Computer Networks 58 (2014) 112–126

Contents lists available at ScienceDirect

Computer Networks

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

Multi-user wireless channel probing for shared key generation with a fuzzy controller

Lihua Dou [a], Yunchuan Wei [a,b,*], Jun Ni [c]

[a] Department of Automation, Beijing Institute of Technology, Beijing 100081, China
[b] Research and Development Center, China Academy of Launch Vehicle Technology, Beijing 100076, China
[c] College of Medicine, The University of Iowa, Iowa City, IA 52242, USA

ARTICLE INFO

Article history:
Received 9 November 2011
Received in revised form 5 March 2013
Accepted 23 August 2013
Available online 7 September 2013

Keywords:
Wireless channel probing
Shared key generation
Multi-user
Fuzzy controller
Information theory
Cryptography

ABSTRACT

Probing the wireless channel in wireless networks to generate a shared key is an increasingly interesting security topic. However, not much work has been focused on wireless channel probing in multi-user applications for Shared Key Generation (SKG). In this paper we propose a scheme of multi-user wireless channel probing using a broadcast approach and a fuzzy controller. In the proposed scheme, the concept of Desired-Weighting Factor (DWF) is introduced to meet a user's Key Generation Rate (KGR) requirement. The experimental results in this primary study show that the fuzzy controller can be used to satisfy KGR requirement by efficiently tuning the probing rate under dynamic conditions. Compared with the conventional Proportional–Integral–Derivative (PID) controller, the proposed probing scheme with a fuzzy controller may produce smaller overshoots and fewer oscillations. The fuzzy controller in the proposed scheme also stabilizes the KGR at desired values, improves the SKG accuracy, enhances the control capability, and increases the entropy rate. The study indicates that the proposed multi-user probing scheme can be used to make a trade-off between probing efficiency and the user's KGR requirement.

1. Introduction

Generating a shared key between two parties (legitimate users) through a wireless channel is an increasingly interesting topic of security in wireless networks [1–14]. The properties of a wireless probing channel such as reciprocity, randomness, and location–specification can be used to produce highly-correlated states in terms of bits for a shared key. Such key generation is information-theoretically secure, since a third party (an illegitimate user) half a wavelength away from the legitimate users may eavesdrop but has difficulty generating the same key in a rich scattering environment where the channel varies rapidly with time and spatial position [15]. The illegitimate user is unable to break down the key even with supercomputing power. One feasible and simple method to generate a shared key through a wireless channel is to use the Received Signal Strength (RSS) [1–4]. The RSS-based method has three major steps: quantization, information reconciliation, and privacy amplification. First, the legitimate users can send channel probing frames to each other to measure the RSS from participating wireless devices. This process is called channel probing. The measured RSS sequences can then be quantized in terms of bits. An information reconciliation process can be applied to correct the difference of bits streams obtained by different users in order to reach an agreement on the key. Often, a privacy-amplification process is then employed to remove unnecessary bits and to minimize the correlation between

[*] Corresponding author. Address: College of Medicine, The University of Iowa, Iowa City, IA 52242, USA. Tel.: +86 13810028259.
E-mail address: weiyunchuanmail@sina.com (Y. Wei).

1389-1286/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comnet.2013.08.027

bits to make strong keys. The detailed steps can be found in [2] and the method implementations can be found in [2–5].

Early work concentrated on theoretical analysis [9–12,14], while recent work has focused on the implementations of Shared Key Generation(SKG) schemes using off-the-shelf wireless devices [1–4,13]. In practical implementations, the phase reciprocity of frequency selective fading channels [12,16] is employed.

Communications in many group-oriented multiple-user applications have various settings, ranging from multicasting in a network layer to teleconferencing/videoconferencing in an application layer. The privacy and integrity of such communications require specific security services. Although peer-to-peer security implementation has become more mature, the security of group communication remains challenging and relatively unexplored. People realize that SKG in group communication is not a simple extension of two-party communication. The demand for specific techniques to generate a group key in multi-user applications in group communication is relatively high [17,18].

As an extension of our previous work [1,34] that only concentrated on two-user application scenarios, this paper focuses on a wireless channel probing technique to generate a shared key for multiple users. The proposed multi-user channel probing scheme is based on broadcasting technology. Without losing generality, in this paper we consider three multi-user network topologies: single cluster, isolated multi-cluster, and networked multi-cluster. In order to meet multiple users' KGR requirement, we introduce an index called the Desired Weighting Factor (DWF). In addition, we employ a fuzzy controller to tune the probing rate for obtaining an actual KGR which is as close as possible to a desired value. We empower each user to have own desired KGR and corresponding DWF. Like the one-time pad cryptographic system, we try to increase the frequency of key changes in applications and provide a large desired-KGR value for high security consideration. In order to study the feasibility and applicability of the proposed SKG scheme on multi-user application scenarios, we experiment with different DWF values. For applications that either cannot tolerate any delay, any failure of key generation (e.g. videoconference), or are sensitive to the key generation rate, we set a large DWF value, while for ones that are not sensitive to the key generation rate we set a small DWF value.

In order to produce smaller overshoots and fewer oscillations, stabilize the KGR at desired values, improve the SKG accuracy, enhance the control capability, and increases the entropy rate, we use a fuzzy controller. The performance evaluation of the fuzzy controller is compared with the Proportional–Integral–Derivative (PID) controller in the proposed channel probing scheme.

The paper is organized as follows. Section 2 presents the system model, adversary model, and problem definition. Section 3 depicts the multi-user wireless channel probing scheme. Section 4 gives the test-bed setup. Section 5 presents experimental results and discussion, followed by a last section that gives conclusion with future work.

2. System model, adversary model and problem definition

2.1. System model

Assume there are N users in a wireless network, with each user considered as a node. Each user has equal communication and computation capacities. We term any two nodes within their communication coverage as a *pair*. Any pair holds a bidirectional wireless link. We consider two legitimate users (say Alice and Bob, as one of the pairs) who want to generate a shared key. Alice and Bob independently apply the following four steps [2]: channel probing, quantization, information reconciliation, and privacy amplification [19], respectively.

Channel probing is first used to collect wireless channel characteristics by legitimate users Alice and Bob. In this step, Alice and Bob exchange their request/reply probing frames within the duration T_p. Alice sends every probing request frame to Bob who instantly replies a packet back to Alice after he receives the request. We assume Alice sends the probing request frame with a fixed interval in single probing duration. At the end of the channel probing, Alice and Bob get channel measurements $\overrightarrow{H}_a$ and $\overrightarrow{H}_b$ respectively as

$$\begin{aligned}\overrightarrow{H}_a &= \{\hat{h}_a[1], \hat{h}_a[2], \hat{h}_a[3], \ldots, \hat{h}_a[N]\}^T \\ \overrightarrow{H}_b &= \{\hat{h}_b[1], \hat{h}_b[2], \hat{h}_b[3], \ldots, \hat{h}_b[N]\}^T\end{aligned} \tag{1}$$

where the superscript T denotes a matrix transpose and $\hat{h}_u[i]$ $(u = a, b; 1 \leqslant i \leqslant N)$ is the estimation of the channel characteristic $h_u[i]$ at time i. The subscript u stands for a user and $\overrightarrow{H}_a$ stands for the set of network channel characteristics in terms of a matrix or vector.

Quantization is used to convert the measured channel characteristics $\overrightarrow{H}_a$ and $\overrightarrow{H}_b$ into bit sequences. Information reconciliation is an error correction process carried out by both legitimate users in order to ensure that the keys generated separately on each side are identical [10]. During the reconciliation, some of the bitwise information may be revealed to an illegitimate user (Eve) from the eavesdropping during the communication between Alice and Bob.

Privacy amplification is a process to reduce or effectively eliminate Eve's partial information about the legitimate key and to minimize the correlation between the bits in a bit stream.

Any pair of legitimate network users would adopt these four processes. The details about how to implement the processes can be found in [2].

2.2. Adversary model

In an adversary model, we assume that there is an adversary (say Eve), who tries to break the key generation by eavesdropping on the communication among legitimate users. In this study, we make the following assumptions.

- Eve can read all the communication and can measure the channels.