

Decentralized Key Management in Ad Hoc Networks

Joseph Binder
Department of Computer Science
Rochester Institute of Technology
Rochester, NY 14623
jsb7384@cs.rit.edu

Hans-Peter Bischof
Department of Computer Science
Rochester Institute of Technology
Rochester, NY 14623
hpb@cs.rit.edu

Alan Kaminsky
Department of Computer Science
Rochester Institute of Technology
Rochester, NY 14623
ark@cs.rit.edu

Abstract—Robust key management services are central to ensuring privacy protection in wireless ad hoc network settings. Existing approaches to key management, which often rely on trusted, centralized entities, are not well-suited for the highly dynamic, spontaneous nature of ad hoc networks. This paper surveys emergent approaches to key management in ad hoc networks and identifies remaining areas of development.

I. INTRODUCTION

The advent of ad hoc networks brought with it a flurry of research focussed on communication and routing protocols. These developments enabled an increased number of applications to harness the benefits of decentralized networks. Examples of such applications range from simple chat programs to shared whiteboards and other collaborative applications. Although intended for diverse audiences and contexts, many of these applications share a common quality: they are information-centric. The information transferred may be a banal conversation between friends, confidential meeting notes shared among corporate executives, or mission-critical military information. Despite the deployment of information-driven applications such as these, the call for ad hoc network security remains largely unanswered.

Ad hoc security is not, however, a concern that has slipped through the cracks unnoticed: numerous research initiatives have been launched to surmount the challenge. The vast majority of these initiatives have focussed their focus on secure routing protocols. However, key management—despite its intrinsic role in achieving security—remains a largely under-developed problem space.

II. SECURITY REQUIREMENTS

The security services of ad hoc networks are not altogether different than those of other network communication paradigms. Specifically, an effective security paradigm must ensure the following security primitives:

- Identity verification
- Data confidentiality
- Data integrity
- Availability
- Access control

Although solutions to the above concerns have been developed and widely deployed in the wired domain, the amorphous,

transient properties of ad hoc networks preclude their adaptation to serverless network environments, which are often comprised of small devices. Instead, security solutions, in general, and key managements should strive for the following characteristics:

- **Lightweight:** Solutions must minimize the amount of computation and communication required to ensure the security services to accommodate the limited energy and computational resources of mobile, ad hoc-enabled devices.
- **Decentralized:** Like ad hoc networks themselves, attempts to secure them must be *ad hoc*: they must establish security without *a priori* knowledge or reference to centralized, persistent entities. Instead, security paradigms must levy the cooperation of all trustworthy nodes in the network.
- **Reactive:** Ad hoc networks are dynamic: nodes—trustworthy and malicious—may enter and leave the network spontaneously and unannounced. Security paradigms must react to changes in network state; they must seek to detect compromises and vulnerabilities; they must be reactive, not protective.
- **Fault-Tolerant:** Wireless transfer mediums are known to be unreliable; nodes are likely to leave or be compromised without warning. The communication requirements of security solutions should be designed with such faults in mind; they mustn't rely on message delivery or ordering.

III. STATE OF THE ART

Key management has been the thrust of several research initiatives in the ad hoc networking domain (e.g., [8], [6], [3] et al). Each of these approaches seeks to establish a public key infrastructure within the constraints of ad hoc networks. Each approach is discussed below.

“Securing Ad Hoc Networks” [8] was one of the first notable publications to propose a public key management service for ad hoc networks. The service itself encapsulates a public/private key pair (K/k). The private key, k , is used to sign other nodes' public keys; the public key, K , is used to verify the signature. The service employs a $(n, t+1)$ threshold scheme to distribute the private key and the digital signing process among n nodes. Each of the n nodes is denoted as

a server node, as it has a special role in the signing service. Combiner nodes—which may be a subset of the server nodes or altogether different nodes—are also required to combine each server’s partial signature. For example, to sign a certificate, each of the n server nodes must generate a partial signature using its share of the private key (k_1, k_2, \dots, k_n) to compute a partial signature of the certificate. Once generated, each server node sends its partial signature to the combiner; the combiner then computes the entire signature. To its credit, [8] was quite progressive at its inception, as its design is largely proactive and capable of handling a dynamic network state. Nonetheless, the service has remnants of its wired predecessor, namely, a trusted authority, and specialized server and combiner nodes. Although the threshold scheme employed allows $t < n$ servers to be compromised without sacrificing the service, its largely centralized approach encapsulates relatively few points of failure and attack.

“Providing Robust and Ubiquitous Security Support for Ad Hoc Networks”[6] presents a natural extension to [1], wherein the signing service is distributed to any node n in the network. For example, if a network member requires a certificate, it need only be in the proximity of *any* $t + 1$ nodes. The service is otherwise similar to [6]. Despite the improved distribution, [6] still requires a trusted party at initialization. Further, because any node in the network may participate in the sharing, a malicious node may masquerade as $t+1$ bogus nodes and reconstruct the private key.

More recently, Hubaux et al have proposed a self organizing public key infrastructure in [3]. Unlike the previous two publications, [3] does not require a trusted authority or any specialized nodes; instead, each node issues its own certificates to other nodes. Each node maintains a limited repository of other nodes’ certificates. When a node wishes to validate a certificate of another node, the nodes combine their certificate repositories; the validating node then examines the merged certificate repository for falsified certificates. If none are found, the certificate is accepted; otherwise it is rejected. The primary drawback of [3] is its initialization time. In long-lived ad hoc networks, such overhead may be admissible; it is likely to be prohibitive in more transient settings.

IV. LOOKING FORWARD

Although each of the above paradigms is effective in its own right, they are all based on a common assumption, namely, point-to-point communication. Public key infrastructures enable nodes with authentic public encryption keys that they may use to establish secure communication with one another. However, many ad hoc networks are collaborative, many-to-many environments. In these settings, public key cryptography is computationally intensive, as each group message must be encrypted $n - 1$ times. Group key management paradigms, which provide a symmetric key that is shared among all group members, have been used throughout the wired networking domain to secure broadcast and many-to-many communication environments; however, very few attempts have been made

to adapt group key management infrastructures to an ad hoc setting.

Dominant group key management paradigms include the well-known CLIQUES project [7], Desmedt et al [2], Kim et al [5], and several others. Each of these protocols is based on the generalized Diffie-Hellman problem, which requires every network member to contribute to the generation of the shared group key. Because they were developed for wired environments, many of these approaches require point-to-point and broadcast mediums, synchronous messaging, and static network topologies. Unfortunately, the wireless, amorphous, transient, many-to-many nature of ad hoc networks precludes many of the assumptions on which the above protocols were developed.

Other research initiatives, such as [1] and [4], have identified the need for secure group communication in ad hoc networks also. However, their work has been largely analytical in nature rather than developmental. We, therefore, see an increasing need for a fully distributed group key management paradigm that can effectively function under the constraints of ad hoc networks. Preliminary research findings indicate that much of the work that has been done with key management in mind for peer-based groups in wired settings can be adapted to wireless, serverless settings. Notable challenges that arise during this adaptation include:

- 1) removing the specific order which nodes participate in key agreement;
- 2) integrating robust authentication into the key agreement protocol;
- 3) distributing the computational overhead of key creation among all nodes;
- 4) removing the need for a controlling or otherwise specialized entity from the protocol;
- 5) and re-examining the need for forward and backward secrecy in spontaneous network contexts.

V. CONCLUSION

In this paper, we identified the security requirements of ad hoc networks and the constraints under which those requirements must be satisfied. We then reviewed current initiatives in the key management area. Following the review, we identified a remaining, yet under-developed approach to variant of key management, namely, group key management. Challenges within this approach were asserted; our ongoing research seeks to surmount these challenges.

REFERENCES

- [1] Eric Anton and Otto Duarte. Group key establishment in wireless ad hoc networks. In *Workshop em Qualidade de Servico e Mobilidade*, 2002.
- [2] Mike Burmester and Yvo Desmedt. A secure and efficient conference key distribution system. In *Advances in Cryptology – EUROCRYPT ’94*, pages 275–286, 1994.
- [3] S. Capkun, L. Buttyan, and J. Hubaux. Self-organized public-key management for mobile ad hoc networks, 2002.
- [4] Maarit Hietalahti. Key establishment in ad-hoc networks.
- [5] Yongdae Kim, Adrian Perrig, and Gene Tsudik. Simple and fault-tolerant key agreement for dynamic collaborative groups. In *Proceedings of the 7th ACM conference on Computer and communications security*, pages 235–244, 2000.

- [6] H. Luo and S. Lu. Ubiquitous and robust authentication services for ad hoc wireless networks, 2000.
- [7] Michael Steiner, Gene Tsudik, and Michael Waidner. CLIQUES: A new approach to group key agreement. In *Proceedings of the 18th International Conference on Distributed Computing Systems (ICDCS'98)*, pages 380–387, Amsterdam, 1998. IEEE Computer Society Press.
- [8] Lidong Zhou and Zygmunt J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.