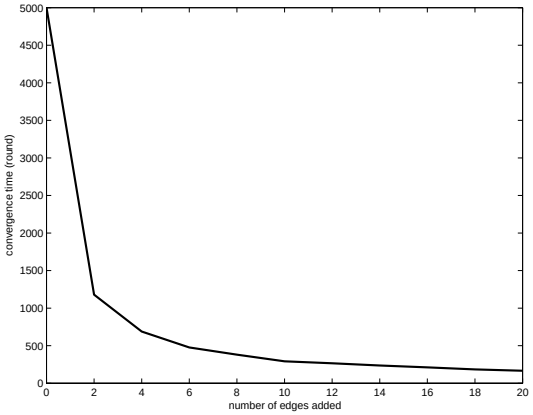

Figure 2: Convergence time

5 Conclusions and Future Work

In this paper, we formally defined a trust establishment strategy only based on local interactions. We showed that under very strict conditions, this self-organized rule is capable to establish a trust-connected graph. However, we provided a very simple and light-weight scheme that guarantees the trust establishment procedure converging to the fully trusted state. We also discussed the topology effects on trust spreading, which enlightens a new way for network management.

The scheme in this paper is a simple weighted average. We believe there are better rules for local interactions, for instance, only nodes with high enough trust value are legitimate to vote. However, though the weighted average rule in this paper is primitive, it's the starting point of our exploration on how reputation is built up in a purely decentralized network. Even though previous works have shown good results on identifying malicious behaviors, we are also working on the analytical proofs.

Appendix

Lemma 1 *If F is a semi-stochastic matrix, then $F^n \to 0$ as $n \to \infty$*

Proof Define $F^n = \{f_{ij}^{(n)}\}$. Without loss of generality, assume $\sum_{k=1}^{N} f_{1k}^{(1)} < 1$ and for $j \neq 1$, $\sum_{k=1}^{N} f_{jk}^{(1)} = 1$.

Define positive integers $m_j = \min\{n | f_{1j}^{(n)} > 0\}, \forall 2 \leq j \leq N$ and $m_1 = 0$. Then

$$f_{1j}^{(n)} \begin{cases} = 0, & \text{if } n < m_j \\ > 0, & \text{if } n = m_j \end{cases}$$

m_j actually represents the shortest path length between 1 and j. Since the graph is connected, $m_j < \infty$. The proof is finished by the following two facts

Fact 1 *$\forall 1 \leq j \leq N$, if $l \geq m_j + 1$, then $\sum_{k=1}^{n} f_{jk}^{(l)} < 1$.*

Fact 2 *Let $m = \max\{m_1, \ldots, m_N\} < \infty$, then $\sum_{k=1}^{N} f_{jk}^{(m+1)} < 1, \forall 1 \leq j \leq N$.*

So the largest eigenvalue of F^m is strictly less than 1. Thus $F^n = (F^m)^{\frac{n}{m}} \to 0$, as $\frac{n}{m} \to \infty$. ■

References

[1] Thomas Beth, Malte Borcherding, and Birgit Klein. Valuation of trust in open networks. In *Proceedings of 3rd European Symposium on Research in Computer Security – ESORICS'94*, pages 3–18, 1994.

[2] Pierre Brémaud. *Markov chains: Gibbs fields, Monte Carlo simulation, and queues.* Texts in applied mathematics; 31. Springer-Verlag New York, Inc., 1999.

[3] 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.

[4] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, page 197. IEEE Computer Society, 2003.

[5] 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.

[6] Sergio Marti and Hector Garcia-Molina. Limited reputation sharing in p2p systems. In *Proceedings of the 5th ACM Conference on Electronic Commerce*, pages 91–101, New York, NY, USA, 2004. ACM Press.

[7] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pages 255–265, Boston, Massachusetts, United States, 2000. ACM Press.

[8] Ueli Maurer. Modelling a public-key infrastructure. In *Proceedings of 1996 European Symposium on Research in Computer Security – ESORICS'96*, pages 325–350, 1996.

[9] Eugene Seneta. *Non-negative matrices and Markov chains.* Springer series in statistics. Springer-Verlag New York Inc., 2nd edition, 1981.

[10] Duncan J. Watts. *Small Worlds: the dynamics of networks between order and randomness.* Princeton University Press, 2004.

[11] Duncan J. Watts and Steven H. Strogatz. Collective dynamics of "small-world" networks. *Nature*, 393:440–442, 1998.

[12] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pages 275–283, Boston, Massachusetts, United States, 2000. ACM Press.