# TRUST DOCUMENT DISTRIBUTION IN MANETS

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

## ABSTRACT

*Mobile ad-hoc networks (MANETs) are used in battlefields where no network infrastructure exists. Users rely on their physical neighbors to communicate with other users that are not in proximity. Accurate trust establishment and maintenance is essential for secure and reliable message transmissions in MANETs. Because of the mobility and dynamics of MANETs, the validity and value of trust documents change with time as well as with battlefield conditions and scenario stage. Thus trust management in MANETs is a much more dynamic problem than in conventional wireline networks, as well as wireless cellular networks. In traditional networks, centralized trusted servers provide necessary trust documents for trust establishment. However, such servers are not available in MANETs. Trust documents are distributed among users in the network. In this paper, we develop and analyze distributed schemes for efficiently and securely distributing trust documents, and updates, so that users are able to establish reliable trust relations with their neighbors. Key performance metrics are time response and availability of documents across the network. Our approach is inspired from network coding, where trust documents are combined during distribution.*

## I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are used in battlefields where no network infrastructure exists. Users rely on their physical neighbors to communicate with other users that are not in proximity. Accurate trust establishment and maintenance is essential for MANETs. Trust relations between neighbors are necessary to make sure that the transmitting messages are not leaked to the enemy. On the other hand MANETs pose several formidable challenges on establishment, control and management of trust relationships due to lack of infrastructure and centralized servers. Because of the mobility and dynamics of MANETs, new trust relations need to be established when users meet new neighbors, and old trust relations need to be updated as well. In addition, the validity and value of trust documents change with time as well as with battlefield conditions and scenario stage. Thus trust establishment and maintenance in MANETs is a much more dynamic problem than in conventional wireline networks, as well as wireless cellular networks.

In traditional networks, trust management relies on centralized control servers, such as trusted third parties (TTPs) and authentication servers (ASs). Those servers are trusted and available all the time. Prior works within this framework ([1], [2], [3], [4]) all assume an underlying hierarchical structure within which trust relationships between ASs are constrained. However, such servers are not available in MANETs, and trust documents are distributed among users in the network.

To establish trust in such a distributed way has several advantages. It saves network resources (power, bandwidth, computation, etc.), which are limited in wireless mobile environments. It avoids the single point of failure problem as well. Moreover, the networks we are interested are dynamic with frequent topology and membership changes, and distributed trust has the desired emergent property ([5]), as users only contact a few and easy-to-reach users. However, it also poses difficulties and new challenges for trust management systems. In this paper, we study the challenges on distributing trust documents in MANETs. Since trust documents are scattered in the network, the problems of how to efficiently and securely store them and where to locate requested documents need to be carefully studied.

The problem of trust document distribution shares many characteristics of distributed peer-to-peer (P2P) file sharing systems ([6], [7]). Trust documents are files to be shared for trust management. Distributed and self-organized P2P systems have many common characteristics with ad hoc networks as well. Thus many trust management systems consist of components that are inspired from P2P systems. For instance, the trust management scheme P-Grid ([8]) is based on scalable replication of tree structures, which is derived from the P2P systems. In [9], the authors use hash-based routing in one of popular P2P networks - Freenet [7] for distribution of trust documents. Request routing in Freenet avoids flooding and improves with time. Files, or trust documents in this context, are replicated by caching

1-4244-1513-06/07/$25.00 ©2007 IEEE

at every node, which causes information to converge to where it is most needed.

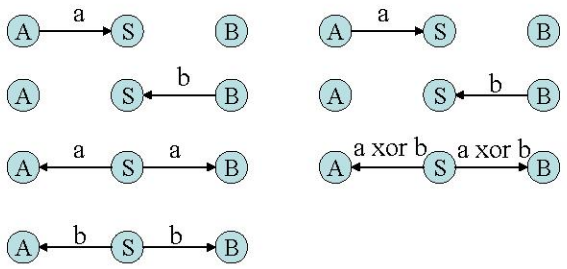
Despite the similarities between trust document distribution and P2P file sharing, there exist several unique properties of trust document distribution. The size of trust documents are a lot smaller compared to the hundreds of million or billion bit files in P2P sharing. The requests in trust document distribution usually aim at multiple documents, for instance, a request may ask for all trust documents about the trustworthiness of node $A$. While in P2P one request explicitly points to one single file. Furthermore, the topology changes in mobile scenarios happen much more frequently than in P2P networks. In this paper, we propose a new trust document distribution scheme that uses *network coding*, and we show that the new scheme handles the above unique properties and performs well in terms of efficiency and security. Network coding has been used in P2P file sharing as well. Gkantsidis and Rodriguez designed a P2P file sharing system named Avalanche, in which intermediate peers produce linear combinations of file blocks as in network coding ([10]). However, again, they are focused on downloading large files from file servers, and our interest is to distribute scattered trust documents.

This paper is organized as follows. Section II introduces the notion of network coding. A general framework of trust management system is provided in Sec. III. Section IV described our network coding inspired trust document distribution scheme in details. The evaluation results of our scheme are shown in Sec. V. Section VI provides conclusions and discusses the future work.

## II. NETWORK CODING

Network coding ([11]) is a recent field in information theory proposed to improve the throughput utilization of a given network topology . In communication networks today, packages are always separated with each other during transmissions. The principle behind network coding is to allow intermediate nodes to encode packets. Instead of simply forwarding data, intermediate nodes my recombine serveral input packets into one or several output packets. An overview of network coding and a discussion of possible Internet applications are given in [12].

To illustrate how network coding improves the propagation of information without global coordination, we consider a simple example in a wireless context with a three node topology. In Figure 1, nodes $A$ and $B$ want to exchange packets via a wireless base station, node $S$. In the traditional way, nodes $A$ and $B$ send packet $a$ and $b$ to node $S$ respectively. Then node $S$ sends packet $b$ and $a$ to node $A$ and $B$ respectively. Because of interference in wireless




(a) Traditional Method (b) Network Coding

Fig. 1. A Simple Network Coding Example

environments, this procedure takes four transmissions as shown on the left side of Figure 1.

If network coding is used, Node $S$ will first linearly combine packets $a$ and $b$, e.g. by binary adding the two packets: $a \oplus b$. Instead of forwarding packets $a$ and $b$ separately, $S$ broadcasts $a \oplus b$. After receiving the encoded packet, both $A$ and $B$ can recover the packet of interest, where the number of transmissions is reduced. This simple example is similar to linear network coding, while the $\oplus$ operation is replaced by linear combinations of data over some finite field. As we will see in this paper, linear network coding makes efficient propagation of trust documents and the associated operations are distributed.

## III. TRUST MANAGEMENT SYSTEMS

Trust management systems are comprehensive. In this section, we describe three components of trust management that we consider to be the most important: trust documents, trust document distribution and trust evaluation policies.

### A. Trust documents

Trust documents are digital credentials for trust. Different trust contexts require different types of credentials. Examples might be your driver's license, your social security card, or your birth certificate. Each of these has some information on it identifying you and some authorization stating that someone else has confirmed your identity. Some credentials, such as your passport, are important enough confirmation of your identity that you would not want to lose them, lest someone use them to impersonate you.

In cyberspace, users rely on digital trust documents. A digital trust document is data that functions much like a physical credential. In this paper, we are focused on digital trust documents, which are called *trust documents* or documents in short. Here are some examples of digital trust documents:

- *Digital certificate*: which is issued by a certificate authority or entity and verifies that a public key is owned by a particular entity. Digital certificates are used to thwart attempts to substitute one person's key for another. A digital certificate consists of three things: a public key, certificate information ("Identity" information about the user, such as name, user ID, and so on) and one or more digital signatures. Digital certificates are widely used in PGP and X.509.
- *IAFIS* (Integrated Automated Fingerprint Identification System): which uses human fingerprints as identities. It has made law enforcement officials capable to easily share information about criminals and quickly compare a suspect's fingerprint image with millions of similar imprints.

The trust documents can be generated by some trusted party as in centralized networks (commanders of the army), by friends who know each other (soldiers in the same group), or by certain monitoring schemes ([13], [14]). Creation of trust documents is not in the scope of this paper.

In MANETs, information is usually partial and incomplete. Uncertainty of trust must be introduced in the trust documents, which is usually represented by a value. This value denotes the degree of trust the issuer of the documents has on the target user. The value can be binary-valued, either trust or distrust, or multiple-valued, such as four levels of trust in PGP [15], or even continuous in an interval, say $[-1, 1]$.

In highly dynamic and mobile environments, the validity and value of trust documents change over time and space. Every user has confidence values on the documents he stores. The confidence value depends on several factors, for instance, time elapsed since the document is issued, and the communication distance taken by the document to reach the user. Normally, the confidence value is a monotonically non-increasing function of the elapsed time and communication distance. When the confidence value is below certain threshold, the corresponding document is considered to be invalid.

As an important security concept, we need consider the integrity and authenticity of trust documents as well. Digital signatures based on public-key cryptography have been studied by Maurer ([16]) and employed in PGP ([15]). However there are several difficulties with this approach: first, we have to assume that there is an immense public key infrastructure in place, which is impractical and prohibitively expensive for mobile devices; second, there has to be a reliable way to find the identities of entities and make sure the identities are not tampered. Those problems are especially important in mobile ad hoc networks with no fixed infrastructure and limited resources. One solution is to make use of side channels. For instance, in [17] and [18], users utilize a location-limited side channel, such as physical contact, to first exchange a small amount of cryptographic information. The information can be used to authenticate standard key exchange protocols performed over the wireless link. In the rest of the paper, we assume authenticity and confidentiality of documents have being achieved by applying certain cryptographic primitives.

### B. Document distribution

As we have discussed, in MANETs trust documents are typically issued and often stored in a distributed manner. Most of existing work ([19], [20], [21], [16]) assumes that one has already gathered all the potentially relevant documents in one place and does not consider how to gather these documents. The assumption that all documents are stored in one place is inconsistent with the idea of decentralized trust management. Document distribution raises many interesting questions. When Alice wants to assess trustworthiness of Bob, where should she look for documents? Often, she cannot look everywhere. How can she efficiently obtain requested documents? In addition, what are the best places to store the documents, such that they can be easily located, well protected and timely updated?

Trust document distribution provides the foundation for the third component: trust evaluation. It provides the input for the evaluation model. Till now, the document management and retrieval problem that exists in distributed ad hoc environments have not been well addressed, which is exactly the focus of this paper.

As one of the first works in the literature, Eschenauer ([9]) proposed a trust establishment scheme based on Freenet ([7]), where trust documents are routed and searched using distributed hash tables (DHT). More specifically, for a particular trust document, its ID is mapped into a value using a universally defined hash function. This hash value also corresponds to a unique node ID in the network. Then the document is routed to and stored in this node. When searching for this particular document, the requester gets the hash value using the same hash function and sets its request destination as the corresponding node. Thus trust documents are routed by hash-based routing instead of flooding.

In the next section, we propose our trust document distribution scheme that uses linear network coding to combine documents during transmissions. Our approach is inherently different with the commonly used request-response approach. We show that our scheme is absolutely distributed, which nicely handles the dynamic nature of the

problem.

### C. Trust Evaluation

As the user obtains necessary trust documents for the target user, he applies an evaluation policy to draw conclusions about the trustworthiness of the target user. Trust evaluation policy design has been an active field of research. Different policies or rules have been developed and studied, such as [20], [16], [22], [21], [23], [24] and [25]. PGP ([15]) is the only practical trust evaluation policy developed and implemented. Based on a very limited notion of uncertainty, PGP handles only the evaluation of trust in a chain of keys, with limited "levels of trust" (i.e. untrusted, marginal, full). Apparently, there is a need to develop new trust policies that apply to different types of trust documents, not just chains of keys, are fine-grained in the sense of uncertainty levels, and are flexible, in the sense that they can apply to incomplete sets of documents.

Although choosing the right model to evaluate trust and obtaining the documents to compute trust go hand in hand, trust document distribution is fairly independent of the specific evaluation model of trust. In the next section, we propose a trust document distribution scheme that uses network coding.

## IV. NETWORK CODING BASED SCHEME

In this section, we describe our proposed scheme for trust document distribution. We will outline the basic operation of this system, emphasizing some algorithmic parameters that affect its performance.

We assume a population of users that are interested in the trustworthiness of a particular user, that is the target user. The trust documents about the target user are initially stored in a number of users scattered throughout the network. These users are the issuers of the trust documents, or they have retrieved these documents from others. In the rest of the paper, we only consider trust documents about one single target user. All the operations are applied on those documents about the particular target user. Each trust document has a unique ID, which is obtained by applying a universally defined hash function to the document.

In MANETs, users cannot directly communicate with all other users; they only communicate with a small subset of users within the physical communication range, which we call the neighborhood. We assume that the neighboring relation is symmetric, i.e. if node $A$ is in the neighborhood of $B$, then, also $B$ is in the neighborhood of $A$. Symmetric channels are necessary in wireless networks, since reliable transmissions require that the two nodes can exchange information to avoid collisions and interference, such as the RTS/CTS messages [26]. In our scheme, users frequently check with their neighbors for new documents. If there are new documents, these documents are forwarded.

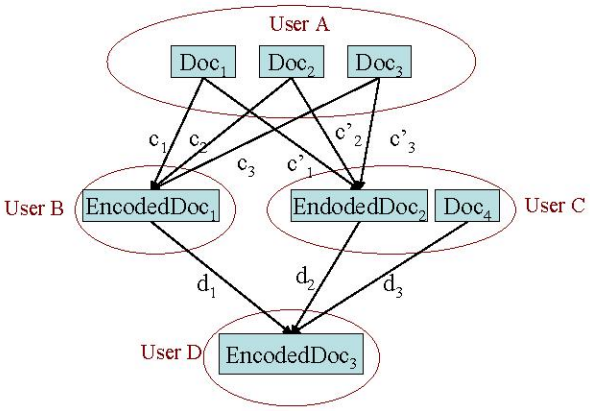



Fig. 2. Operations of the network coding system

Whenever a user wants to forward trust documents to another node, it produces a linear combination of all the documents it currently stores. The operation of the system is best described in the example of Figuer 2. Assume that initially user $A$ stores several trust documents about a particular target user. User $A$ will combine all the documents to create an *encoded document* as follows. It will pick some random coefficients $c_1$ and $c_2$, then multiply each trust document $i$ with $c_i$, and then add the results of the multiplications together, shown as follows

$$\text{EncodedDoc}_1 = (c_1 \cdot \text{Doc}_1) + (c_2 \cdot \text{Doc}_2). \quad (1)$$

All these operations take place in a finite field. If more than one user request trust documents from $A$, $A$ randomly picks different sets of coefficients for these users. Observe that the probability that two distinct users get the same set of coefficients depends on the size of the field. If the field is very small such "collisions" may happen and they will reduce the performance of the system. In most practical cases a field of size $2^{16}$ should be enough.

User $A$ will then transmit to user $B$ the result of addition, $\text{EncodedDoc}_1$, the IDs of the encoded trust documents and the coefficient vector $\mathbf{c} = (c_i)$. Assume now that user $A$ has also another encoded document $\text{EncodedDoc}_2$, with its associated coefficients $\mathbf{c}'$. User $A$ transmits it to user $C$ who stores another trust document, $\text{Doc}_4$. User $D$ is a neighbor of both user $B$ and user $C$. He requires trust documents from both $B$ and $C$. User $B$ randomly picks one coefficient $d_1$ and user $C$ picks two random coefficient $d_2$ and $d_3$. We have that

$$\begin{aligned} \text{EncodedDoc}_3 \;=\; & (d_1 \cdot \text{EncodedDoc}_1) \\ & +(d_2 \cdot \text{EncodedDoc}_2) \\ & +(d_3 \cdot \text{Doc}_4). \end{aligned} \quad (2)$$

The coefficient vector associated with the new encoded document is equal to

$$d_1 \cdot [c_1, c_2, c_3, 0] + d_2 \cdot [c'_1, c'_2, c'_3, 0] + d_3 \cdot [0, 0, 0, 1]$$

and the corresponding document IDs are $\text{Doc}_1$, $\text{Doc}_2$, $\text{Doc}_3$ and $\text{Doc}_4$.

Observe that given $n$ distinct trust documents, a user can recover them after receiving $n$ encoded documents for which the associated coefficient vectors are *linearly independent* from each other. The reconstruction process is similar to solving linear equations.

Our network coding scheme involves only local interactions. Users need not be aware of the existence of any trust document and its location. They only contact their neighbors to check whether there are new documents or new encoded documents. This is a great advantage as compared to any request-response scheme, such as the Freenet-based scheme. Request-response schemes require routing tables. If the topology of the network changes, new nodes come in or some nodes move out, routing tables need to be updated immediately. While, our scheme adapts quickly to the topology changes, since users only contact their current neighbors. In addition, request-response schemes require that users know the document IDs before sending out requests, which needs global information exchange. Our scheme operates without knowing any document ID.

We have mentioned that there are different types of trust documents with various confidence values. In addition, the importance of these documents varies dramatically. In other words, the trust documents in the network are *heterogeneous*. A good trust document distribution scheme should take such heterogeneity into consideration. Documents with high confidence values and of high importance should have high priority in transmission and they should be recovered before other documents. The simplest solution is to transmit these high priority documents separately. However, this solution essentially doubles the resources used for transmitting these documents. In our system, we mark these high priority documents, and they are always considered to be new documents. Therefore, whenever a user with high priority documents wants to forward his documents, he always combines the high priority documents with all other documents. In this way, these high priority documents have much higher chance to be recovered.

## V. Evaluation

In this section, we study the performance of our trust document distribution scheme that uses network coding and compare it with the Freenet-based approach in [9]. To evaluate the performance, we calculate the time it takes for each user to obtain all trust documents for the target user and the load of the network.

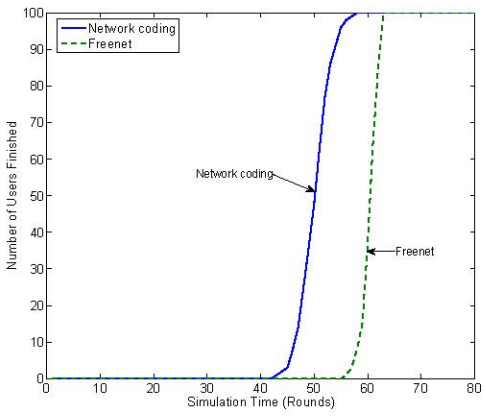



Fig. 3. Number of nodes finishing over time

To study the performance of relatively large number of users, we have implemented both our network coding based scheme and the Freenet based scheme in MATLAB. There are 100 nodes randomly placed in the $1 \times 1$ square. If the distance between two nodes is less than or equal to $0.2$, they considered to be neighbors. Assume that 20 distinct documents are randomly stored in these nodes. All users want to obtain these 20 documents.

The simulation is round based. For our network coding based scheme, at the beginning of each round, each user contacts its neighbors to discover whether there are new documents or encoded documents. When new documents are obtained, users encode them according to the operations described in Sec. IV. Once a user can recover all the trust documents, we designate that he has finished, and the number of rounds it takes is called the *finish time*. For the Freenet based scheme, each user sends out a request for one of the documents he does not store. The routing scheme of the requests is described in [9]. Once the requested document is found and sent back, a new request is generated for another document the user does not store. The user stops sending requests once he obtains all documents. Documents are replicated by caching at every node they pass.

We start by comparing the performance of finish time. In Figure 3, we plot the finish time of each node, where the $x$-axis represents the simulation time and the $y$-axis represents the number of nodes that have finished. The performance of the network coding based scheme is better compared to the Freenet based scheme. Because by combining the documents with network coding, within a few rounds, documents can be spread throughout the

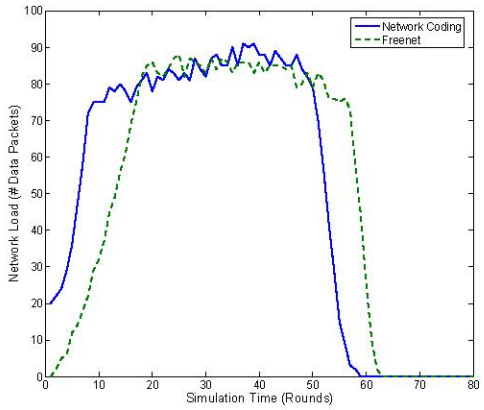



Fig. 4. Network load over time

network. While for the Freenet based scheme, just one document is transmitted per round, and the search phase at the beginning takes long time.

Figure 4 gives the load of the network with time. The total network load of the two schemes is close to each other. While, the network coding based scheme converges much faster than the Freenet based scheme.

## VI. CONCLUSIONS

In this paper, we presented a scheme to distribute trust documents in ad hoc networks based on network coding and ideas from P2P file-sharing systems. The advantages of our scheme are its adaptability to network changes and its efficiency. Our evaluation results show the advantage of our scheme compared to previous schemes.

As future work, we plan to analyze the parameters under different network settings and further explore the influence of mobility and malicious nodes. In this work, we assume that transmissions are perfect. However, in mobile ad hoc networks, transmission failures and errors are very common. It is our future plan to investigate how resilient our scheme is to failures and errors.

## ACKNOWLEDGEMENT

This work is 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 is also supported by the U.S. Army Research Office under grant No DAAD19-01-1-0494.

## REFERENCES

[1] J. Steiner, C. Neuman, and J. I. Schiller, "Kerberos: An authentication service for open network systems," in *USENIX Workshop Proceedings, UNIX Security Workshop*, 1988, pp. 191–200.

[2] V. D. Gligor, S.-W. Luan, and J. Pato, "On inter-realm authentication in large distributed systems," in *Proceedings of the IEEE Conference on Security and Privacy*, 1992, pp. 2–17.

[3] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, "A calculus for access control in distributed systems," *ACM Transactions on Programming Languages and Systems*, vol. 15, no. 4, pp. 706–734, September 1993.

[4] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, "Authentication in distributed systems: Theory and practice," *ACM Transactions on Computer Systems (TOCS)*, vol. 10, no. 4, p. 265 C 310, November 1992.

[5] V. D. Gligor, "Security of emergent properties in ad-hoc networks," in *Proceeding of the Security Protocols Workshop*, Sidney Sussex College, Cambridge, UK, April 2004, pp. 256–266.

[6] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for Internet applications," in *Proceedings of the ACM SIGCOMM '01 Conference*, San Diego, California, August 2001, pp. 149–160.

[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] K. Aberer, "P-Grid: A self-organized access structure for p2p information systems," in *Proceedings of 9th International Conference on Cooperative Information Systems*, 2001, pp. 179–194.

[9] L. Eschenauer, "On trust establishment in mobile ad-hoc networks," Master's thesis, Electrical and Computer Engineering Department, University of Maryland, College Park, 2002.

[10] C. Gkantsidis and P. Rodriguez, "Network coding for large scale content distribution," in *Proceedings of IEEE INFOCOM*, vol. 4, Miami, FL, March 2005, pp. 2235–2245.

[11] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[12] P. Chou, Y. Wu, and K. Jain, "Network coding for the internet," in *Proceedings of IEEE Communication Theory Workshop*, Capri, 2004.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*. Boston, Massachusetts, United States: ACM Press, 2000, pp. 255–265.

[14] Y. Zhang, W. Lee, and Y.-a. Huang, "Intrusion detection techniques for mobile wireless networks," *ACM/Kluwer Wireless Networks Journal (ACM WINET)*, vol. 9, no. 5, pp. 545–556, September 2003.

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

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

[17] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," in *Proceedings of Symposium on Network and Distributed Systems Security (NDSS'02)*, San Diego, California, February 2002.

[18] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proceedings of the 7th International Workshop on Security Protocols*. London, UK: Springer-Verlag, 2000, pp. 172–194.

[19] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The role of trust management in distributed systems security," *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, pp. 185–210, 1999.

[20] 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.

[21] M. K. Reiter and S. G. Stubblebine, "Authentication metric analysis and design," *ACM Transactions on Information and System Security*, vol. 2, no. 2, pp. 138–158, 1999.

[22] R. Levien and A. Aiken, "Attack-resistant trust metrics for public key certification," in *Proceedings of the 7th USENIX Security Symposium*, San Antonio, Texas, January 1998, pp. 229–242.

[23] A. Jøsang, "An algebra for assessing trust in certification chains," in *Proceedings of the Network and Distributed Security Symposium (NDSS)*, 1999.

[24] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in *WiSe '04: Proceedings of the 2004 ACM workshop on Wireless security*. ACM Press, 2004, pp. 1–10.

[25] T. Jiang and J. S. Baras, "Trust evaluation in anarchy: A case study on autonomous networks," in *Proceedings of Infocom*, Barcelona, Spain, April 2006.

[26] IEEE Std 802.11, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," 1999.