IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

EFFICIENT KEY MANAGEMENT IN MISSION CRITICAL WIRELESS ADHOC NETWORKS

Sri B.J.R. Somayajulu ME (CSE)
Head, Department of Computer Science
KVR, KVR & MKR College,
Khajipalem

Abstract

Mission-critical networks show great potential in emergency response and/or recovery, health care, critical infrastructure monitoring, etc. Such mission-critical applications demand that security service be anywhere, anytime. However, it is challenging to design a key management scheme in current mission-critical networks to fulfill the required attributes of secure communications, such as data integrity, authentication, confidentiality, non repudiation, and service availability. In this paper, we present a self-contained public key-management scheme, a scalable method of cryptographic key management (SMOCK), which achieves almost zero communication overhead for authentication, and offers high service availability. In our scheme, a small number of cryptographic keys are stored offline at individual nodes before they are deployed in the network. To provide good scalability in terms of the number of nodes and storage space, we utilize a combinatorial design of public-private key pairs, which means nodes combine more than one key pair to encrypt and decrypt messages. We also show that SMOCK provides controllable resilience when malicious nodes compromise a limited number of nodes before key revocation and renewal.

Key Words: Wireless Adhoc Networks

Introduction:

The wireless communication revolution is bringing fundamental changes to data networking, telecommunication, and is making integrated networks a reality. By freeing the user from the cord, personal communications networks, wireless LAN's, mobile radio networks and cellular systems, harbor the promise of fully distributed mobile computing and communications, any time, anywhere. A wireless ad hoc network (WANET) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring typical network infrastructure equipment, such as a wireless router or access point.

In most cases, a PC, laptop or smartphone Wi-Fi interface is used to build an ad hoc network (Figure 1). In other situations, devices such as wireless sensors are designed to work primarily in an ad hoc mode.

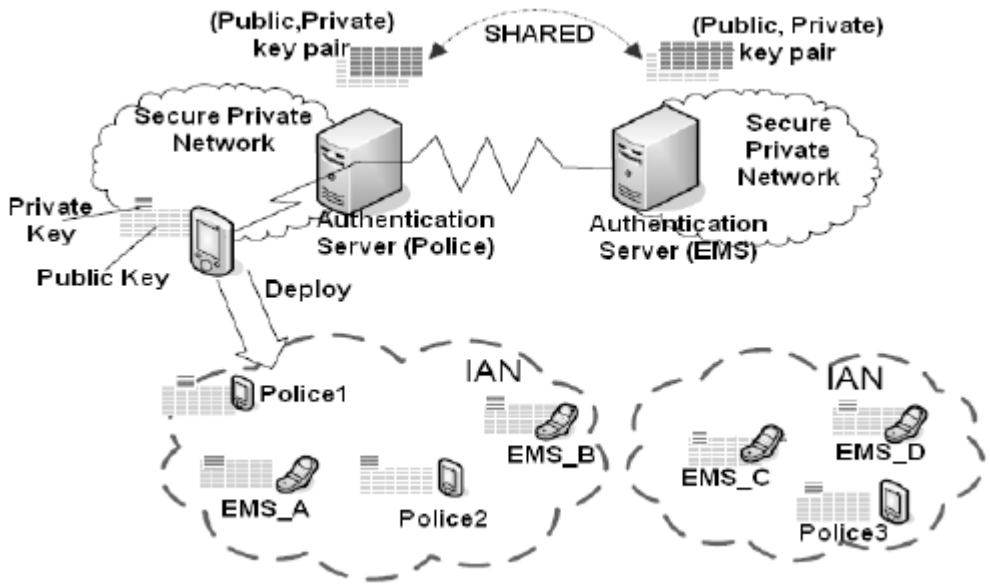

Figure 1. Two Authentication Servers Police Department and emergency Medical Service (EMS)

Because the devices in the ad hoc network can access each other's resources directly through basic peer-to-peer (P2P) or point-to-multipoint modes, central servers are unnecessary for functions such as file sharing or printing. In a WANET, a collection of devices or nodes -- such as a wireless-capable PC or Smartphone -- is responsible for network operations, such as routing, security, addressing and key management

AD HOC NETWORK WORK

Devices configured for ad hoc functionality require a wireless network adapter or chip, and they need to be able to act as a wireless router when connected. When setting up a wireless ad hoc network, each wireless adapter must be configured for ad hoc mode instead of infrastructure mode. All wireless devices connecting to an ad hoc device need to use the same service set identifier (SSID) and wireless frequency channel number.

Instead of relying on a wireless base station, such as a wireless access point (WAP) or Wi-Fi router, an ad hoc device takes on this role and coordinates the flow of messages to each node in the network. The individual wireless endpoints connected to ad hoc network forward packets to and from each other. Makeshift by nature, ad hoc wireless networks are most useful when wireless infrastructure isn't available -- for example, if there aren't any access points or routers within range and cabling cannot extend to reach the location where additional wireless communication is needed.

It's important to note that not all ad hoc networks are built using a PC or Smartphone. In fact, Wi-Fi access points can be configured to work in either ad hoc or infrastructure mode as well. Typically, Wi-Fi networks configured for infrastructure mode are created and managed using equipment such as Wi-Fi routers or a combination of WAPs and wireless controllers that provide the necessary network intelligence. Ad hoc networks are also commonly set up to provide temporary wireless network access created by a computer or Smartphone. The use of more sophisticated network protocols and network services found on infrastructure-

based wireless networks, such as IEEE 802.1x authentication, usually are not suitable or necessary for short-lived ad hoc networks.

USE OF AD HOC WIRELESS NETWORK

Deciding when to employ ad hoc versus infrastructure mode depends on the use. For example, users who want a WAP to act as a permanent access point should choose infrastructure mode with an on-site or cloud-based wireless LAN (WLAN) controller. But ad hoc mode might be a good option for a user setting up a temporary wireless network between a small numbers of devices. A perfect example of this is to use a cellular-connected Smartphone that is configured in Wi-Fi ad hoc mode so that Wi-Fi capable laptops can connect to the Wi-Fi ad hoc network to gain internet access over the Smartphone's cellular internet link. This method bypasses any need for a WAP or WLAN controller.

Ad hoc networks require minimal configuration and can be deployed quickly, which makes them suitable for emergencies, such as natural disasters, military conflicts or when travelling. Thanks to the presence of dynamic and adaptive routing protocols, these networks can be configured quickly. These impromptu, on-demand networks are useful for putting together a small, inexpensive all-wireless LAN without the need for wireless infrastructure equipment. They also work well as temporary access to the internet if wireless access points or routers fail.

TYPES OF AD HOC WIRELESS NETWORKS

Types of WANETs vary by application need and use. Choosing a wireless ad hoc network type depends on the wireless equipment capabilities, physical environment and purpose of the communication.

MANET

A mobile ad hoc network involves mobile devices communicating directly with one another. A MANET is a network of wireless mobile devices without an infrastructure that are self-organizing and self-configuring. A MANET is sometimes referred to as an "on-the-fly" or "spontaneous network." Examples of MANETs include smart home lighting, ad hoc streetlight networks, ad hoc networks of robots, disaster rescue ad hoc networks and hospital ad hoc networks. In many cases, these networks use proprietary or non-TCP/IP networking standards for communication.

IMANET

Internet-based mobile ad hoc networks support internet protocols, such as TCP/IP (Transmission Control Protocol/Internet Protocol) and User Datagram Protocol (UDP). The iMANET employs a TCP/IP network-layer routing protocol on each connected device to link mobile nodes and set up distributed routes automatically. IMANETs may also be used in the collection of sensor data for data mining for a variety of use cases, such as air pollution monitoring.

SPAN

Smartphone ad hoc networks employ existing hardware, such as Wi-Fi and Bluetooth, and software protocols built into a Smartphone operating system (OS) to create P2P networks without relying on cellular carrier networks, wireless access points or other traditional network infrastructure equipment. Different from traditional hub-and-spoke networks, such as Wi-Fi Direct, SPANs support multi-hop relays. Multi-hop relay is the process of sending traffic from device A to device C using intermediary device B. Therefore, device A and C do not need to have a direct P2P connection established for traffic to reach its destination. Because SPANs are fully dynamic in nature, there is no group leader in this type of application and, thus, peers can join or leave without harming the network.

Vehicular ad hoc network

This network type involves devices in vehicles that are used for communicating between them and roadside equipment. An example is the in-vehicle safety and security system OnStar.

WMN

Wireless mesh networks are comprised of radio networks set up in a mesh topology and frequently consist of mesh clients, mesh routers and gateways. In mesh networking, the devices -- or nodes -- are connected so at least some, if not all, have many paths to other nodes. This creates many routes for information between pairs of users, increasing the resilience of the network if a node or connection fails. WMNs are useful in situations where a temporary wireless network is required or in more permanent scenarios where network cabling cannot be run to create an infrastructure-based wireless network.

ADVANTAGES OF AN AD HOC NETWORK

Ad hoc mode can be easier to set up than infrastructure mode when just connecting a handful of devices without requiring a centralized access point. For example, if a user has two laptops and is in a hotel room without Wi-Fi, they can be connected directly in ad hoc mode to create a temporary Wi-Fi network without a router. The Wi-Fi Direct standard -- a specification that allows devices certified for Wi-Fi Direct to exchange data without an internet connection or a wireless router -- also builds on ad hoc mode. It enables devices to communicate directly over Wi-Fi signals.

OTHER BENEFITS OF WIRELESS AD HOC NETWORKS INCLUDE THE FOLLOWING:

- Because ad hoc networks do not require infrastructure hardware such as access points or wireless routers, they provide a low-cost way of direct client-to-client or client-to-internet communication.
- Ad hoc networks are easy to configure and offer an effective way to communicate with devices nearby when time is of the essence and running cabling is not feasible.

- The temporary, often impromptu qualities of ad hoc networks can make them less vulnerable to security threats.
- An ad hoc network linking a small number of devices might be more practical than a traditional infrastructure-based network that can connect many more devices.

REFERENCES:

[1] S.A. Camtepe and B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks. In Proceedings of 9th European Symposium On Research in Computer Security (ESORICS 04), 2004.

[2] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy, pages 197C213, 2003.

[3] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), pages 42C51, Washington, DC, USA, October 27-31 2003.

[4] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, pages 41C47, November 2002.

[5] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), pages 52C61, October 2003.

[6] S. Zhu, S. Setia, and S. Jajodia. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), pages 62C72, October 2003.

[7] F. Delgosha and F. Fekri. Threshold Key-Establishment in Distributed Sensor Networks Using a Multivariate Scheme.In Proceedings of 25th IEEE INFOCOM, April 2006.

[8] P. Traynor, H. Choi, G. Cao, S. Zhu, T. La Porta. Establishing Pair-Wise Keys in Heterogeneous Sensor Networks. In Proceedings of 25th IEEE INFOCOM, April 2006.

[9] G. Gaubatz, J. Kaps, and B. Sunar. Public keys cryptography in sensor networks — revisited. In The Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS), 2004. [10] D. J. Malan, M. Welsh, and M. D. Smith. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, October 2004.

[11] B. Lai, S. Kim, and I. Verbauwhede, Scalable session key construction protocol for wireless sensor networks. In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES).

[12] S. Kent and T. Polk. Public-key infrastructure (x.509) (pkix) charter. Available at http://www.ietf.org/html.charters/pkixcharter. html.

[13] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. IEEE Network Magazine, Nov. 1999.

[14] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In Proceedings of the 9th IEEE International Conference on Network Protocols (ICNP 2001), 2001.