

A Cross-Layer Key Establishment Scheme in Wireless Mesh Networks

Yuxin Zhang¹, Yang Xiang¹, Xinyi Huang^{1,2,*}, and Li Xu²

¹ School of Information Technology, Deakin University
Burwood, VIC 3125, Australia

² Fujian Provincial Key Laboratory of Network Security and Cryptology
School of Mathematics and Computer Science, Fujian Normal University
Fuzhou, 350108, China
{yuxinz,yang.xiang}@deakin.edu.au, {xyhuang,xuli}@fjnu.edu.cn

Abstract. Cryptographic keys are necessary to secure communications among mesh clients in wireless mesh networks. Traditional key establishment schemes are implemented at higher layers, and the security of most such designs relies on the complexity of computational problems. Extracting cryptographic keys at the physical layer is a promising approach with information-theoretical security. But due to the nature of communications at the physical layer, none of the existing designs supports key establishment if communicating parties are out of each other's radio range, and all schemes are insecure against man-in-the-middle attacks. This paper presents a cross-layer key establishment scheme where the established key is determined by two partial keys: one extracted at the physical layer and the other generated at higher layers. The analysis shows that the proposed cross-layer key establishment scheme not only eliminates the aforementioned shortcomings of key establishment at each layer but also provides a flexible solution to the key generation rate problem.

Keywords: Key establishment, Cross-layer, Coding, Channel phase, Wireless mesh networks.

1 Introduction

Wireless mesh networks (hereinafter, WMNs) becomes a research hotspot due to its low costs for deployment, easy expansion, and capability of self organization and self configuration. WMNs consists of two types of entities: mesh routers and mesh clients [1]. Mesh clients are stationary or mobile devices, and mesh routers form the mesh backbone for mesh clients. Each node (including mesh clients and mesh routers) in WMNs serves as a host and as a router, but mesh clients are not as powerful as mesh routers. As shown in Fig. 1, mesh clients can access the networks through mesh routers or meshing with other mesh clients directly [1].

* Corresponding author.

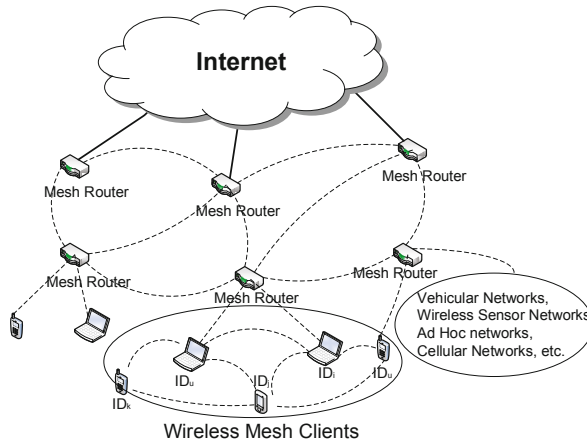


Fig. 1. Hybrid WMNs [1]

To secure wireless communications among clients, cryptographic keys are needed to provide confidentiality, integrity and authentication services. As a fundamental problem, key establishment has been extensively and intensively studied. Existing designs can be classified into two main types: asymmetric key establishment schemes and symmetric key establishment schemes. Most of them are implemented at higher layers (Fig. 2 shows the system model). However, there are some disadvantages in those schemes. For example, a large portion of them rely on the intractability of computational problems, and some of those problems will become tractable on quantum computers. Specifically, costly computation operations are needed to be executed in asymmetric key based schemes. In symmetric key based schemes, e.g., key pre-distribution schemes, considerable memory spaces are used to pre-load secrets.

To obtain communication keys with information-theoretical security, there is an increasing interest in extracting keys by exploiting the wireless channel. In the typical multipath environments, the wireless channel between two clients (e.g., Alice and Bob) experiences a time-varying, stochastic mapping between the transmitted and received signals. This mapping (commonly termed fading) is unique, location-specific and reciprocal, namely, the fading is invariant within the channel coherence time whether the signals are transmitted from Alice to Bob or vice-versa. In wireless communications, coherence time is a statistical measure of the time duration over which the channel impulse response is essentially invariant. Based on communication theory [2], the fading decorrelates over distances of the order of half a wavelength, λ . Thus, the signals transmitted between Alice and Bob and the signals transmitted between Alice (or Bob) and the eavesdropper (who is at least $\lambda/2$ away from the clients) experience independent fading. For instance, at 2.4 GHz used in IEEE 802.11b and 802.11g, these properties ensure that the eavesdropper cannot get useful information as long as it is roughly $\lambda/2 = 6.25$ cm away from Alice and Bob.

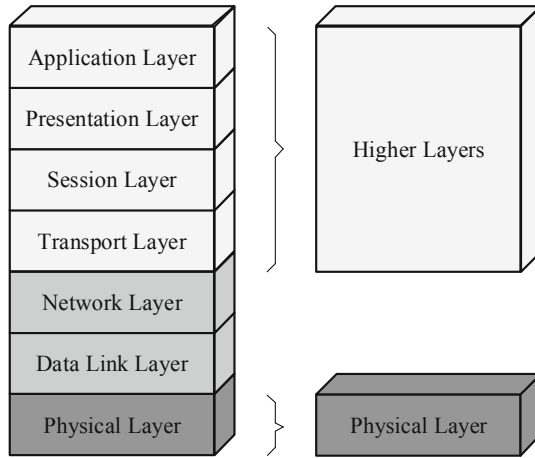


Fig. 2. The system model

But as a coin always has two sides, physical layer based key extraction schemes cannot establish communication keys securely when two clients are out of each other's radio range. It is due to the fact that the two clients must forward the fluctuated states to untrusted relay devices. Besides, the key generation rate of those schemes is quite slow (about 1 bit/sec, and more details will be given in Section 2.2), which constraints their applications.

Our Contribution. Many schemes have been proposed to extract secret keys from the wireless channel at the physical layer (a brief review of closely related works shall be given in Section 2), but few of them can securely and efficiently extract keys when two clients are out of each other's communication range. Facing the practical requirement, this paper presents a cross-layer key establishment scheme by employing the characteristics of the physical layer and higher layers corporately. Our scheme possesses the following properties:

1. Our scheme is specifically designed for assisting two remote mesh clients, who are out of each other's radio range, to establish a secure communication key;
2. In this paper we propose a cross-layer key establishment scheme. The channel phase is employed by clients to extract a partial key at the physical layer, and *XOR* coding is used to obtain another partial key at higher layers. The communication key is determined by these two partial keys;
3. The security of our scheme is guaranteed by two-fold: a partial key generated by coding at higher layers and the other partial key extracted via the wireless fading channel at the physical layer. Security analysis shows that our scheme is secure against man-in-the-middle attacks and node capture attacks; and
4. According to the needs of practical applications, e.g., security concerns and environmental conditions, the proposed design provides a flexible solution to

key generation rate problem. Clients in our scheme can dynamically adjust the length of the generated partial key (extracted at the physical layer). Definitely, a shorter partial key (extracted at the physical layer) will contribute to a higher key generation rate.

Organization of This Paper. The remainder of this paper is organized as follows. We present a brief overview on the related work in Section 2. Section 3 reviews the preliminaries required in this paper. The proposed scheme is described in Section 4, and its security and performance analysis is given in Section 5. Section 6 concludes this paper.

2 Related Work

A number of key establishment schemes were presented, for example, the Diffie-Hellman protocol allows two clients to establish a shared secret key over an insecure channel without prior knowledge. Symmetric key pre-distribution schemes, on the other hand, need to pre-load keys or secrets at clients. Due to restrictions on length, in this section we only focus on the closely related works.

2.1 Establish Keys Using *XOR* Coding

At higher layers, *XOR* coding technology was employed to establish secret keys in [3], where a mobile device S was used to bootstrap networks. In key pre-distribution phase, system authority: (a). produces a Vernam cipher R^1 , generates a large key pool P , and computes *XOR* coding blocks $\{K_i \oplus R\}$ s; (b). stores mobile device S with coding blocks $\{K_i \oplus R\}$ s and corresponding identifiers; and (c). selects r keys and key identifiers from key pool P for each sensor node. After deployment, S broadcasts *HELLO* messages and neighbor nodes A and B respond by sending their key identifiers. Upon receiving the identifiers id_A and id_B from node A and B respectively, mobile device S computes $K_i(A) \oplus R \oplus K_i(B) \oplus R$ and broadcasts $K_i(A) \oplus K_i(B)$. Based on the received *XOR* coding $K_i(A) \oplus K_i(B)$, A and B can easily recover each other's key (A owns $K_i(A)$, computes $K_i(A) \oplus K_i(A) \oplus K_i(B)$, and obtains $K_i(B)$. B can obtain $K_i(A)$ by executing similar operations). Then they can negotiate a communication key using $K_i(A)$ and $K_i(B)$. Liu et al. improved and applied it to a cluster-based hierarchical network in [5].

2.2 Extract Keys Using the Wireless Fading Channel

It is possible to extract secret bits from the physical layer, and the fundamental bounds are pointed out in [6, 7]. However, the authors of [6, 7] only provided theoretical results without giving explicit constructions. But it motivates other

¹ A Vernam cipher R is a binary sequence introduced in [4]. It is randomly generated according to a Bernoulli (1/2) distribution and its size is equal to the key size.

schemes using the attenuation of amplitude, deviation of phase or decline of other physical quantities to extract secret bits at the physical layer.

The attenuation of amplitude was employed to extract secrets in [8–11]. Mathur et al. used the crucial characteristics in [8] that the received signals at the receiver are modified by the channel in a manner unique to the transmitter-receiver pair. In Mathur et al.'s scheme, two wireless devices evaluated the envelope of multipath fading channel between them by probing a fixed test frequency, and quantized the evaluation into secret bits. Furthermore, the authors validated their algorithm using the 802.11a packet preamble on a FPGA-based 802.11 platform. They showed that it is possible to achieve key establishment rates of 1 bit/sec in a real indoor wireless environment. In [9], Received Signal Strength (RSS) was used as a channel statistic. By exploiting quantization, information reconciliation and privacy amplification, Jana et al. evaluated the effectiveness of secret key extraction from RSS variations in a variety of environments and settings. Besides, Vehicle-to-Infrastructure communication keys and Vehicle-to-Vehicle communication keys were extracted in [10]. In [11], an environment adaptive secret key generation scheme was proposed.

Deviation of phase (or phase offset) was used to extract secret bits in [12–15]. To increase the key bit generation rate, Zeng et al. exploited multiple-antenna diversity in [12] to generate secret keys for wireless nodes and implemented it on off-the-shelf 802.11n multiple-antenna devices. Pairwise key generation approach and group key generation approach were presented in [13] by utilizing the uniformly distributed phase information of channel responses under narrowband multipath fading models. A cooperative key generation protocol was proposed in [14] to facilitate high rate key generation in narrowband fading channels with the aid of relay node(s). Zhuo et al. [15] presented a multihop key establishment scheme based on the assumption that the network is biconnected, and the security of [15] is guaranteed against adversaries in a single path.

It is also proved in [16, 17] that decline of other physical quantities are available to extract secret bits. Liu et al. came up with a novel idea to extract cryptography keys in [16]. Noticing that the fading exhibited in RSS measurements follows similar increasing or decreasing trend despite of the mismatch of absolute values, they proposed a fading trend based secret key extraction scheme. Liu et al. presented another idea in [17] to mitigate the non-reciprocity component by learning the channel response from multiple Orthogonal Frequency-Division Multiplexing (OFDM) subcarriers.

However, there are some practical requirements that schemes [8–17] failed to securely fulfill. For example, (1). It is a practical requirement in WMNs that two remote clients should establish a secret key to secure their communications. The schemes in [15, 16] provide solutions to fulfill this requirement, but some problems still exist in their schemes. The proposed scheme in [15] is based on the assumption that the network is biconnected, i.e., there are at least two disjoint paths between any pair of nodes. This assumption limits its practicality. In [16], a collaborative key extraction scheme is designed under the assistance of relay nodes. However, the extracted key is not secure as it is known by one of the

relay nodes; (2). Designed schemes should be secure against man-in-the-middle attacks. Until now, the existing physical layer based key extraction schemes failed to secure against this kind of attacks. Realizing that it is possible to utilize the characteristics of the physical layer and higher layers cooperatively to meet foregoing requirements, in this paper we present a cross-layer key establishment scheme. At higher layers, we use coding to gain partial secrets; At the physical layer, we employ the channel phase to extract other partial secrets. The details of our scheme will be described in Section 4.

3 Preliminaries

This section presents some preliminaries required in this paper.

3.1 Extract Secret Bits from the Wireless Fading Channel

The characteristic of the wireless channel between two wireless devices provides them an access to extract secret keys, even in the presence of an eavesdropper [8, 9]. An example is given in Fig. 3.

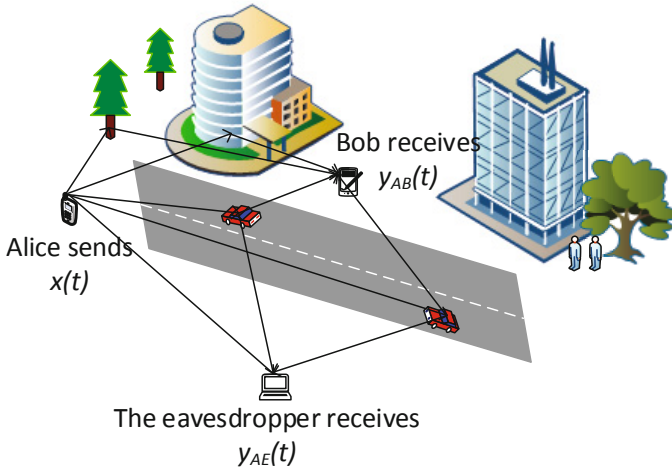


Fig. 3. An example of fading

In Fig. 3, Alice sends a sinusoidal signal $x(t) = A \sin(w_c t + \phi_0)$ to Bob. Here A is the amplitude, w_c is the angular frequency, and ϕ_0 is the initial phase. Due to the multipath environment, noise, and/or mobile environment, the sinusoidal signals received at Bob and the eavesdropper are different. Let $y_{AB}(t)$ and $y_{AE}(t)$ denote the signals received by Bob and the eavesdropper, and they can be written as:

$$\begin{aligned} y_{AB}(t) &= A_{AB} \sin(w_c t + \phi_0 + \phi_{AB}) + n_{AB}(t), \\ y_{AE}(t) &= A_{AE} \sin(w_c t + \phi_0 + \phi_{AE}) + n_{AE}(t). \end{aligned}$$

Here, A_{AB} and A_{AE} are the modulated amplitudes, and they are functions of path loss and shadowing; ϕ_{AB} and ϕ_{AE} are the deviated phases, and they are depend on delay, Doppler, and carrier offset ². $n_{AB}(t)$ and $n_{AE}(t)$ denote the additive white Gaussian noise.

Upon receiving $y_{AB}(t)$, Bob sends the signal $x(t) = A \sin(w_c t + \phi_0)$ back to Alice in the coherence time. Similarly, Alice and the eavesdropper will receive $y_{BA}(t)$ and $y_{BE}(t)$, and they can be written as:

$$\begin{aligned} y_{BA}(t) &= A_{BA} \sin(w_c t + \phi_0 + \phi_{BA}) + n_{BA}(t), \\ y_{BE}(t) &= A_{BE} \sin(w_c t + \phi_0 + \phi_{BE}) + n_{BE}(t). \end{aligned}$$

By assuming that key extraction operations are executed in the coherence time, we have $\phi_{AB} = \phi_{BA}$. If the eavesdropper is more than $\lambda/2$ away from Alice and Bob, it cannot extract any useful secrets by making use of his received signals. Taking Fig. 3 as an example, ϕ_{AE} and ϕ_{AB} (ϕ_{BE} and ϕ_{BA}) are statistically independent as long as the eavesdropper is more than $\lambda/2$ away from Bob (Alice).

3.2 Assumptions

There are three types of participants in our cross-layer key establishment scheme, i.e., the system authority, mesh routers and mesh clients. We assume that:

1. Operations related to the system authority are carried out in a secure environment, while mesh routers and mesh clients are not physically secure. Particularly, mesh routers are equipped with tamper-detection technology and they can erase secret information when captured. However, any secret data stored in mesh clients will be exposed once they are captured by adversaries;
2. The area of mesh clients is covered by the wireless transmission radius of mesh routers;
3. A mesh client is able to securely apply for a secret S from the system authority for the first time it joins the mesh networks; and
4. Key extraction operations at the physical layer are executed in the coherence time to ensure $\phi_{AB} = \phi_{BA}$ as shown in Section 3.1.

3.3 Adversary Model

As assumptions made in [8–17], the adversary is at least $\lambda/2$ away from legitimate clients, and it can eavesdrop the communications among clients. We also assume that the adversary knows the key establishment scheme and it can perform phase estimation during key generation process. In addition, the adversary aims to derive the secret keys generated between legitimate mesh clients, and

² Path loss, shadowing, delay, Doppler, and carrier offset are components in analysis of a communication system. Please refer to [2] for more information.

it is not interested in interrupting the key generation scheme by jamming the communications. Different from the schemes in [8, 9, 13], we assume that relay clients are not fully trusted, and node capture attacks and man-in-the-middle attacks are considered in this paper.

4 A Cross-Layer Key Establishment Scheme in WMNs

This section is devoted to the description of our cross-layer key establishment scheme for two mesh clients who are beyond each other's communication range.

4.1 Overview

As shown in Fig. 4, the scheme consists of five phases, and details of each phase will be followed in Section 4.2.

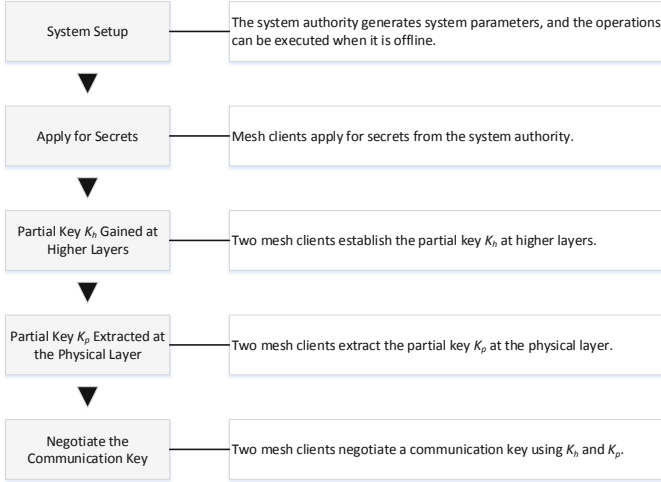


Fig. 4. Five phase of our cross-layer key establishment scheme

4.2 A Cross-Layer Key Establishment Scheme

System Setup: Assume that the population of residents in a community is P . For each individual, there are about Q devices (like PC s or phones) may serve as mesh clients and access the WMNs through mesh routers or directly meshing with other mesh clients. It means that there are about $M = PQ$ mesh clients in this area. During the system setup phase, the system authority

- Chooses N independent secrets S_1, S_2, \dots, S_N from a finite field GF_q , for $N \geq M$. Let id_i be the identifier of secret S_i ;

- Computes $S_i^2, S_i^3, \dots, S_i^e$, for $i = 1, 2, \dots, N$. e is the expected times that secret S_i be used to establish communication keys;
- Chooses a secure hash function $H(x)$;
- Produces Vernam cipher R_{ij} s, i.e., binary sequences drawn randomly according to a Bernoulli ($\frac{1}{2}$) distribution. Here $i = 1, 2, \dots, N$, $j = 1, 2, \dots, N$, and $i \neq j$. The generated R_{ij} s should possess the characteristic that $R_{ij} = R_{ji}$;
- Computes coding blocks $\{H(S_i^k) \oplus R_{ij}\}$ s, for $2 \leq k \leq e$; and
- Loads $\{id_i, k : H(S_i^k) \oplus R_{ij}\}$ s at mesh routers.

To facilitate understanding, we provide a flowchart of computing coding blocks in Fig. 5. Note that R_{ij} s possess the characteristic $R_{ij} = R_{ji}$.

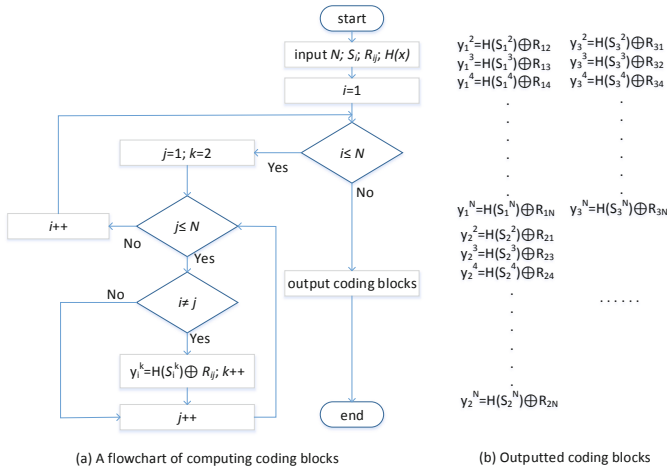


Fig. 5. A flowchart of computing coding blocks

Apply for Secrets: We assume that mesh client i is able to apply for a secret S_i and the corresponding secret identifier id_i from the system authority securely for the first time it joins the mesh networks.

Partial Key K_h Gained at Higher Layers: When two mesh clients u and v want to establish a communication key, they should execute following operations:

- Say *HELLO* to each other and exchange secret identifiers id_u, id_v . This operation can be completed by employing forward function of multiple relay clients; and
- Send a request, $\{\text{req}: id_u, id_v\}$, to mesh routers.

Upon receiving the request, mesh routers retrieve the stored coding blocks $\{id_i, k : H(S_i^k) \oplus R_{ij}\}$ s and reply mesh clients u, v with $\{id_u, x; id_v, y : H(S_u^x) \oplus H(S_v^y) = H(S_u^x) \oplus R_{uv} \oplus H(S_v^y) \oplus R_{vu}\}$ publicly.

Then, mesh clients u and v :

- Compute $H(S_v^y)$ and $H(S_u^x)$, separately. Taking client u as an example, it owns S_u , computes $H(S_u^x)$ and $H(S_u^x) \oplus H(S_u^x) \oplus H(S_v^y)$, and obtains $H(S_v^y)$. Client v can obtain $H(S_u^x)$ by executing similar operations;
- Negotiate the partial key K_h using $H(S_u^x)$ and $H(S_v^y)$. For example, client u and v can compute $K_h = H(H(S_u^x) \| H(S_v^y))$. Here, $\|$ is the connection operation.

Partial Key K_p Extracted at the Physical Layer: The basic idea of key extraction algorithms at the physical layer is to employ the inherent channel randomness associated with distinct pairwise links, i.e., the sinusoidal signal transmitted back and forth between two mesh clients will experience the same phase variation over the coherence time period. We assume that there are x relay clients between u and v , denoted as r_1, r_2, \dots, r_x . As depicted in [13], the key extraction scheme contains $|K_p|/\log_2(q)$ round, and there are two time slots (ST_1 and ST_2) in each round. Here $|K_p|$ is the length of K_p . In ST_1 :

- Mesh client u chooses ϕ_1 uniformly at random from $[0, 2\pi]$, and sends the sinusoidal signal $x(t) = A \sin(w_c t + \phi_1)$ to relay client r_1 ;
- Relay client r_i forwards the signal to relay client r_j , where $r_i, r_j \in \{r_1, r_2, \dots, r_x\}$ and $1 \leq i < j \leq x$;
- Relay client r_x forwards the signal to mesh client v .

The steady-state portion of the beacon received at mesh client v can be written as

$$y_{u \rightarrow v}(t) = A' \sin(w_c t + \phi_1 + \phi_{ur_1} + \phi_{r_1 r_2} + \dots + \phi_{r_x v}) + n'(t),$$

where $n'(t)$ denotes the additive white Gaussian noise, and ϕ_{ij} denotes the phase offset when the signal is transmitted from client i to client j . After ST_1 , client v gets $\phi_{u \rightarrow v} = \phi_1 + \phi_{ur_1} + \phi_{r_1 r_2} + \dots + \phi_{r_x v}$. In ST_2 :

- Mesh client v chooses ϕ_2 uniformly at random from $[0, 2\pi]$ and sends the sinusoidal signal $x(t) = A \sin(w_c t + \phi_2)$ to relay client r_x ;
- Relay client r_j forwards the signal to relay client r_i , where $r_i, r_j \in \{r_1, r_2, \dots, r_x\}$ and $1 \leq i < j \leq x$;
- Relay client r_1 forwards the signal to mesh client u .

Similarly, the steady-state portion of the beacon received at mesh client u can be written as

$$y_{v \rightarrow u}(t) = A'' \sin(w_c t + \phi_2 + \phi_{vr_x} + \phi_{r_x r_{x-1}} + \dots + \phi_{r_1 u}) + n''(t).$$

After ST_2 , client u obtains $\phi_{v \rightarrow u} = \phi_2 + \phi_{vr_x} + \phi_{r_x r_{x-1}} + \dots + \phi_{r_1 u}$.

At the end of first round, both client u and v can compute the phase components Φ_1

$$\text{client } u : \quad \Phi_1 = \phi_{v \rightarrow u} + \phi_1 \bmod 2\pi,$$

$$\text{client } v : \quad \Phi_1 = \phi_{u \rightarrow v} + \phi_2 \bmod 2\pi.$$

As shown in [13], we can map Φ_1 into the quantization inter/index using the formula:

$$Q_x = k \quad \text{if } x \in [\frac{2\pi(k-1)}{q}, \frac{2\pi k}{q}),$$

for $k = 1, 2, \dots, q$. Thus, the quantization of phase value generates $\log_2(q)$ bits secret. To extract the partial key K_p with length $|K_p|$, mesh clients u and v need to repeat the operations (presented in ST_1 and ST_2) for $|K_p|/\log_2(q)$ round.

Due to the presence of noise and interference, manufacturing variations, half-duplex mode of communication and estimation errors, *secure sketch* can be applied to reconcile the differences in the bit streams (refer to [13] for details).

Negotiate the Communication Key: After completing the aforementioned operations, mesh clients u and v obtain shared partial keys K_h and K_p . Then they can negotiate the communication key K using K_h and K_p . For example, the communication key can be computed as: $K = H(K_h \| K_p)$.

This completes the description of our cross-layer key establishment scheme.

5 Security and Performance Analysis

In this section, we analyze the security and performance of our cross-layer key establishment scheme.

5.1 Security Analysis

The security of our proposed cross-layer key establishment scheme is guaranteed by two-fold: the partial key K_h generated at higher layers and the partial key K_p extracted at the physical layer.

At higher layers, coding is employed to ensure the security of the partial key K_h . Under the assumption that a mesh client is able to apply for a secret S from system authority securely for the first time it joins the mesh networks, any pair of clients can compute and obtain K_h . Take **Partial Key K_h Gained at Higher Layers** as an example, only clients u and v can decode $H(S_u^x) \oplus H(S_v^y)$, obtain $H(S_v^y)$ and $H(S_u^x)$, and compute $K_h = H(H(S_u^x) \| H(S_v^y))$ correctly.

At the physical layer, it is widely assumed that an adversary cannot obtain the identical channel response for key generation if it is at least $\lambda/2$ away from communicating clients [8–17], and this has been validated in real experiments in [8, 9]. During **partial key K_p extracted at the physical layer** phase, the adversary will experience independent channel variations as long as it is more than 6.25 cm away from the communicating nodes. Here we let the carrier frequency be 2.4 GHz. In our scheme, the communicating nodes include clients u , v and relay clients r_1, r_2, \dots, r_x .

Resilience against Man-in-the-Middle Attacks. When the fading channel is employed to extract secret keys, Mathur et al. pointed out in [8] that two clients will suffer from man-in-the-middle attacks if they are not within each

other's communication range. Just as other physical layer based schemes, the partial key K_p extracted from the wireless fading channel are vulnerable to man-in-the-middle attacks. But the communication key K generated in our scheme is secure against such kind of attacks. The reason is that the communication key in our scheme is computed as: $K = H(K_h || K_p)$. Recall that K_h is computed by coding at higher layers. Without secret S_u or S_v , an attacker cannot compute K_h correctly. So it cannot cheat the communicating clients. The cross-layer key establishment design makes the scheme resist against man-in-the-middle attacks when two clients are beyond each other's radio range.

Resilience against Node Capture Attacks. Our cross-layer key establishment scheme is secure against node capture attacks. Assume that the adversary obtains a secret S_w by capturing client w . It can impersonate client w and try to establish communication key with legitimate client v . The adversary can obtain $H(S_v^y)$ after mesh routers replied $H(S_w^x) \oplus H(S_v^y)$. However, it cannot obtain $H(S_v^{y-1})$ or $H(S_v^{y+1})$ by using $H(S_v^y)$ due to the one way hash function. Furthermore, it cannot obtain those clients' secrets who established communication keys with client v , because client v establishes communication keys with different clients using different secret codings. For coding $H(S_v^y) \oplus R_{vw}$, it is only used between clients w and v . So, the leak of a secret in our scheme will not contribute to other secrets' insecurity.

5.2 Performance Analysis

Probability of Successful Partial Key Generation. During **partial key K_p extracted at the physical layer** phase, each node (source node and destination node) generates an initial phase randomly. As assumed in [13], all observations in different time slots or at different nodes are affected by independent noise realizations. Let T_0 be the observation time, f_s be the sampling rate and N be the number of samples in the observation. The estimation errors converge to zero-mean Gaussian random variables with variances σ_ϕ^2 when N increases, and it can be lower-bounded by the Cramer-Rao bounds (CRB) [18]. Recall that the amplitude of the transmitted sinusoid signal is A , when estimating it in white noise with Power Spectral Density (PSD) $\frac{N_0}{2}$, the CRBs for the variance of the phase estimate is given as (refer to schemes [13, 18] for details)

$$\sigma_\phi^2 \geq \frac{2f_s N_0 (2N - 1)}{A^2 N (N + 1)} \approx \frac{4N_0}{A^2 T_0} \quad (1)$$

When N is sufficiently large, $\frac{f_s}{N} = \frac{1}{T_0}$. As described in **Partial key K_p Extracted at the Physical Layer**, there are x relay nodes. Thus, the variance of the accumulated estimation errors across $x + 2$ nodes is $\sigma_{(x+2)}^2 = (x + 2)\sigma_\phi^2$. Wang et al. present the average probability of quantization index agreement P_{QIA} in [13] as

$$P_{QIA} = \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} P_{QIA}(\phi) \frac{q}{2\pi} d\phi \approx \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} P_i^{(x+2)}(\phi) \frac{q}{2\pi} d\phi \quad (2)$$

$$\text{where } P_i(\phi) = \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} \frac{1}{\sqrt{2\pi\sigma_{(x+2)}}} e^{-\frac{(y-\phi)^2}{2\sigma_{(x+2)}}} dy.$$

Randomness of Key. To extract high entropy secret bits from wireless fading channel, most of the related schemes rely on node mobility or channel variations. In a static environment the adversary has the ability to predict the changes of channel phase when clients u and v are stationary (it is pointed out in [9, 17]). However, our cross-layer key establishment scheme can provide communication keys with sufficient randomness even in a static environment. In our scheme, ϕ_1 and ϕ_2 are chosen uniformly at random from $[0, 2\pi]$ by clients u and v respectively, which contributes to the randomness of the partial key K_p . Besides, secrets S_u, S_v are generated randomly by the system authority, the partial key K_h is obtained by $K_h = H(H(S_u^x)||H(S_v^y))$, and the communication key is computed as $K = H(K_h||K_p)$. Due to the randomness of K_p and K_h , our scheme can provide random communication keys in the dynamic or static environment.

Key Rate. Due to the fact that in the time slots where the channel changes slowly, a limited number of key bits can be generated. It has been investigated by previous work in [8] that two wireless clients can generate a communication key at about 1 bit/sec by using off-the-shelf 802.11a hardware. This constraint significantly limits their practical applications [14]. The cross-layer key establishment scheme provides a flexible solution to this limitation. In practical applications, clients in our scheme can dynamically adjust the length of the generated partial key K_p based on actual application requirements, e.g., security concerns and environmental conditions. Definitely, a short partial key K_p will save the partial key generation time at the physical layer, and this will contribute to a high key generation rate. Our cross-layer key establishment scheme will degrade to *XOR* coding based scheme when the length of partial key K_p is “0”.

Storage, Communication and Computation Complexities. We consider the storage, communication and computation costs of our scheme from two parts: the partial key K_h generated at higher layers and the partial key K_p extracted at the physical layer. To obtain the partial key K_h , client u needs to: (a). apply a secret S_u and the corresponding secret identifier id_u from the system authority; (b). exchange identifiers id_u, id_v with client v and send request $\{\text{req: } id_u, id_v\}$ to mesh routers; (c). compute K_h using S_u after receiving $\{id_u, x; id_v, y : H(S_u^x) \oplus H(S_v^y)\}$. To extract partial key K_p , client u needs to repeat the operations (presented in ST_1 and ST_2) for $|K_p|/\log_2^{(q)} = 16$ rounds when $|K_p| = 64$ bits and $q = 16$.

Specifically, our cross-layer key establishment scheme will degrade to *XOR* coding based scheme when $|K_p| = 0$. In this case, our scheme has the same security level as [3, 5]. Recall that each node needs to pre-load r keys and $N - 1$ coding blocks in [3] and [5], respectively. So, our scheme has a significant advantage over [3, 5] from the aspect of storage costs at clients. The light storage costs

at mesh clients are achieved by migrating all coding blocks to mesh routers (recall that mesh routers have much more storage space than clients). To establish communication keys, clients need to exchange identifiers. Obviously, communication costs of clients in our scheme are the same with [3, 5]. However, comparing with schemes [3, 5], computation costs are higher in our scheme. Because client u in [3, 5] only needs to execute *XOR* coding, but it needs to compute S_u^x , $H(S_u^x)$, and *XOR* coding in our scheme.

We now compare the computation cost of our cross-layer key establishment scheme (consumed at higher layers when computing S_u^x) with the technique of asymmetric key cryptography. To achieve a security level of 80-bit, our scheme shall require one modular exponentiation with the length of 40-bit when $|K_h| = |K_p| = 40$, while it requires at least one modular exponentiation with the length of 1024-bit using asymmetric key techniques such as the RSA.

Take sensor node MICAz mote as an example, it is equipped with an 8-bit AVR processor (the ATmega128) and has only 4 kB of RAM and 128 kB flash memory [19]. To the best of our knowledge, the fastest software implementation of modular multiplication (mod-mul) for such 8-bit AVR processors roughly requires 240 clock cycles for operand with a length of 40-bit and roughly 220596 clock cycles for a 1024-bit operand. It means that the costs of performing a 1024-bit modular multiplication equal to 920 times of performing a 40-bit modular multiplication. It is the same case for modular squaring (mod-sqr). Thus, we have

$$\begin{aligned}\text{mod-mul-1024} &= 920 \times \text{mod-mul-40, and} \\ \text{mod-sqr-1024} &= 920 \times \text{mod-sqr-40}.\end{aligned}$$

The basic method to perform modular exponentiation (mod-exp) is called “square-and-multiply” method. Take an n -bit modular exponentiation as an example, the computation costs for the modular exponentiation roughly need n times modular squaring and $n/2$ times modular multiplication operations. In this case, the computation costs of modular exponentiation are

$$\begin{aligned}\text{mod-exp-1024} &= 1024 \times \text{mod-sqr-1024} + 512 \times \text{mod-mul-1024} \\ &= (1024 \times 920 \times 0.8 + 512 \times 920) \times \text{mod-mul-40} \\ &= 1224704 \times \text{mod-mul-40, and} \\ \text{mod-exp-40} &= 40 \times \text{mod-sqr-40} + 20 \times \text{mod-mul-40} \\ &= 52 \times \text{mod-mul-40.} \\ (\text{mod-sqr} &= 0.8 \times \text{mod-mul})\end{aligned}$$

So, one 1024-bit modular exponentiation is at least 20000 times more expensive than one 40-bit modular exponentiation.

We can accelerate the 1024-bit modular exponentiation using hardware acceleration technologies: The implementation of modular multiplication for a 1024-bit operand can be accelerated to $3\mu\text{s}$ with a hardware accelerator [20]. Together with micro controllers running at a frequency of 8MHz, a 1024-bit modular multiplication only requires $3\mu\text{s} \times 8M = 24$ clock cycles. This can also meet the

practical requirement³. But in wireless mesh networks, mesh clients consist of various devices, including laptop/desktop PC, pocket PC, PDA, IP phone, RFID reader, BACnet (building automation and control networks) controller and tiny wireless sensor nodes. Assuming each device with hardware acceleration would be too strong to hold in certain situations. It is obvious that an efficient protocol without the need of hardware acceleration, such as the one proposed in this paper, can better suit the nature of wireless mesh networks.

6 Conclusion

As a fundamental security technology, key establishment has been widely studied in wireless mesh networks. Many key establishment schemes are proposed, and they are implemented at the physical layer or higher layers. However, due to the characteristics of these layers, there are some inherent disadvantages in those schemes. This paper presents a cross-layer key establishment scheme, with which the communication key is determined by two partial keys: one extracted at the physical layer and the other generated at higher layers. The analysis shows that the proposed cross-layer key establishment scheme not only eliminates the shortcomings of key establishment at each layer but also provides a flexible solution to the key generation rate problem.

Acknowledgement. The authors would like to thank anonymous reviewers for their helpful comments, and Dr. Zhe Liu (from the University of Luxembourg) for his generous sharing of simulation data.

Xinyi Huang is supported by Distinguished Young Scholars Fund of Department of Education, Fujian Province, China (JA13062), Fok Ying Tung Education Foundation (Grant NO. 141065), National Natural Science Foundation of China (Grant NO. 61202450), Ph.D. Programs Foundation of Ministry of Education of China (Grant NO. 20123503120001) and Fujian Normal University Innovative Research Team (NO. IRTL1207).

References

1. Akyildiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: A survey. *Computer Networks* 47(4), 445–487 (2005)
2. Goldsmith, A.: *Wireless communications*. Cambridge University Press (2005)
3. Oliveira, P.F., Barros, J.: A network coding approach to secret key distribution. *IEEE Transactions on Information Forensics and Security* 3(3), 414–423 (2008)
4. Vernam, G.: Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.* 45(2), 109–115 (1926)

³ To be more precise, a 1024-bit modular multiplication with hardware acceleration is roughly 10 times more efficient than a 40-bit modular multiplication without hardware acceleration.

5. Liu, J., Sangi, A.R., Du, R., Wu, Q.: Light weight network coding based key distribution scheme for MANETs. In: Lopez, J., Huang, X., Sandhu, R. (eds.) NSS 2013. LNCS, vol. 7873, pp. 521–534. Springer, Heidelberg (2013)
6. Maurer, U.M.: Information-theoretically secure secret-key agreement by not authenticated public discussion. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 209–225. Springer, Heidelberg (1997)
7. Maurer, U.M., Wolf, S.: Secret-key agreement over unauthenticated public channels I: Definitions and a completeness result. *IEEE Transactions on Information Theory* 49(4), 822–831 (2003)
8. Mathur, S., Trappe, W., Mandayam, N.B., Ye, C., Reznik, A.: Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In: MOBICOM, pp. 128–139. ACM (2008)
9. Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N., Krishnamurthy, S.V.: On the effectiveness of secret key extraction from wireless signal strength in real environments. In: MOBICOM, pp. 321–332. ACM (2009)
10. Zan, B., Gruteser, M., Hu, F.: Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems. *IEEE Transactions on Vehicular Technology* 62(8), 4020–4027 (2013)
11. Premnath, S.N., Jana, S., Croft, J., Gowda, P.L., Clark, M., Kasera, S.K., Patwari, N., Krishnamurthy, S.V.: Secret key extraction from wireless signal strength in real environments. *IEEE Transaction on Mobile Computing* 12(5), 917–930 (2013)
12. Zeng, K., Wu, D., Chan, A.J., Mohapatra, P.: Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In: INFOCOM, pp. 1837–1845. IEEE (2010)
13. Wang, Q., Su, H., Ren, K., Kim, K.: Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: INFOCOM, pp. 1422–1430. IEEE (2011)
14. Wang, Q., Xu, K., Ren, K.: Cooperative secret key generation from phase estimation in narrowband fading channels. *IEEE Journal on Selected Areas in Communications* 30(9), 1666–1674 (2012)
15. Hao, Z., Zhong, S., Yu, N.: A multihop key agreement scheme for wireless ad hoc networks based on channel characteristics. *The Scientific World Journal* 2013 (2013)
16. Liu, H., Yang, J., Wang, Y., Chen, Y.: Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In: INFOCOM, pp. 927–935. IEEE (2012)
17. Liu, H., Wang, Y., Yang, J., Chen, Y.: Fast and practical secret key extraction by exploiting channel response. In: INFOCOM, pp. 3048–3056. IEEE (2013)
18. Rife, D.C., Boorstyn, R.: Single tone parameter estimation from discrete-time observations. *IEEE Transactions on Information Theory* 20(5), 591–598 (1974)
19. Liu, Z., Großschädl, J., Wong, D.S.: Low-weight primes for lightweight elliptic curve cryptography on 8-bit AVR processors. In: INSCRYPT 2013. LNCS. Springer (2013)
20. Lin, W.C., Ye, J.H., Shieh, M.D.: Scalable montgomery modular multiplication architecture with low-latency and low-memory bandwidth requirement. *IEEE Transactions on Computers* 63(2), 475–483 (2014)