Applicability of Public Key Infrastructures in Wireless Sensor Networks

Rodrigo Roman and Cristina Alcaraz

Computer Science Department,
University of Malaga, Spain
{roman,alcaraz}@lcc.uma.es

Abstract. Wireless Sensor Networks (WSN) are becoming a key technology in the support of pervasive and ubiquitous services. The previous notion of "PKC is too expensive for WSN" has changed partially due to the existence of new hardware and software prototypes based on Elliptic Curve Cryptography and other PKC primitives. Then, it is necessary to analyze whether it is both feasible and convenient to have a Public Key Infrastructure for sensor networks that would allow the creation of PKC-based services like Digital Signatures.

Keywords: Wireless Sensor Networks, Public Key Cryptography, Public Key Infrastructure.

1 Introduction

Wireless Sensor Networks [1] can be considered as a key technology to support pervasive and ubiquitous services. They can be applied to a wide number of areas: such as farmland monitoring, smart office, detection of out-of-tolerance environmental conditions, emergency medical care, wearable smart uniforms, etc. However, these networks are quite difficult to protect, because every node becomes a potential point of logical and physical attack.

In this context, it would be extremely useful to have a cryptographic primitive such as Public Key Cryptography (PKC) in order to create services such as Digital Signatures. The use of PKC in sensor networks has been usually considered as "nearly impossible", but at present some studies [4] have started to consider the possibility of utilizing PKC in a highly-constrained networks. It is then the purpose of this paper to review the state of the art of PKC for sensor networks, and to analyze if it is both feasible and convenient to have a working Public Key Infrastructure in a sensor network environment.

The rest of this paper is organized as follows: In section 2 the architecture of a wireless sensor network is explained, alongside with how PKC could influence on solving some major security problems. In section 3, the major PKC primitives that could be applied to constrained environments such as sensor nodes are presented and studied. Finally, in section 4, there is a deep analysis of the applicability of Public Key Infrastructures to a sensor network environment, and in section 5, the conclusions are presented.

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 313–320, 2007.

2 Wireless Sensor Networks

A Wireless Sensor Network, as a whole, can be seen as the "skin" of a computer system, since it is able to provide any physical information of a certain region or element to any external system. The ability of measuring their environment is not the only benefit of these networks: thanks to the wireless capabilities and the limited computational power of their elements, they are easy to set up, are capable of self-configuring themselves, and are relatively inexpensive. The main elements of a sensor network are the sensor nodes and the base station - the "cells" of the system and its "brain".

Sensor nodes are small and inexpensive computers that have limited computational and wireless capabilities: a typical sensor node uses a microcontroller of 8Mhz with 4KB of RAM and 128KB of ROM, and incorporates a transceiver compliant to low-power, low duty standards such as IEEE 802.15.4. On the other hand, the base station is a powerful, trusted device that acts as an interface between the user of the network and the nodes. Regarding their internal configuration, the nodes of the network can group themselves into clusters where all the organizational decisions inside a cluster are made by a single entity called "cluster head" (hierarchical configuration), or all the nodes can participate in both the decision-making processes and the internal protocols (flat configuration).

In a sensor network, amongst other issues, it is extremely important to provide certain basic security mechanisms and protocols in order to avoid attacks from malicious adversaries [3]. It was recently when Public Key Cryptography (PKC) started to be considered as a viable solution for this purpose. Since, in most cases, a node does not know in advance who will be on its neighborhood, PKC can be used for both authenticating such nodes and for allowing the secure exchange of pairwise keys. Any procedure that requires the participation of the base station can also take advantage of these primitives. For instance, it is possible to securely distribute new code to the nodes of the network if it has been previously signed by the base station. Lastly, there are many other services that can effectively use PKC: authenticated broadcast, data source authentication in data aggregation, privilege delegation, etc.

3 Public Key Cryptography Primitives for Sensor Networks

3.1 Existing PKC Primitives

The computational requirements of PKC primitives are quite expensive in comparison with other cryptographic primitives, such as Symmetric Key Encryption (SKE). For instance, the most popular algorithm for public key encryption, RSA [5], is quite inefficient when implemented in sensor nodes. However, there exists other PKC approaches based on various mathematical problems that can be specially useful in highly-constrained environments. The first example is the Rabin signature algorithm [6], proposed by Michael Rabin in 1979. It is very similar to