Protocols for Supporting a Public Key Infrastructure in Ad Hoc Networks*

Mike Burmester and Alec Yasinsac

Department of Computer Science, Florida State University,
Tallahassee, Florida 32306-4530, U.S.A.
{burmester,yasinsac}@cs.fsu.edu

Abstract. Ad hoc networking technologies allow mobile devices to communicate by utilizing one another as communication relays. Resulting networks are highly dynamic, with nodes entering and leaving the network, for short duration membership. This absence of structure complicates planning in these networks, resulting in networks with limited functionality when their topology (their nodes and links) has highly varying and unpredictable characteristics.
We propose protocols for a Public Key Infrastructre (PKI) suitable for ad hoc networks that are based on threshold cryptography technology, adapted to general access structures.
Keywords: Ad hoc networks, security, access structures, threshold cryptography

1 Levels of trust in ad hoc networks

Ad hoc networking techniques allow mobile devices to communicate among themselves by utilizing one another as communications relays. These networks have no fixed infrastructure and are highly dynamic. The absence of structure complicates and limits planning for these networks, potentially resulting in networks with limited functionality when their nodes and links have highly varying and unpredictable characteristics. As a simple illustration, message delivery is unreliable, even unlikely, if the communication latency is greater than the node lifetime within the network [19].

One essential limitation that befalls structure-less and structure-starved networks is the inability to establish a cryptographically secure Public Key Infrastructure (PKI). As a result, there is presently little theoretical foundation for securing these networks. In this paper, we propose a group PKI for ad hoc networks that is based on threshold cryptography techniques for appropriate access structures.

As we alluded to earlier, ad hoc networks are dynamically formed with no fixed structure. Traditionally, tacit structural assumptions allowed reasoning about such networks. The most common targets for structure are assumptions

* This material is based on work supported in part by the U.S. Army Research Laboratory and the U.S. Army Research Office under grant number DAAD 19-02-0235.

about the properties of the network nodes. For example, any dynamic (reactive) routing algorithm must assume that the lifetime of the route to destination node is longer than the duration of the routing algorithm itself, otherwise the target node cannot be reached before the route is established. However, this assumption is rarely stated. Research in ad hoc networks varies greatly because no broad classification of such networks exists. However, there are a great many de facto assumptions that guide much of the ongoing work. These often-overlooked assumptions presume unproven minimum node and path lifetime and ill-founded minimum and maximum network density and size bounds.

2 Public Key Infrastructures

Modern cryptography is based on three milestone technological advances:

1. Establishment of strong symmetric key encryption schemes [18, 14]
2. Creation of Public Key Cryptography [9, 16]
3. Introduction of secure Key Exchange Protocols [15]

Unfortunately, none of these technologies resolves the classic key distribution problem for dynamic networks with no fixed infrastructure. Solutions such as Kerberos key distribution [1] and the proposed solutions for Public Key Infrastructures [21] rely on significant fixed, or slowly evolving [4], infrastructures and require substantial associated set-up overhead. Such key exchange solutions are not appropriate for ad hoc networks.

More recently, flexible PKIs have been proposed for the ad hoc environment [22, 13]. These methods are more suitable to dynamic networks than their predecessors in that they can support dynamic reconfiguration, yet they assume a substantial amount of synchronization between the nodes. Such overhead is highly undesirable in ad hoc networks.

2.1 Threshold cryptography

Threshold cryptography has been proposed [5, 7] as a mechanism to distribute the power to perform Public Key Cryptography operations, for example, to digitally sign or encrypt data. Parties are issued shares of a secret key and use these to execute the cryptographic application in a distributed way. For each application, in their computations, the parties learn no more about the cryptographic operation than is strictly necessary to execute the application. For a successful execution, a threshold of the parties is needed.

2.2 Adapting threshold-based systems

An important question for any ad hoc service is how the service is able to perform under periods of rapid change. In our case, the question is how the system will continue operations if the original operating properties that established the

threshold parameters become unworkable due to normally dynamic activity in the network. For example, what happens if a number of key certifiers leave the group, resulting in fewer than the threshold number of key certifiers?

A more challenging (and possibly more interesting) problem occurs when the size of the network increases so much that the key certifiers become bottlenecks, i.e. they are not able to handle the volume of key requests generated in the network. In such a case, we would like to be able to modify a t-of-n threshold cryptosystem to a t'-of-n' system.

The obvious solution is to reform the network with new parameters and new key certifiers. Alternatively, we prefer to extend the existing structure if we can do so in a way that minimizes the overhead. Adaptive threshold schemes have been proposed to modify threshold secret sharing schemes [10, 8] but these are highly complex and require synchronization among the members that is difficult or impossible to accomplish in ad hoc networks. That is, for these schemes to work, the key certifiers must know that the scheme has changed and what the details of the change are.

2.3 Threshold cryptographic operations

The foundation of threshold cryptography [6] is that a threshold of participants is able to accomplish a designated cryptographic operation. More specifically, if n is the number of participants and t is the threshold, a (t, n)-threshold cryptographic scheme allows any t or more qualified participants to execute the operation. A threshold access structure, denoted by Γ, defines the qualified sets of participants that are able to execute the cryptographic threshold operation. For example, if G is a set with the three qualified participants a, b, and c, in a (2,3) threshold scheme, then $\Gamma(G) = \{(a, b), (a, c), (b, c), (a, b, c)\}$.

Most cryptographic applications involve (t, n)-threshold access structures. However, general access structures [2] reflect a variety of properties of ad hoc network nodes. We use the term "general" to reflect any monotone access structure, with or without the threshold limitation. For example,

$$\Gamma(G') = \{\{a\}, \{b, c, d\}, \{e, f\}, \text{ and all supersets of these}\}$$

is a general access structure for the set of participants $G' = \{a, b, c, d, e, f\}$. We shall also use the notation Γ_0 to denote minimal access structures. For the earlier example,

$$\Gamma_0(G') = \{\{a\}, \{b, c, d\}, \{e, f\}\}$$

is a minimal access structure of Γ.

Notice that we can also identify the maximal unauthorized sets of Γ, as

$$B_0 = \{\{b, d, e\}, \{b, d, f\}, \{b, c, e\}, \{b, c, f\}, \{d, c, e\}, \{d, c, f\}\}.$$

Here, maximal means that all unauthorized sets are characterized without redundancy. That is, for $0 < i \neq j \leq n = |B_0|$, no B_i is a subset of B_j for any two

elements in B_0, since all subsets of unauthorized sets are necessarily unauthorized, thus are redundant. The notion of maximal unauthorized sets is essential to our construction in section 3.2.

In the next section we show how a general access structure is ideally suited to model security infrastructure aspects of ad hoc networks.

3 Access structures for key certification in ad hoc networks

In order to systematically accomplish any security goals, we must agree on some representative characteristics of the network nodes and links. While distributed methods prefer to rely on similar or homogeneous nodes, often, in heterogeneous applications, some nodes have more authority or trust placed in them than others in order to accomplish one or more group-oriented tasks. A node that acts as a key certifier reflects this property, requiring additional functionality and, in some sense, more authority than other nodes in the network.

In our model, the key certifier is not a single node; but rather is a group of nodes that jointly accomplish key certification for the group. This induces, in a natural way, an access structure on the nodes of the network.

It may also be the case that some key certifiers have more authority than others, essentially, that they are *more trusted*. The crux of this section is that trust levels can be reflected by implementation of threshold cryptography techniques employed against general access structures. Specifically, less trusted key certifiers may be paired with more trusted key certifiers in their respective qualified certification groups, while more trusted key certifiers may form small (or exclusive) certification groups with the same authority.

3.1 The overarching architecture

Utilizing certificates for group membership results in a natural partitioning of all possible communicating nodes into two categories, each with two sub-categories:

1. Outsiders
   (a) Uninterested nodes that never intend to join the group, but may be in the group communication reach [20].
   (b) Non-group members that may have desire and capability to join the group.
2. Insiders
   (a) Group members.
   (b) Key Certifiers. These trusted group members, in appropriate certification sets of the access structure, act as a group membership certifier.

We acknowledge the first of these as potential intruders, but since they will *always* be outsiders, we claim that the normal PKI characteristics should protect against them, thus we are otherwise uninterested in them. We claim that the

primary role of a dynamic PKI is to robustly and securely utilize key certifiers to promote members from outsiders to group members, and to revoke them. As we noted earlier, there are many PKI schemes proposed for that purpose for non-dynamic models. The problem that we address is that of protecting the group from dishonest key certifiers, similarly to that presented in [13], but we go beyond with a novel mechanism that supports the dynamic nature of ad hoc networks.

Two main contributions of our scheme are that:

a. It is based on general access structures
b. That it can be adapted in simple way that corresponds directly to the needs in ad hoc networks.

Thus, our focus is on key certifiers. Our scheme is expandable [8, 10, 11], and has the added advantage that it allows key certifiers to be granted different trust levels.

As an example, consider a network with $n = 5$ key certifier nodes $\{n_1, n_2, n_3, n_4, n_5\}$, where any $t = 3$ nodes collectively act as the key certifier, or are considered key certifier participants. A standard threshold scheme [17, 2, 5] grants all triples of key certifier participants equal trust, by allowing them to collaborate to sign as the key certifier. Hence, each key certifier has one third of the signing power. General access structures allow nodes to be granted varying degrees of trust. For example, n_1 may be sufficiently trusted that it alone is allowed to promote nodes from outsiders to group membership by granting them a public key certificate, while nodes n_2 and n_3 are required to collaborate in order to issue a new certificate, and nodes n_4 and n_5 may be required to join together with n_3 to promote nodes to group membership. The minimal access structure for this arrangement is defined by:

$$\Gamma_0 = \{\{n_1\}, \{n_2, n_3\}, \{n_3, n_4, n_5\}\}$$

With this structure, outsiders have three options for achieving promotion to group membership by convincing each member of one of the three qualified certifying sets.

3.2 A threshold certification scheme for general access structures

Mapping general access structures to threshold structures. As a starting point for our scheme, we use any access structure Γ for the qualified certifying sets. Then, we map Γ to a threshold structure Γ^* using the approach in Ito [12], or an approach similar to Horng [11]. The first reduction is rather inefficient, with the realized scheme being an (n, n)-threshold scheme for relative large n. The latter is more efficient giving a (k, n)-threshold scheme with smaller values of k and n.

As threshold structure, we propose to use an RSA threshold signature scheme [6].

An Illustration. Consider the network consisting of four key certifier participants $C = \{1,2,3,4\}$. Given the access structure $\Gamma_0(C) = \{(1,3),(2,4)\}$, then $B_0 = \{(1,2),(1,4),(2,3),(3,4)\}$. Since $|B_0| = 4$, by Ito, et al [12], Γ can be mapped to a (4,4) threshold access structure Γ^*.

We must select RSA parameters: p, q primes with $|p| = |q|$, $n = pq$, and $d, e \in Z_{\phi(n)}$, with $\phi(n) = (p-1)(q-1)$ and $d \cdot e = 1 \pmod{\phi(n)}$. Then,

- $\mathrm{sig}_C(m) = h(m)^d \pmod{n}$ and,
- $\mathrm{ver}_C(\mathrm{sig}_C(m)) = 1$ iff $h(m) = \mathrm{sig}(m)^e \pmod{n}$,

for a suitable hash function h.
Thus, we must select Γ^*-shares d_{ij} such that $x^{d_{1,2}} \cdot x^{d_{1,4}} \cdot x^{d_{2,3}} \cdot x^{d_{3,4}} = x \pmod{n}$, and such that the holders cannot learn anything about the factorization of n. These shares can be generated using the algorithm given in [3] by Boneh and Franklin. We map the Γ^*-shares to Γ-shares by selecting the members of the sets in the access structure as in Ito, et al. [12], to jointly interact with the Boneh/Franklin RSA generation algorithm.

Specifically, members 1 and 2 corresponding to $(1,2) \in B_0$ collaborate to act as virtual user U_1; members 1 and 4 corresponding to $(1,4) \in B_0$ collaborate to act as virtual user U_2; members 2 and 3 corresponding to $(2,3) \in B_0$ collaborate to act as virtual user U_3; members 3 and 4 corresponding to $(3,4) \in B_0$ collaborate to act as virtual user U_4. The shares $d_{i,j}$ are produced directly from the input contributed by the corresponding U_i virtual user.

We now distribute to each key certifier U_i, $i = 1,2,3,4$ a Γ-share, s_i whose shadows are comprised of shares from the Γ^* scheme as:

$$\begin{array}{lll} U_1: & s_1 = (d_{2,3}, d_{3,4}) & \text{(exclude 1)} \\ U_2: & s_2 = (d_{1,4}, d_{3,4}) & \text{(exclude 2)} \\ U_3: & s_3 = (d_{1,2}, d_{1,4}) & \text{(exclude 3)} \\ U_4: & s_4 = (d_{1,2}, d_{2,3}) & \text{(exclude 4)} \end{array}$$

Notice that with this distribution, U_1 and U_3 jointly possess each of the four shares necessary to sign in the Γ^* (4,4)-threshold scheme, as do U_2 and U_4, as is required in the given access structure $\Gamma_0(C)$.

We note that distributed RSA computation is complex and expensive. Even though this computation need only be conducted one time, for the sake of efficiency, our key certification scheme may be implemented by having a trusted member generate and distribute the shares of the RSA key scheme.

3.3 Extending the certification scheme

Because of the nature of ad hoc networks, as nodes enter or leave the network, qualified certifier sets C belonging to Γ will evolve, eventually reducing to sets C' that are not qualified C^* (not in Γ). If this is the case with all such sets C in Γ, then there will remain no qualified certifying sets in the network.

To maintain the operational capability of the certifying nodes, Γ must be able to evolve dynamically to address the ad hoc nature of the network. This evolution must be proactive, in the sense that it must protect the access structure

from proactive threshold attacks [10]. For this purpose, we propose to combine the methodologies of Horng [11] and Frankel , et al [10].

Should a key server desire to distribute share, say d_1, to users 5 and 6, he would construct shares $d_{1,5}, d_{1,6}$ such that: $x^{d_{1,5}} \cdot x^{d_{1,6}} = x^{d_1} \pmod{n}$. To do this, he would select at random with uniform distribution[1] the share $d_{1,5} \in Z_n$. He would then compute $d_{1,6} = d_1 - d_{1,5}$ and issue share $d_{1,5}$ to user 5 and $d_{1,6}$ to user 6. Now, members 5 and 6 can jointly act as key server 1, essentially where any computation using d_1 is required.

3.4 Node demotion

Group membership revocation. In our scheme, demotion occurs via certificate revocation. There are many mechanisms proposed for this purpose, with certificate revocation lists being the most common. We submit that the short-lived nature of ad hoc networks will result in very few such revocations. While revocation lists will be flooded, the overhead will be low because there will be relatively few revocations resulting in short lists, infrequently transmitted.

Key certifier demotion. Our model reflects the advanced trust placed in key certifiers via the selected access structure. For this reason, the need for key certifier demotion will be minimized. In the case where key certifier demotion is necessary, we recognize that our scheme is a distributed construction. Thus, we propose that key certifiers may issue certifier revocation lists that blacklist malicious certifiers, effectively demoting them by removing all certifying access sets that contain that member from the access structure Γ.

4 Conclusion

The classic problem of secure and efficient key exchange continues to challenge security researchers. Advances in this area tend to be incremental, seemingly with one step backward for each two (or fewer) steps forward. The problem is further exacerbated in ad hoc networks, where the structure leveraged in many of the incremental advances in key exchange is necessarily unavailable. In this paper, we propose utilizing threshold cryptographic techniques for a key exchange system for ad hoc networks. Due to the nature of ad hoc networks, only distributed services are suitable, and other key exchange infrastructures have been suggested. Our system has two primary distinguishing characteristics:

1. It is extendible, allowing modification on the fly, as the network changes
2. It enables systematic implementation of authority levels.

[1] The distribution $\mathcal{D}^*_{\phi(n)}$ induced on $Z_{\phi(n)}$ by this selection is ε-statistically indistinguishable from the uniform distribution $\mathcal{D}_{\phi(n)}$, where $\varepsilon = \mathcal{O}(2^{-|n|/2})$. Indeed: $\frac{1}{2}\sum_{n-\phi(n)} |\frac{2}{n} - \frac{1}{\phi(n)}| + \frac{1}{2}\sum_{\phi(n)-(n-\phi(n))} |\frac{1}{n} - \frac{1}{\phi(n)}| < \frac{(2\phi(n)-n)(n-\phi(n))}{n\phi(n)} < \frac{(n-4\cdot 2^{|n|/2})\cdot 3\cdot 2^{|n|/2}}{2^{|n|}(n-2\cdot 2^{|n|/2})} = \mathcal{O}(2^{-|n|/2})$, when $|p| = |q|$.

5 Acknowledgements

We would like to thank N. Asokan and Le-Van Tri for helpful comments.

References

1. S.M. Bellovin and M. Merritt. Limitations of the kerberos authentication system. *Computer Communications Review*, October 1990.
2. G.R. Blakley. Safeguarding cryptographic keys. *in Proceedings of the National Computer Conference, FIPS Conf.erence Proceedings*, 48:313–317, 1979.
3. D. Boneh and M. Franklin. Efficient generation of shared rsa keys. *In B.S. Kaliski Jr., editor, Advances in Cryptology, CRYPTO '97*, Volume 1294 of Lecture Notes in Computer Science:425–39, Springer-Verlag, 1997.
4. M. Burmester and Y.G. Desmedt. Secure communication in an unknown network using certificates. *Advances in Cryptology - Asiacrypt '99, Lecture Notes in Computer Science 1716, Springer, Berlin*, pp. 274–287, 1999.
5. Y. Desmedt and Y. Frankel. Threshold cryptosystems. *In Crypto 89, Springer-Verlag Lecture Notes in Computer Science*, 435:307–315, 1990.
6. Y.G. Desmedt. Threshold cryptography. *European Trans. on Telecommunications*, 5(4):449–457, July-August 1994.
7. Y. Desmedt. Some recent research aspects of threshold cryptography. *In Proc. of the 1st Intl. Information Security Workshop*, pp. 158–173, 1997.
8. Y. Desmedt and S. Jajodia. Redistributing secret shares to new access structures and its applications. *Technical Report ISSE TR-97-01*, George Mason University, July 1997.
9. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976.
10. Y. Frankel, P. Gemmel, P. MacKenzie, and M. Yung. Optimal resilience proactive public-key cryptosystems. *In Proceedings of the* 38th *Symposium on Foundations of Computer Science*, 1997.
11. G. Horng. A new method for constructing multiple assignment schemes for generalized secret sharing. *Journal of Information Science and Engineering*, 17:959–965, 2001.
12. M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing any access structure. *Proceedings of IEEE Globecom '87*, pp 99–102, 1987.
13. A. Khalili, J. Katz, and W.A. Arbaugh. Toward secure key distribution in truly ad-hoc networks. *IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet*, Orlando, FL, January 28, 2003.
14. National Bureau of Standards (NBS). *Data Encryption Standard.* Federal Information Processing Standard, Publication 46, NBS, Washington, D.C., January 1977.
15. R.M. Needham and M.D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, Vol. 21(12):993–999, December 1978.
16. R.L. Rivest, A, Shamir, and L.M. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, Vol. 21(2):120–126, February 1978.

17. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, November 1979.
18. C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.
19. A. Yasinsac. Rates of Change in Ad Hoc Networks. To appear in the Proceedings of the Information Resources Management Association International Conference (IRMA2003), Philadelphia, PA, May 18–21, 2003.
20. A.Yasinsac and J.A. Davis. Modeling protocols for secure group communication in adhoc networks. *Tenth International Workshop on Security Protocols*, Cambridge, UK, Apr 17–19, 2002, LNCS.
21. P. Zimmermann. *The Official PGP User's Guide*. MIT Press, Cambridge, MA., 1995 (second printing).
22. L. Zhou and Z.J. Haas. Securing ad hoc networks. *IEEE Network Magazine*, 13(6):24–30, Nov./Dec. 1999.