Securing Authentication and Privacy in Ad hoc Partitioned Networks

Sankar Kaliaperumal*
Computer Science Department
Florida State University
kaliaper@cs.fsu.edu

Abstract

Security is a major concern in the design of modern communication systems. It is particularly challenging with wireless networks such as ad hoc networks. Ad hoc Networks are dynamically reconfigured. For this reason they are vulnerable to several major security threats.

This paper focuses on authentication and privacy in partitioned ad hoc networks. We consider the problem of managing revocation lists and discuss privacy issues.

1. Introduction

Ad hoc networks [5, 15] do not have a fixed network topology. Nodes are mobile and can communicate with each other while in range, but otherwise are disconnected. This node mobility causes frequent changes of the network topology, and possible partitioning. Ad hoc networks can be used to model several wireless applications, such as military operations in which the nodes are military units (soldiers, tanks and other vehicles, planes, etc.) equipped with wireless communication devices and more generally wireless communication system in which the fixed network is restricted. The restructuring of such networks is usually due to their mobility; however, it can also be caused by the enemy. The enemy can destroy captured devices try to use them to gather information or undermine the operations.

The traditional model for static networks with Byzantine faults [7] may be used to describe some of the security threats of ad hoc networks, but what characterizes ad hoc networks is that their structure changes continuously. Furthermore, the tools which are used to establish the security (authentication, confidentiality, integrity, availability and non-repudiation) of traditional networks cannot in general be easily adapted for the requirements of ad hoc networks, particularly when these get partitioned. Such issues must be addressed in order to secure ad hoc networks.

*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 DAAD19-02-1-0235.

2 Authentication in Ad hoc Networks

Ad hoc networks use wireless data transmission. This makes them susceptible to *passive* attacks (eavesdropping) and *active* attacks (message replay, message substitution, impersonation, Denial of Service attacks, etc). Mobile nodes usually have low physical security. For example in the battlefield they can be easily captured or compromised. We also have *insider* attacks. In the Byzantine threat model such attacks can be directed to both the nodes and the controlling authorities (for example, a penetrated controlling authority may authorize nodes under the control of the adversary). Consequently, a centrally controlled trust infrastructure managed by a single Certification Service is a single point of failure. We therefore must use a distributed Certification Service in which the trust is managed by several authorities. The traditional approach is to use threshold cryptography [6]. This approach can be extended by using the proactive techniques proposed by Frankel, Gemmel, Mackenzie and Yung [11, 12]. These improve the robustness of the network system by allowing periodic public key updates [14]. Such an approach is used by Zhou and Haas [20] and by Luo, Zerfos, Kong, Lu and Zhang [17].

However with this approach one has to assume that every node of the network has two-way access to a (distributed) Certification Service, which manages the public key infrastructure. This may not be always possible for a network which gets partitioned in an ad hoc way. Several other approaches have been used [16, 18, 19], but all rely on the availability of a centrally managed Certification Service.

3 The Communication Graph: Partitions

The communication graph of an ad hoc network consists of the nodes of the network and links which corresponds to direct (one-hop) communication links. Communication between any two nodes A and B is only possible if there

Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w'03)
0-7695-1873-7/03 $17.00 © 2003 IEEE

is a (multi-hop) path which links A to B. Any two nodes can communicate if the communication graph is connected. The problem with ad hoc network is that their communication graph is continuously reconfigured, and may become disconnected. Disconnected graphs are partitioned graphs for which communication is restricted to the (connected) partitions.

4 Authenticated Ad hoc Partitions

There are several Public Key Infrastructure (PKI) models that can be used to describe non-centralized trust management systems. For an ad hoc partition, with possible Byzantine faults, it is clear that no single node can be trusted with the management of an authentication infrastructure. In our protocol, it is therefore entrusted to the partition itself. Whatever infrastructure is used, it is important that it allows regular key updates, so as to address issues such as key revocation, key compromise, key expiration, etc. Since the partitions are disconnected this has to be restricted to the partitions, if there is no access to the Certification Service.

4.1 Model

We use a Byzantine threat model [7] in which the number of faulty nodes is bounded by *k*. We shall assume that each node of U has a secret/public key pair (SK_U, PK_U) which is certified by a (possibly distributed) Certification Service. These keys will be used to authenticate communication. The communication will be via multi-hop paths in the communication graph N. We shall assume that N is partitioned and that at time *t*, $N = \cup {P_i}^t$, where ${P_i}^t$ are its partitions. All nodes will have one-way access to the Certification Service so that they can access certificate lists.

4.2 A Partition Authentication Protocol

Since the certificate list is managed by the Certification Service and all the nodes can access it, we are only concerned with revocation in partitions, which cannot be forwarded to the Certification Service in our model. Revocation lists have to be available in all partitions with faulty nodes, otherwise the faults will be uncontrollable. We also need sufficient connectivity in each partition to guarantee secure communication. A Revocation Certificate for the public key PK_{U^*} of a faulty node U^* is a multi-signature [2] certificate:

$$msig_{PK_{U_1}, PK_{U_2}, \ldots, PK_{U_{k+1}}}(PK_{U^*}, revoke),$$

where $U_1, U_2, \ldots, U_{k+1}$ are nodes of the network. In such a certificate, $(k+1)$ nodes revoke the certificate of node U^*. Because of our bound k on the number of faulty nodes, $(k+1)$ certificates are sufficient to prevent faulty nodes from framing a non-faulty node.

We shall make the following assumptions:

- *Maintaining revocation lists in partitions*:
  If the certificate of the nodes $U_1^*, U_2^*, \ldots, U_s^*$ is revoked in a partition ${P_i}^t$, then for all partitions ${P_j}^{t'}$ with $t' > t$, we require that:

  $$either\ {P_i}^t \cap {P_j}^{t'} = \emptyset \quad or\ |{P_i}^t \cap {P_j}^{t'}| \geq k+1.$$

  This condition guarantees that if s faulty nodes $U_1^*, U_2^*, \ldots, U_s^*$ migrate to ${P_j}^{t'}$ (along with up to $k-s$ possibly undetected faulty nodes) there will always be at least one non-faulty node to pass on the revocation lists.

- *Reliable communication*:
  Each partition ${P_i}^t$ with revocation lists for *s* nodes is at least $2(k-s)+1$ connected. This is needed to prevent Denial of Service attacks by the faulty nodes.

5 Privacy

Although we have not discussed privacy, it is easy to establish it by using appropriate cryptographic tools (for example, the Diffie-Hellman Key exchange [8]). However, there is still a traceability problem. The adversary can monitor the communication traffic in the partitions and obtain useful information. This is particularly important in military applications.

In this section we consider an authentication protocol in which nodes are assigned ID's, which are then used to certify secret/public authentication keys. These keys are linked to the identity (ID) of the user.

5.1 Registration

Each node *U* of the ad hoc network is first assigned a long term secret/public identity pair: $(ID_{U,sec}, ID_{U,pub})$ by a Certification Service. This pair is determined by a one-way cryptographic trapdoor function *f*. $ID_{U,pub}$ is a binary string that identifies the node *U*. For example it contains a physical description of *U*, a serial number, the date of manufacture, etc. $ID_{U,sec}$ is determined by using the trapdoor of f: $ID_{U,pub} = f(ID_{U,sec})$. There are several trapdoor one-way functions that may be used for this purpose. We propose the Feige-Fiat-Shamir [9] identification scheme in which $ID_{U,sec}$ is the quadratic residue of $ID_{U,pub}$ modulo a composite number *n*, i.e. $ID_{U,pub} = (ID_{U,sec})^2 \bmod n$, where $n = pq$, with p, q primes. The prime factors of n are the trapdoor and are used to determine the quadratic residue $ID_{U,sec}$. With this identification system, finding pairs of

Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w'03)
0-7695-1873-7/03 $17.00 © 2003 IEEE

numbers x, y for which $y = x^2 \bmod n$, and for which y has the proper format, is as hard as factoring. Although for many applications the Certification Service is one entity, if required (for security reasons) we can distribute it's functionality using threshold cryptography techniques [6].

The lifespan of the long-term secret/public identity pair ($ID_{U,sec}$, $ID_{U,pub}$) will be that of the system. This means that the identification process must not expose any knowledge about the secret key. For this purpose we use the Feige-Fiat-Shamir *interactive identification proof system of knowledge* [9]. Interactive Proof systems leak no knowledge other than one bit: the truth (or falsehood) of the statement in consideration. There are several variants one may wish to consider. For example, the Fiat-Shamir [10] signature scheme (a non-interactive proof which leaks minimal knowledge) or the Burmester-Desmedt [3] broadcast interactive proof system which is a multiple verifier proof system.

We shall assume that the long-term secret/public identity pair ($ID_{U,sec}$, $ID_{U,pub}$) is stored on a tamper-resistant device which is attached to the node in a tamper-resistant way. The adversary cannot detach this from its device and use it on another device without destroying it (i.e. we require that the identity of a node cannot be detached from that node).

5.2 A Partitioned Authentication Protocol

Each node *U* in the partition first chooses an updated secret/public key pair (SK_U, PK_U) and then proves to all its neighbors that PK_U is it's chosen public key, by linking it to its identity $ID_{U,pub}$. This can be achieved by using a zero knowledge proof system of knowledge of both $ID_{U,sec}$ and SK_U. We may use the Fiat-Shamir signature scheme [10] (in this case security is proven in the Random oracle model by Bellare and Rogaway [1]), or a variant of the broadcast interactive proof system by Burmester-Desmedt [3]. Once the local neighborhood infrastructure is established, the partition infrastructure can be determined by using the Burmester-Desmedt unknown networks protocol [4]. The security of this protocol depends on the number of faulty nodes *t*. If *k* is bound on the number of faults, the security of the network is proven [4] provided the partition is $(2k + 1)$ connected and $t \leq k$. Security is reduced to that of identification scheme and the signature scheme.

6 Concluding Remarks and Open Problems

We have considered the problem of securing ad hoc networks in the general case when the network is partitioned. With large networks, scalability is a major concern. To establish the structure (graph) of a partition we can use the method proposed in the Burmester-Desmedt unknown networks protocol [4]. Each node, Round Robin floods an authenticated query:

Who is there? send me a list of your neighbors.

Round Robin is used to prevent Denial of Service attacks. The graph is then easily determined. Nodes communicate via $(2k + 1)$ vertice-disjoint paths. However, this protocol is not very efficient.

Open Problems

- Find efficient ways to establish the structure of the partition.
- Extend the unknown network protocol for proactive security.

Acknowledgment

I would like to thank Dr. Mike Burmester for his comments and suggestions which helped to improve the quality of the article.

References

[1] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. *First Annual Conference on Computer and Communications Security*, pp 62–73, 1993.

[2] C. Boyd. Digital multisignatures. *IMA Conference on Cryptography and Coding, H. Baker and F.C. Piper, Claredon Press*, pp 241–246, 1986.

[3] M. Burmester and Y. Desmedt. Broadcast interactive proofs. *Eurocrypt 91, Lecture Notes in Computer Science 547, D.W. Davies , Springer-Verlag*, pp 81–95, 1991.

[4] M. Burmester and Y. 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] R.L. Davies, R.M. Watson, A. Munroe and M. Barton. Adhoc wireless networking contention free multiple access. *Proceedings of 5th IEEE conference on Telecommunications*, pp 73–77, 1995.

[6] Y. G. Desmedt. Threshold cryptography. *European Transactions on Telecommunications*, 5(4):449–457, 1994.

[7] D. Dolev, C. Dwork, O. Waarts and M. Yung. Perfectly secure message transmission. *Journal of the ACM*, 40(1):17–47, 1993.

[8] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644-654, 1976

[9] U. Feige, A. Fiat and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[10] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology CRYPTO '86, Lecture Notes in Computer Science, Springer Verlag*, 263:186–194, 1987.

Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w'03)
0-7695-1873-7/03 $17.00 © 2003 IEEE

[11] Y. Frankel, P. Gemmel, P. Mackenzie and M. Yung. Proactive RSA. *Crypto '97, Lecture Notes in Computer Science, Springer Verlag*, pp 440–452, 1997.

[12] Y. Frankel, P. Gemmel, P. Mackenzie and M. Yung. Optimal resilience proactive public key crypto systems. *38th Annual Symposium on Foundations of Computer Science*, pp 384–393, 1997.

[13] S. Goldwasser, S. Micali and C. Rackoff. The knowledge complexity of interactive proofsystems. *SIAM Journal of Computing*, 18(1):186–208, 1989.

[14] H. Hezberg, D. Jarecki, H. Krawzyk and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. *Crypto '95*, pp 339–352, 1995.

[15] D.B. Johnson Routing in ad hoc networks of mobile hosts. *Mobile Computing Systems and Applications*, pp 158–163, 1994.

[16] Q. Li and D. Rus. Sending messages to mobile users in disconnected ad hoc wireless networks. *In proceedings of ACM MOBICOM '00*, pp 44–55, 2000.

[17] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang. Self-securing ad hoc wireless networks. *7th International Symposium on Computers and Communications*, pp 567–574, 2002.

[18] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang. Providing robust and ubiquitous security support for manet. *9th INternational Conference on Network Protocols*, pp 251–260, 2001.

[19] M. Reiter. Distributing trust with the rampart tool kit. *Communications of the ACM*, 39(4):71–74, 1996.

[20] L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT-w'03)
0-7695-1873-7/03 $17.00 © 2003 **IEEE**