UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INFORMATICA "RENATO M. CAPOCELLI"

DOTTORATO DI RICERCA IN INFORMATICA

XIII CICLO

ABSTRACT

ID-Based Key Agreement for WANETs

Coordinatore:
Prof. Giuseppe Persiano

Candidato:
Francesco Rossi

Tutor:
Prof. Alfredo De Santis

Co-tutor:
Prof. Giovanni Schmid

ANNO ACCADEMICO 2013/2014

Abstract

The increasing interest about wireless ad hoc networks (WANETs) is due to some key features not owned by traditional networks such as nodes mobility, network self-organization and the ability to rely on infrastructure-less setup. WANETs can be used in many application scenarios such as health care, environmental monitoring, military and many others commercial applications.

Unfortunately, the open nature of the communication channel exposes WANETs to a great number of security threats (e.g. jamming, eavesdropping, node replication, unfairness, wormhole, packet injection). The security of WANETs hinges on node authentication, which by mean of Cryptography can be obtained through key distribution mechanisms. Moreover, WANET applications often require the establishment of session keys, that will be used for encryption, message authentication and others cryptographic purposes.

In this thesis we present a cryptographic framework for WANETs, named JIKA (Java framework for ID-based key agreement) which simulates a key generation center (KGC) and offers an ID-based key distribution service for signature schemes and key agreement protocols. Moreover, JIKA makes use of elliptic curve cryptography (ECC) which allows fast computations, small key size and short signatures of messages. It includes two new ID-based signature schemes (IBS-1 and IBS-2) which get shorter signatures, an ID-based two-party key agreement protocol

(eFG) and two new group key agreement protocols (GKA v1 and GKA v2). GKA protocols are full-contributory and offer implicit key authentication through the ID-based signature schemes described above, at the cost of just two rounds. They provide resilience against passive and active attacks performed by external adversaries. In order to emulate executions on a WANET, we run the above algorithms on the embedded device Raspberry PI. This device supports standard wireless adapters that can be used to setup a WANET through a suitable configuration. The same tests were executed on a Personal Computer platform, so as to compare experimental results between devices with very different computational resources. The test results show that our algorithms outperform notable algorithms proposed so far in the literature. In particular, group key agreement protocols are affordable for a quite large number of parties, also on resource constrained devices such as the Raspberry PI.