Trust Infrastructures for Wireless, Mobile Networks

Mike Burmester
Computer Science Department
Florida State University
Tallahassee, FL 32306-4530

850.644.6410 (voice)
850.644.0058 (fax)

Alec Yasinsac (Contact Author)
Computer Science Department
Florida State University
Tallahassee, FL 32306-4530

850.644.6407 (voice)
850.644.0058 (fax)

Abstract

Trust in ad hoc networks is an open area of research. The ad hoc environment has characteristics that are fundamentally different from fixed networks in a way that makes establishing, recalling, and maintaining trust relationships difficult. The dynamic nature of the network and the heterogeneity of the hosts are two issues that complicate establishing trust.

In this paper, we consider five trust infrastructures that support dynamic networks and detail the properties and qualities of these infrastructures.

Keywords: Mobile networks, public key cryptography, trusted systems, wireless security

Topic area: Computer Security

1 Introduction

Mobile Ad hoc Networks (MANETs) have received significant attention in the past five years [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]. Research to date primarily focused on mechanisms for key exchange, secure message passing, and infrastructure protection particularly secure routing in MANETs. There is little work that addresses the trust policies that these mechanisms would support. That is the focus of this paper; i.e. to classify several categories of trust infrastructures that support dynamic networks like MANETs, and to detail the properties that these models amplify.

Trust models for distributed systems have been examined extensively in the literature [11,12]. MANETs share many of the complexities of more general Internet applications. For example, nodes may be independent in the sense that they have:

1. No prior relationship
2. No common peers
3. No shared proprietary software
4. Different transmission capabilities
5. Different memory capabilities
6. Different processing capabilities
7. Different mobility characteristics
8. Different lifetime properties

Because of the impact of these properties (and many others that we do not list), any comprehensive trust infrastructure must be able to identify salient characteristics of the environment and to adjust to the nature of its participants. Our goal is to identify a set of trust models that addresses many of the characteristics that are important in MANET trust models.

In the following section, we address the categories of characteristics that our models reflect. The following sections detail the models that we propose. We summarize and conclude the paper and address future work in the final sections.

2 Trust Issues

Trust is a highly abstract concept and it is unlikely that any simple definition can comprehensively capture ALL of the nuances of the essence of trust. Thus, we informally define trust as a behavioral expectation of one party toward another. We may view trust from two perspectives:

1. That of a party awarding trust to another party (Do I trust you?), and
2. That of a party gaining the trust of another party (You can trust me).

For the duration of this paper, we speak from the perspective of one party trying to determine how to award trust to another party, unless we specifically indicate otherwise. Thus, define the trust operation => as a directed graph edge, where A => B means that A and B are nodes on a trust graph and A trusts B for some behavior.

To get a better feel for the essential characteristics of trust, we examine a few trust properties. First, trust need not be reflexive, for example, party A may trust party B, but B does not trust A.

Similarly, trust is context driven, e.g. A may trust B for event x, but not for event y. Trust may also be qualitative rather than Boolean (e.g. A may trust B MORE THAN C). Trust relationships may be fixed or dynamic. Dynamic trust relationships best fit the demands of MANETs. Models for dynamic trust must support establishing, changing, permanently revoking trust between parties. Just these properties greatly complicate trust model discussions.

When considering trust relationships, the network environment must also be considered. As with most distributed applications, presence of a Trusted Third Party (TTP) can facilitate some trust issues. Clearly, if two parties (say A and B) unknown to one another both have a two-way trust relationship with the same third party (C), then C can be an effective intermediary for trusted transactions between parties A and B.

Ad hoc networks are void of infrastructure components that would typically be preferred targets as TTPs. Thus, TTPs must be elected or assigned via novel or well known election algorithms defined for this purpose in distributed networks.

Finally, in any stateful trust model, trust must be represented in a persistent structure of some type. Certificates are the de facto standard structures for representing trust relationships that are protected by cryptography. The essence of certificates is that they are portable and bind a key to an entity, thus guaranteeing the authenticity of actions performed with an associated key.

We also propose the use of a token system, where the token protects trust in other, more subtle ways. The difference between certificates and the tokens that we propose may be considered analogous to the relationship between checks and cash. Checks guarantee payment by tying the purchaser to some identifying information (like a certificate), while the value of cash is self contained (like a token). We address use of tokens in Section 4.

3 Establishing Trust Through Observed Behavior

A natural, and maybe the best, way of acquiring trust is through direct observation. At its most fundamental level, trust is a decision, subject to emotions and intuition. In this scenario, personal observation is preferred over second-hand methods because of the hints, nuances, and *feels* that can be garnered. Though feel is not considered in computer trust systems, there are advantages to direct observation.

Not all actions give insight into trustworthiness. The challenge then, is to:

1. Observe trust-related actions
2. Translate the observations into a trust decision

A challenge to trust management systems is that trust relationships need to be constructed before they are exercised. A strength of this model is that it is neighbor-based, thus trusts can be recorded in three dimensional structures and only directly observed actions need be evaluated.

There are four categories of activity that affect trust:

1. Trust-earning actions over time
2. Trust earning actions by count
3. Trust earning actions by magnitude
4. Trust defeating actions

The connotation of these categories is straightforward. The first is that observation of an entity over a long period with no trust violations is a valid confidence builder. Similarly, observing a large number of transactions with all positive trust properties also bolsters confidence. Finally, observations of actions that require more than average confidence (trust with millions of dollars) with no trust violations also lends confidence in the observed entity. As is true with the common rule of thumb, observation of a single dishonest act can offset an otherwise unblemished reputation.

Combinations of the first three allow cautious parties to grant trust frugally. Untrustworthy parties will be challenged to conduct a sufficient quality and quantity of trustworthy actions to gain trust. On the other hand, observation of malicious, reckless, or otherwise unpredictable actions allows reduction or revocation of awarded trust.

4 An Economic Trust Model

The economic opportunity provided by the Internet has driven rapid establishment of many new trust models. Companies like E-Bay, Amazon, and Priceline[1] conduct all of their business with customers that they have no personal relationship or interaction with. Early work on supporting trust models were from the business perspective [13].

[1] www.ebay.com, www.amazon.com, www.priceline.com

Some work has been done more recently to identify models that support cryptographic protection of trust relationships [14]. Zhong et al. propose a token-based trust model, parties accumulate trust transaction-by-transaction. For trust-earning actions, parties are awarded tokens that can be retained and later presented to reflect the earned trust. If additional trust information is gathered, tokens may be revoked or restricted.

This novel approach to trust acquisition has many properties that are well-suited to ad hoc networks. Tokens can be created, awarded, and verified via distributed algorithms, allowing a global aspect to trust decisions. Conversely, if the trust algorithm is well understood, parties that desire to perform malicious acts can become sleepers, behaving perfectly until they acquire sufficient trust to allow successful mischief.

5 Transitive Trust

Transitive trust is a natural model that is implemented in some of the most used security systems [15, 16]. Unfortunately, *caveat emptor* must be our guide, as there are inherent dangers in assuming transitive trust [17]. Most importantly, transitive trust must be explicit, i.e. parties must know that if they place their trust in one party, that they are systematically and automatically placing their trust in other (potentially unknown) parties as well.

We propose a mechanism that captures the essence of a positive trust relationship through transitive trust. Essentially, in this model trust is always acquired transitively, and a fundamental property of the acquisition process is the length of the trust path. Essentially, the further a target is from the source in terms of hops, the lower the awarded trust. By combining them with flow techniques, we can extend this to multi-paths; the larger the number of link-disjoint paths between the source and target, the greater the trust. Finally, there is a minimal amount of trust (i.e. a floor value) that is expected for any trust path.

Notationally, T_{sdj} reflects the trust that a source s awards to a target d. We use the letter h to represent the hop distance between the source and the target, f is the selected trust floor value, and n is the number of disjoint trust paths between s and d. When a trust decision is required, trust is awarded transitively, based on Equation 1.

$$T_{i,j} = \sum_{in}^{i=1} f + \frac{1}{2^{h_i}} \qquad \text{Equation 1}$$

This algorithm guarantees that trust information from parties nearer to the source receives greater credit than information from sources further disconnected. Moreover, it allows the source to establish a minimum amount of trust for each path connecting the source to the destination.

6 Promoting Trust

Trust may be considered a two party relationship or there may be environments where nodes take on a group trust properties, as in the famous Bell and LaPadula model [18]. One way to form trust management functionality is to establish a trust promotion system. In [19], the authors give a mechanism for implementing trust promotion, but do not detail the reflected trust model. We highlight that model in this section.

Consider the simple environment shown in Figure 1 where all nodes can be categorized into the following five groups (from most to least trusted):

1. Highly trusted
2. Trusted
3. Unknown
4. Untrusted
5. Highly untrusted

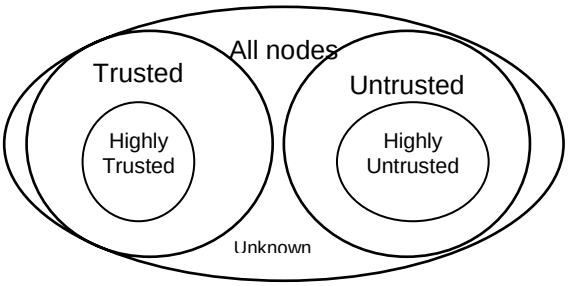

Figure 1

We can then establish rules for promoting and demoting members between groups. These rule sets will be identified by the desired promotion rule (e.g. 3 -> 2). If promotion is not allowed for highly untrusted parties, no rule set is established with user class 5 as the source.

The model is further naturally extended to designate a subset of class 1 and 2 groups as "promoters". These promoters are responsible for determining if requestors meet the promotion requirements as designated in the promotion rules and in taking action to effect the justified group movement. While promotion is requested directly, demotion must be requested second hand.

The strength of this model is that promotion and demotion decisions are local and responsible parties are elected through clearly designed, fair algorithms. This distributed approach can support even highly dynamic networks.

7 Secured Trust

The final model that we propose is a type of financial model. Specifically, the central party in the model is a trusted third party that guarantees the trust level of a party. Similar to secured loans, if the guaranteed trust is violated, the guarantor will deliver the promised security to the offended party.

Secured trust is a pure form of transitive trust. It is unique in that trees are limited to one hop relationships and that the trust is secured by a value that is contractually agreed. As with secured financial interactions, the secured value may take many forms, including the following:

1. Co-signed trust certificate
2. Trust Insurance policy
3. Trust bond
4. Trust collateral

These procedures correspond to similar models in the financial world. For a co-signed certificate, the co-signing party would have credentials that exceed those of the target and would assume liability for any adverse events that occur as a result of a trust breech.

The insurance model is similar, except that the security is provided by a well-recognized organization that promises benefits to the executor of the policy.

The last two models are similar in that the trust target provides the value that secures the trust. The value can be monetary, property, or other item or issue of suitable value to the source.

8 Conclusions

In this paper, we provide several models for managing trust in ad hoc networks. The models that we present address many of the properties that make trust establishment in ad hoc networks difficult. These models are highly distributed and allow dynamic trust establishment, revocation, and management. The models that we propose support reasoning in multi-level trust environments and distinguish between local and global trust considerations.

This collection of trust models reflects novel properties and views of transitive trust relationships. We capture the relevance of transitive trust paths through distance-relative trust quantification.

9 Future Work

This work reflects a first attempt to define trust models supporting ad hoc networks. Clearly, this paper is preliminary. We envision developing linear, or more generally, partially ordered metrics to support specific environments and rules of thumb to guide model development for ad hoc networks. Based on these models, we will prove the security properties that the developed systems exhibit.

10 References

[1] Guisseppe Ateniese, Michael Steiner, Gene Tsudik, "New Multi-party Authentication Services and Key Agreement Protocols", IEEE Journal of Selected Areas in Communications, Vol. 18, No. 4, Apr 2000, pp. 1-13

[2] Michael Steiner, Gene Tsudik, and Michael Waidner, Key Agreement in Dynamic Peer Groups", IEEE Transactions on Parallel and Distributed Systems, Vol. 1, No. 8, Aug 2000, pp 769-80

[3] L. Zhou and Z.J. Haas, Securing Ad Hoc Networks, *IEEE Network Magazine, vol. 13, no.6*, December 1999.

[4] Aram, Khalili, Jonathan Katz, and William A. Arbaugh, "Toward Secure Key Distribution in Truly Ad-Hoc Networks", IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003

[5] S. Corson and J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, RFC2501, January 1999.

[6] C. Perkins and E. Royer, Ad hoc On-Demand Distance Vector Routing, *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, USA 1999, 90-100.

[7] D. Johnson, D. Maltz, J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-hop Wireless Ad Hoc Networks," Ad Hoc Networking 2001, pp. 139-172.

[8] C.E. Perkins and E.M. Royer, "Ad hoc on-demand distance vector routing," *In 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, February 1999

[9] Papadimitratos and Z.J. Haas, Secure Routing for Mobile Ad hoc Networks, *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, San Antonio, USA, 2002.

[10] J. Marshall, V. Thakur, and A. Yasinsac, "Identifying Flaws in the Secure Routing Protocol", Proceedings of The 22nd International Performance, Computing, and Communications Conference (IPCCC 2003) April 9-11, 2003, pp. 167-174

[11] Grandison, T. and Sloan, M., "A Survey of Trust in Internet Applications", IEEE Communications Surveys, 4th Quarter, 2000

[12] M. Blaze, J. Feigenbaum, and J. Lacy: "Decentralized trust management". In

Proceedings of the 1996 IEEE Symposium on Security and Privacy, pp.164-173, May 1996.

[13] Harold Pardue, "A Trust-based Model of Consumer-to-consumer Online Auctions*",* *The Arrowhead Journal of Busines*s, pp. 69-77

[14] Sheng Zhong, Jiang Chen, and Richard Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks", In *Proceedings of INFOCOM 2003*

[15] Phil Zimmermann, "The Official PGP User's Guide", Cambridge, MA.: MIT Press, 1995 (second printing).

[16] J. Steiner, C. Neuman, and J.I. Schiller, ‘‘Kerberos: An Authentication Service for Open Network Systems,’’ in *Proc. Winter USENIX Conferenc*e, , Dallas (1988)

[17] Bruce Christianson and William S. Harbison, "Why Isn't Trust Transitive", Proceedings of the 4th International Workshop on Security Protocols", LNCS, pp. 171 - 176 , 1996

[18] D. E. Bell and L. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model, M74-244, MITRE Corp. Bedford, MA, 1973

[19] Michael Burmester and Alec Yasinsac, "Protocols for a Dynamic Key Exchange System for Ad Hoc Networks", The Eleventh International Workshop on Security Protocols, Cambridge, UK, Apr 2-4, 2003, LNCS