ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

An over-the-air key establishment protocol using keyless cryptography

Yuexin Zhang [a,b], Yang Xiang [a,b], Tao Wang [c], Wei Wu [d,*], Jian Shen [e]

[a] Centre for Cyber Security Research, Deakin University, Geelong, VIC 3220, Australia

[b] The State Key Laboratory of Integrated Services Networks, Xidian University, China

[c] University of South Florida, Tampa, FL 33620, USA

[d] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China

[e] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China

HIGHLIGHTS

- We present a key establishment protocol using keyless cryptography.
- The protocol is design for two nearby wireless devices.
- Two devices can establish a secret key by sending random signals to each other.
- The analysis shows that our protocol is a low cost key establishment protocol.

ARTICLE INFO

Article history:
Received 27 August 2016
Received in revised form
22 November 2016
Accepted 9 December 2016
Available online xxxx

Keywords:
Key establishment
Security
Anonymous channel
Source indistinguishability

ABSTRACT

Today, an increasing number of devices wirelessly communicate with each other. However, due to the nature of wireless transmission, the communications are vulnerable to many adversarial attacks such as eavesdropping. Key establishment is one of the fundamental and widely studied countermeasures for securing the communications. In certain applications, the wireless devices may be energy-constrained, such as sensor nodes. Thus, energy intensive asymmetric key establishment protocols are infeasible. Additionally, in some scenarios, it is not practical to assume that all the devices pre-share certain secrets. Motivated by these observations, this paper presents an over-the-air key establishment protocol using keyless cryptography. Specifically, the proposed protocol is designed without using asymmetric key cryptography and pre-shared secrets. More specifically, our protocol provides a concrete construction to transform the wireless channel into an anonymous channel, and two wireless devices can establish a secret key by directly sending random signals to each other. The performance analysis shows that the energy consumption of our protocol is around 176 times cheaper than that of the Diffie–Hellman key exchange protocol. Additionally, it takes only 159.04 *ms* to establish a key with 112 secret bits.

1. Introduction

In recent years, an increasing number of devices are equipped with wireless interfaces and microprocessors. Using these devices, we can access the Internet and keep connected with others. In certain applications, a device needs to directly communicate with other nearby devices. Thus, many protocols are designed for nearby devices' communications, such as the Device-to-Device (D2D) communication, Near Field Communication (NFC), and the IEEE standard 802.15.4. Specifically, in these protocols, messages are directly transmitted between two nearby devices (without employing forwarders and routers). Due to the nature of wireless transmission, the communications are vulnerable to many adversarial attacks. For instance, the adversary can eavesdrop the communications and conduct malicious attacks. Recently, a new class of attack, the Advanced Persistent Threat (APT), has emerged. Specifically, the APT is defined by the US National Institute of Standards and Technology (NIST) as: "An adversary that possesses

* Corresponding author.
E-mail addresses: yuexinz@deakin.edu.au (Y. Zhang), yang.xiang@deakin.edu.au (Y. Xiang), taow@mail.usf.edu (T. Wang), weiwu@fjnu.edu.cn (W. Wu), s_shenjian@126.com (J. Shen).

http://dx.doi.org/10.1016/j.future.2016.12.013
0167-739X/

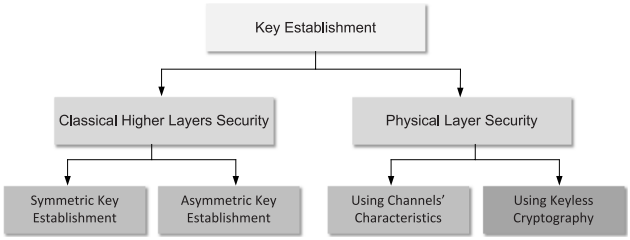

Fig. 1. Overview of existing key establishment.

sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)" [1,2].

To ensure the security and privacy of communications, cryptographic keys need to be established. Until now, key establishment protocols have been extensively and intensively studied, and classical designs can be classified into two main types, namely, asymmetric key establishment protocols and symmetric key establishment protocols (as shown in Fig. 1). Specifically, in asymmetric key establishment protocols (e.g., the Diffie–Hellman key exchange protocol [3]), costly computation operations, such as the exponentiation operations, need to be executed. In symmetric key establishment protocols (e.g., the key pre-distribution protocols [4,5]), however, considerable memory spaces are used to pre-load secrets.

In certain applications, the wireless devices may be energy-constrained devices (i.e., powered by batteries), such as sensor nodes. Thus, the energy intensive asymmetric key establishment protocols are excluded. Besides, the wireless devices (such as sensor nodes, smart phones, tablets, and laptops) are produced by different factories, and they are integrated with different technologies. Thus, it is not a practical assumption that all these devices are pre-loaded with certain secrets when they leave factories. Motivated by these observations, in this paper, we aim to design a key establishment protocol without using asymmetric key cryptography and pre-shared secrets.

It is a challenging topic to establish secret keys without using energy intensive asymmetric key cryptography and pre-shared secrets, and the topic has been undertaken in two ways, namely, (a) extracting keys by taking advantage of the wireless channels' characteristics, such as the received signal strength (RSS) and channel impulse response (CIR) [6,7]; and (b) establishing keys using keyless cryptography [8].

For those key establishment protocols using characteristics of the wireless channels, some issues still remain unsatisfactory. For instance, asymmetric effects introduced by the multipath fading, the key generation rate needs to be improved, and a dynamic environment is needed to provide sufficient entropy. For those key establishment protocols using keyless cryptography, two devices can establish a secret key with light consumptions. Specifically, an anonymous channel is needed to guarantee that the adversaries cannot identify the source of the eavesdropped messages. Namely, the anonymous channel achieves source indistinguishability (please refer to Section 3.2 for details). However, these key establishment protocols are designed based on human assistance (e.g., shaking the devices), or they are designed without giving a concrete construction to transform the wireless channel into an anonymous channel.

Our contribution. In this paper, we present an over-the-air key establishment protocol using keyless cryptography. Specifically, our key establishment protocol possesses the following properties:

1. Our key establishment protocol is specifically designed for assisting users, who do not pre-share any secrets and have no access to the on-line trusted third party, to establish secret keys. Specifically, in order to establish a secret key, two users in our protocol show off their wireless devices, and directly send analog signals to each other.
2. The protocol provides a concrete construction to transform the wireless channel into an anonymous channel. Specifically, to achieve source indistinguishability, users move into proximity and introduce randomness to the signals (in order to achieve spatial indistinguishability). Besides, in each round, signals are sent at randomly chosen times (in order to achieve temporal indistinguishability).
3. Our protocol is a low-cost key establishment protocol. The performance analysis shows that energy consumption of our protocol is about 176 times cheaper than that of the Diffie–Hellman key exchange protocol [3], and it only takes around 159.04 ms to establish a key with 112 secret bits.

Organization of the paper. The remainder of this paper is organized as follows. In the next section, we present a brief overview on the related work. Section 3 reviews the preliminaries required in this paper. Then, the proposed protocol is described in Section 4, and its security and performance analysis are provided in Section 5 and Section 6, respectively. In Section 7, we conclude this paper.

2. Related work

In this section, we review those closely related key establishment protocols. Namely, key establishment protocols using keyless cryptography, and key establishment protocols for full-duplex NFC.

2.1. Key establishment protocols using keyless cryptography

The key establishment protocol using keyless cryptography is introduced for the first time in [8], and it is optimized by [9–12]. Specifically, these protocols are designed based on the anonymous channels. A broadcast channel is said to be an anonymous channel if it achieves source indistinguishability. Namely, the adversary can eavesdrop the transmitted messages over the channel, but she cannot identify the source of the messages (please refer to Section 3.2 for details).

For instance, users in [10] can establish a key with k secret bits by executing following operations:

- Alice randomly chooses $\frac{k}{2}$ bits $C_a = [C_a^1, C_a^2, \ldots, C_a^{\frac{k}{2}}]$. Similarly, Bob randomly chooses $\frac{k}{2}$ bits $C_b = [C_b^1, C_b^2, \ldots, C_b^{\frac{k}{2}}]$;
- Alice builds $\frac{k}{2}$ messages $m_A^1, m_A^2, \ldots, m_A^{\frac{k}{2}}$ using C_a. For instance, the message m_A^i is built by following the rule that, the source identifier of m_A^i is set to be *Alice* if $C_a^i = 1$. Otherwise, it is set to be *Bob*. Following the same rule, Bob builds $\frac{k}{2}$ messages $m_B^1, m_B^2, \ldots, m_B^{\frac{k}{2}}$ using C_b; and
- In the ith round, either Alice or Bob (with equal probability) sends an empty packet m_A^i or m_B^i at time t_i, where t_i is chosen uniformly at random in the interval $[(i-1)T_r, iT_r]$ (T_r is a constant parameter).

The secret bits are represented by identifying the correct or incorrect identifiers of the messages. For example, in the ith round, Alice and Bob set the ith bit of secret key K to be 1, if the sender and recipient address of m^i is correct. Otherwise, it is set to be 0. The security of [10] relies on the source indistinguishability, and the source indistinguishability requires that the exchanged messages are temporal indistinguishability and spatial indistinguishability.

Please cite this article in press as: Y. Zhang, et al., An over-the-air key establishment protocol using keyless cryptography, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.12.013