On the Possibility of Key Agreement Using Variable Directional Antenna

Hideki Imai[12], Kazukuni Kobara[21], and Kirill Morozov[21]

[1] Department of Electrical, Electronic and Communication Engineering,
Chuo University, Japan
[2] National Institute of Advanced Industrial Science and Technology (AIST), Japan
{h-imai,k-kobara,kirill.morozov}@aist.go.jp

Abstract. This paper evaluates security of the key agreement system for wireless networks proposed recently by Aono et al. This system exploiting the reciprocal property of radio communication channel shows a high potential for providing unconditional security where protection is provided even against an eavesdropper with *unlimited* computing power. However, a rigorous security analysis was missing there. In this work, we move towards it: we define and compute the information measures characterizing for the legitimate parties and the eavesdropper their uncertainty about the generated key. Furthermore, we show a method for choosing parameters of this system such that the parties succeed in generating a common key while the adversary is ignorant about it with high probability. We also point out that the system needs strengthening using *privacy amplification* in order to achieve unconditional security under some reasonable (as we shall argue) assumptions: a) that an eavesdropper did not intercept more information on the key candidates than he is expected to; and b) truly random number generation. To illustrate our results, we provide a number of experimental measurements (performed in the typical wireless network environment) which allow us to conclude that using this system one can achieve unconditionally secure key agreement as long as the eavesdropper is not located too close (at the order of tens of centimeters) to the players.

1 Introduction

Wireless Local Networks (WLAN) have become popular in the recent years. At the same time, security concerns arose in different aspects and, in particular, in the key management [11]. The main motivation for our work is to resolve the key establishment problem in an ultimate way: We investigate a key establishment system with *unconditional* (or *information-theoretic*) security. Key establishment includes a process of key agreement, when two interacting legitimate users generate a common key which is unknown to the adversary who intercepts on their communication, and a process of key transport when a secure key generated by one of the users is securely delivered to the others. In this work, we consider only key agreement between the two legitimate parties (we shall call them just the "parties" or "the players"). In unconditional setting, the security is provided in information-theoretic sense: the adversary (or the "eavesdropper") can only obtain a negligible (in some security parameter) information about the shared key. This implies that protection is guaranteed even against eavesdroppers with *unlimited* computing power.

A general scenario for unconditionally secure key agreement was first presented by Wyner in his seminal paper [20]. It was followed by extensive research on key agreement based on the noisy communications modeled as discrete memoryless channels, finalizing in an excellent series of papers by Maurer and Wolf, see [14–16] and the references therein.

This area however, did not receive a lot of attention by engineers as the main problem had resided in providing a substantial (and guaranteed) advantage to the players over the eavesdropper in terms of noise. The channel connecting the parties (the *main* channel) should be less noisy than that connecting the parties with the eavesdropper (the *wire-tap* channel). Although without such the advantage unconditional key agreement remains theoretically possible [13], its practical implementation would have rather high communication complexity.

The recent development and increasing popularity of mobile and wireless networks raised security concerns for these areas. In particular, for key-exchange it was desirable to obtain a higher protection than the current conventional cryptography provides. In 1995, a novel approach by Hershey, Hassan and Yarlagadda [8] was introduced. Their idea was to exploit the reciprocal property of radio communication channel which provides that for two communicating entities, for a short period of time, the channel has similar properties in both directions. In other words, at those moments the two parties must experience noise with very similar error patterns, if they do not move too fast. In order to obtain those patterns, they exchange some publicly known message in a short time interval. For instance, a party A sends a zero-vector to a party B, then upon receiving this message (which is, in fact, the error pattern), B immediately replies with a zero-vector. A obtains his error pattern, which will be very similar to the B's one. Now, these error patterns can be used for computing the common key shared by A and B. Security here comes from the fact that given the complex properties of a real communication channel, it is quite hard for the eavesdropper to learn the error patterns of the parties unless the eavesdropper manages to intercept very near to either of them. We emphasize that the good receiving equipment does not immediately give the adversary a big advantage as his location with respect to the parties is also very important. At the same time, the players need to randomize their patterns from one transmission to the other, otherwise the generated common keys will be highly dependent. In [8], it was proposed to implement this scheme using mobile radio, where randomization is provided by changing environment as the users move.

Recently, Sasaoka et al. [1] have built an implementation of such key agreement system for WLAN. As in a standard office environment, most of the terminals usually remain in a fixed position most of the time, the randomization of error patterns is provided by exploiting a kind of variable directional antenna – electrically steerable parasitic array radiator (ESPAR) [12] – in order to make the reciprocal property work analogously to [8]. The parties in this system are an access point (AP) equipped with ESPAR and the user terminal (UT). The difference compared to [8] is that a fluctuation of a received signal strength indicator (RSSI) [3] rather than a fluctuation of delay profiles is used. However – although being efficient and practical – the system [1] does not provide unconditional (but only computational) security for the parties. The reason is that it releases a substantial amount of information on the key as the parties publicly exchange its parity check bits as well as its hash value for confirmation.

1.1 Related Results

The related result is the work of Barros and Rodriquez [4] where the noisy channel is modeled as a quasi-static Rayleigh fading channel. They show an (existential) possibility result for unconditionally secure key agreement in this model. Basically, it is the same model as ours because the reciprocal property is a direct consequence of multipath fading in radio communications. The difference is that in their idealized model, the parties have advantage over the eavesdropper only in some particular transmissions but not all the time as the empirical reciprocal property suggests. Hence, this interesting possibility result is non-constructive as in a practical implementation, one must enable the parties to learn which transmissions are advantageous to them.[4]

A constructive result on practical unconditionally secure key agreement in the Gaussian wiretap scenario by Bloch et al. [5] constructs and optimizes the LDPC codes which perform well in this scenario. However, for this scheme to be suitable for practical implementation, the parties must know for sure the location of the eavesdropper that is not always possible in the real life.

1.2 Our contribution

The contributions of this paper are:

1. A rigorous security analysis for the scheme [1] (in the case of passive eavesdropping) and pointing out the necessary (simple) modifications with which the system can be used for unconditionally secure key agreement; the modified system must in addition use the standard approach with employing *privacy amplification* which allows for reducing (to a negligible value) the eavesdropper's information on the key.
2. New experimental results as compared to [1]. These experiments conducted in a typical WLAN installation have confirmed that the modified scheme is efficient and practical.
3. Discussion on practical aspects of unconditionally secure key agreement implementation using the presented approach.

[3] Basically, RSSI is a measured amplitude of a received radio signal on some fixed frequency.

[4] However, it is claimed in [4] that this can be arranged in time-division multiple access (TDMA) systems.

To our best knowledge, this is one of the first[5] practical schemes which allows for unconditionally secure key agreement based on noisy radio communication.

The paper is organized as follows: in Section 2, we provide some brief information on technology and hardware used for this system as well as underlying tools from coding theory, and some cryptographic definitions. Section 3 presents the proposed key agreement system, while its security analysis is provided in Section 4. Section 5 contains our experimental results. Finally, we provide concluding remarks and open questions in Section 6.

2 Preliminaries

2.1 Technology and Hardware

The proposed key agreement scheme is designed for use in a standard wireless network setting (for instance, an office). Usually, access points and user terminals are equipped with standard antennas which are omni-directional, i.e., they radiate, roughly speaking, in all the directions with equal strength. Furthermore, the parties do not move too often and too fast and so do the usual reflectors and absorbers of the electromagnetic waves, such as furniture, equipment and others. Therefore, unlike in a mobile radio communication scenario,[6] the generated key here might not be sufficiently randomized. Besides, a radiation pattern of the standard antenna is known to the eavesdropper, thus he might be able to gain some side information on the error patterns.

The solution provided in [1] was to equip the access point AP with a directional antenna with variable radiation pattern. From technological point of view, electronically steerable antenna fits best for this purpose. A natural demand for our antenna is to be low-cost and easy-to-implement given the hardware available at the market. It turns out that electrically steerable passive array radiator (ESPAR) antennas (for details see [12, 18] and the references therein) suit these demands well.

According to [1], their version of ESPAR antenna generates 2^{48} different radiation patterns.

2.2 Error-correcting Codes

Binary linear error-correcting $[n, k, d]$ codes are a well-studied topic, see, e.g. [17]. Let $\mathbf{H}$ denote a parity check matrix of the code $[n, k, d]$.

In our case, we deal with a slightly non-standard scenario where the information transmitted by the sender will not be a codeword but only a *syndrome* $syn(x) = \mathbf{H}^T x$, of some information bits $x \in \{0, 1\}^n$ while their noisy version (denoted by x') is already known to the receiver.

From this syndrome, the decoding algorithm allows for recovering x, given its noisy version $x' = x \oplus e$, where e is an error vector. In details, the sender is to

[5] Counting [5] as the other first one.

[6] Where the reciprocal principle was first used in [8].

announce the syndrome $syn(x)$, so that the receiver can calculate $\mathbf{H}^T x' \oplus \mathbf{H}^T x = \mathbf{H}^T e$ (by linearity) and then, using the decoding algorithm, the coset leader $\hat{e}$. Clearly, $\hat{e} = e$, if the code is capable to correct errors in the noisy channel, so the receiver recovers x as $x' \oplus \hat{e} = x \oplus e \oplus e = x$.

2.3 Cryptographic Notions

Communication Model *Adversarial Behavior.* Two basic types are usually considered: 1) *passive* attacks, i.e., eavesdropping on the parties' communication and trying to compute any information on the key from the intercepted data; and 2) *active* attacks, i.e., when in addition to the previous attack, the adversary is also interfering into the parties' data exchange, for instance, aiming at impersonating himself as legitimate player.

In this work, we consider only the passive case. Protection from active attacks can be also provided [16].

Number of Used Antennas. The use of several antennas may give to the parties more freedom (and possible advantages) in sending/receiving error patterns. At the same time, it can increase the eavesdropper's capabilities in the case of improper management. The eavesdropper's access to several antennas may increase his ability to stage a successful attack. In this paper, we focus on the case where both honest and malicious players have only one antenna.

2.4 Key Agreement: Security Definition

Here is the formal definition of unconditionally secure key agreement [14]. Let X, X' and Z be random variables describing the correlated random variables in possession of the legitimate users AP, UT, and eavesdropper E, respectively, and let C denotes the transcript of AP and UT's communication over public noiseless channel, let N_K be an integer and let $\varepsilon > 0$.

Definition 1. *An unconditional key agreement protocol is* secure*, if it has the following properties: AP and UT accept an outcome of the protocol as their keys K_{AP} and K_{UT}. Furthermore, there exists a perfectly uniform N_K-bit string K such that*

$$\Pr[K_{AP} = K_{UT} = K] \geq 1 - \varepsilon$$

and

$$H(K|ZC) \geq N_K - \varepsilon$$

hold, where $H(\cdot|\cdot)$ is the conditional (Shannon) entropy.

In other words, after the protocol the eavesdropper must be left with no information about the generated key, except with some (typically very small) probability ε.

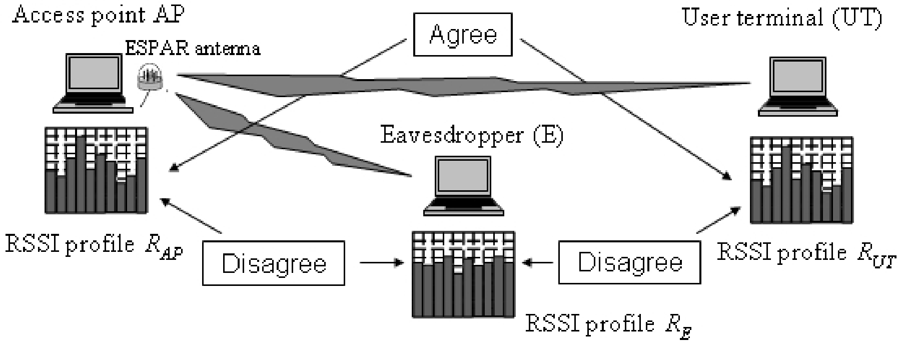

Fig. 1. System configuration.

3 Key Agreement System

In this section, the key agreement protocol (which is a modified version of the protocol from [1, Section IV]) based on ESPAR is presented. We add a probing phase where the error characteristics of the channel is estimated. This allows us to optimize the error-correcting procedure. Besides, in this case, the parties do not need to send a confirmation (like the hash value of the key candidate in [1]). They shall know the expected number of errors prior to the protocol and thus they shall be able to adjust the error correction procedure accordingly.

For completeness, we recap our setting (see Fig. 3): the access point AP exchanges some fixed messages with the user terminal UT and measure their received signal strength indicators (RSSI)[7] denoted R_{AP} and R_{UT}, respectively. These vectors will be highly correlated due to the reciprocal property of the radio communication channel [8]. This means that the message which two players quickly exchange is likely to be corrupted by a highly correlated error pattern. The correlation, however, depends quite strongly on the physical location of the player: the other receiver (i.e., eavesdropper E) even being closely located to either of the two parties will experience only a weekly correlated noise corresponding to E's RSSI R_E. Then, R_{AP} and R_{UT} can be used for computing the common key.

Next, we introduce the *initialization phase* where the channel characteristics are estimated.

3.1 Initialization Phase

This phase consists of two independent parts: a probing of the communication channel and an estimation of the eavesdropper's information.

[7] These are the reactance values at each parasitic element of the ESPAR antenna.

Channel Probing The probing is performed by AP and UT, its goal is to estimate an error rate for the channel. Its basic idea: the players exchange the data, as if they were taking part in the real key agreement; create their key candidates (denoted by Y_{AP} and Y_{UT}, resp.), but, at the same time, save their RSSI vectors R_{AP} and R_{UT}. Then, they announce Y_{AP} and Y_{UT} to each other, compare them against R_{AP} and R_{UT} and estimate the error rate for different RSSI values.

Differentiating the quality of bits in Y_{AP} and Y_{UT} by the corresponding absolute values [8] of R may not be the best option as the domain can be quite big. We use the following encoding: sort the elements of R by their values (in the increasing order) and encode them as their order L. Suppose $|R| = N_p$, then $L \in \{1, \ldots, N_p\}^{N_p}$, where $L(1)$ and $L(N_p)$ are, respectively, the smallest and the largest elements in R (see Fig. 2); they correspond to the most reliable bits in the key candidates Y.

In order to collect the statistics for the channel noise, the parties exchange N_t profiles and compute an estimated error rate for each of N_p levels. Let $err \in \mathbb{N}^{N_p}$ be an error counter used by both AP and UT. They will each keep a separate counter but as their values will be the same, we shall refer to them as err for simplicity. We assume err to be filled with zeroes initially.

A *packet* is a standard block of information used by the wireless network. No matter which technology is actually used, we assume that the packet's information fields contain some fixed publicly known data, say zeroes. In other words, in the noisy exchange AP and UT always send the same information to each other.

Protocol 1 Probing

```
1. For $j = 1$ to $N_t$ do:
   (a) For $i = 1$ to $N_p$ do:
         i. AP sends a packet to UT. UT measures the RSSI value, quantizes
            and saves it as $R_{UT}(i)$.
        ii. Upon receiving, UT sends the packet to AP. AP measures the RSSI
            value, quantizes and saves it as $R_{AP}(i)$.
       iii. AP changes the radiation pattern at random.
       Endfor.
       AP and UT conclude with their RSSI value sets $R_{AP}$ and $R_{UT}$, resp.
   (b) AP and UT both perform the following:
         i. $R$ is sorted in increasing order and is encoded as a set of levels
            $L \in \{1, \ldots, N_p\}^{N_p}$. Then, they encode $L$ into the binary string $Y$
            as follows: $Y(i) = 0$, if $L(i) \leq N_p/2$ and $Y(i) = 1$ otherwise (see
            Fig. 2). AP and UT conclude with $Y_{AP}$ and $Y_{UT}$, respectively.
        ii. AP and UT announce $Y_{AP}$ and $Y_{UT}$ to each other. For $i = 1, \ldots, N_p$,
            AP and UT compute: $err(i) = err(i) + 1$, if $Y_{AP}(i) \neq Y_{UT}(i)$.
   Endfor.
```

[8] Henceforth, when writing R we mean "R_{AP} and R_{UT}" (as above) or "either R_{AP} or R_{UT}" depending on the context. The same applies for Y and other sets defined simultaneously for both AP and UT.

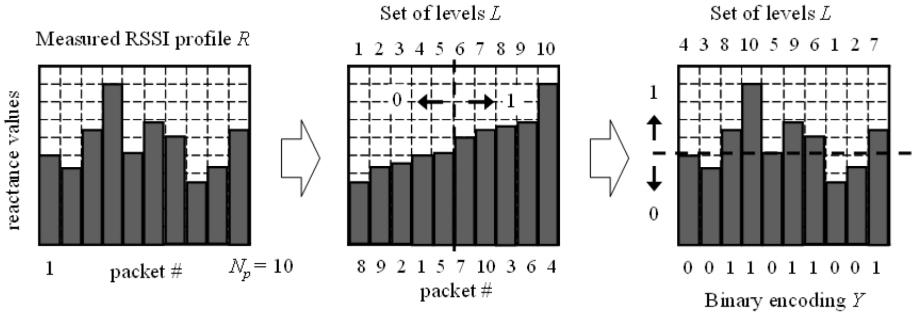

Fig. 2. Quantization of RSSI profiles.

2. AP and UT compute the estimated error rates for each level as follows: For $i = 1, \ldots, N_p$: $p_i = err(i)/N_t$.

Clearly, the estimates p_i are getting closer to the actual rates as N_p and N_t are increasing.

Estimation of Eavesdropper's Information According to Definition 1, the protocol is unconditionally secure, if the eavesdropper E learns only a negligible information on the generated key K. This can only be achieved by using cryptographic techniques (in combination with the aforementioned information transmission techniques) because E can always obtain a non-negligible information on the key candidates by intercepting on the data transmission.

It is well known that the *privacy amplification* [9] [3, 2] can be applied in order to increase E's uncertainty about the resulting key. In order to this to work, one must be sure (or assume) that the adversary did not obtain more then a certain threshold on the parties' correlated randomness (i.e., error patterns).

In this paper, we investigate the probability distribution on the data shared by AP, UT and E in the key agreement protocol Key-Agree from Subsection 3.3. We provide the method for calculating the mutual information on their data and show the possibility of constructing an unconditionally secure key agreement using this protocol. The details on application of privacy amplification technique and protection against active eavesdroppers are out of scope of this paper. It is a matter of our ongoing research.

In a general case, a key agreement protocol would require as a parameter an upper bound on the information about the exchanged data available to E. Hence, it is the task of a security administrator to establish such the upper bound for a particular environment where the protocol is used. An obvious way to do it would be to perform the experiment where the adversary is placed in the most advantageous situation for him: for instance, the best possible location, the best

[9] Also known in theoretical computer science as *left-over hash lemma* [10, 9].

intercepting equipment (which one wants to be protected from), the smallest background noise, etc.

3.2 General Idea

We assume that AP and UT both use the binary linear block code $[n, k, d]$ which can correct up to $t = (d-1)/2$ errors. t will be used as a parameter in the protocol.

The scheme follows these steps of the classical paradigm for unconditionally secure key agreement based on noisy channels:

1. *Data transmission* which aims at creating correlated data with the parties. This part is the same as Step 1 in the Probing protocol. The key candidates are computed from these data as in Step 1(b)i of the same protocol.
2. *Information reconciliation* is needed for correcting errors in the key candidates. It is made in two steps: 1) using the error rate estimates p_i (computed in Probing) all low quality bits are removed such than no more than t (minus some margin) expected errors remain; 2) AP computes the syndrome of $[n, k, d]$-code for the resulting key candidate and sends this syndrome to UT. UT corrects errors in his key candidate, reconciling it with AP's one.
3. *Privacy amplification* is performed in order to reduce E's information on the resulting shared key.

We assume that the length of the key (denoted by $|K|$) is a requirement which is known to both parties in advance. We also assume that AP and UT has performed the protocol Probing prior to their key-exchange, hereby they both possess p_i for $i = 1, \dots, N_p$.

3.3 Protocol

The parameters in this protocol are $|K|$, estimated error probabilities p_i for the levels $i = 1, \dots, N_p$ and the error correction capability t for the $[n, k, d,]$ code.

Protocol 2 Key-Agree

1. Using $|K|$, p_i and t, AP computes an expected number of packets N_c.
2. **For** $i = 1$ to N_c **do:**
   (a) AP sends the packet to UT. UT measures the RSSI value $R_{UT}(i)$.
   (b) Immediately upon receiving, UT sends the packet to AP who measures R_{AP}.
   (c) AP changes the radiation pattern at random.
   Endfor.
   AP and UT each conclude with their RSSI value sets R_{AP} and R_{UT}, resp.
3. Both AP and UT do the following: R is sorted in increasing order and encoded as a set of levels $L \in \{1, \dots, N_c\}^{N_c}$. Then, L is encoded into the binary string Y as follows: $Y(j) = 0$, if $L(j) \leq N_c/2$ and $Y(j) = 1$ otherwise (see Fig. 2). AP and UT conclude with Y_{AP} and Y_{UT}, respectively.

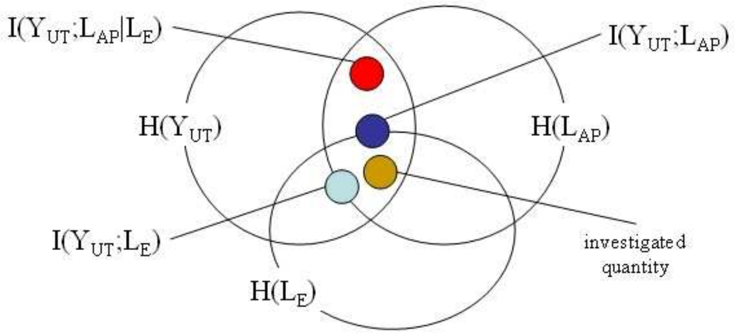

Fig. 3. Entropy relations for L_{AP}, Y_{UT} and L_E.

4. AP and UT decrease the discrepancy between Y_{AP} and Y_{UT} such that the expected Hamming distance between them becomes less than t: AP announce to UT positions of the most noisy bits in Y_{AP}, they both remove them, then UT does the same such that the above condition is satisfied from both AP's and UT's points of view.
5. AP computes the syndrome $syn(Y_{AP})$ using the check parity matrix of $[n, k, d]$ and sends it to UT, who uses the syndrome and the decoding algorithm of the code in order to reconcile Y_{UT} and Y_{AP}. Finally, AP and UT accept Y_{AP} and corrected version of Y_{UT}, resp. as their common key K.

4 Security Analysis

Fig. 3 depicts the entropies and their relation for L_{AP}, Y_{UT} and L_E. The intersection between $H(L_{AP})$ and $H(Y_{UT})$ depicts the amount of information on Y_{UT} one can obtain after learning L_{AP}. It is, in fact, $I(Y_{UT}; L_{AP})$, the mutual information between Y_{UT} and L_{AP}.

It is used for upper bounding the information transmission rate, i.e., the number of error-free bits UT and AP can share after applying ideal error correction divided by the number of packets they exchanged.

Even if the error-free bits can be obtained with ideal error correction, they cannot be used instantly since the eavesdropper may get some information on them. The latter information is given by the intersection between $H(L_E)$ and $I(Y_{UT}; L_{AP})$, it is marked as "investigated quantity" in Fig. 3. For the sake of simplicity, we upper bound this quantity with $I(Y_{UT}; L_E)$ since $I(Y_{UT}; L_E)$ can be calculated easily using the error probabilities p_i obtained in the Probing protocol. Such the upper bound follows obviously from the fact that the intersection is covered by $I(Y_{UT}; L_E)$ in Fig. 3.

Hence, $I(Y_{UT}; L_{AP}|L_E)$ – the amount of information which AP and UT can share with unconditional security (based on L_{AP}) – is lower-bounded by

$$I(Y_{UT}; L_{AP}|L_E) \geq I(Y_{UT}; L_{AP}) - I(Y_{UT}; L_E). \tag{1}$$

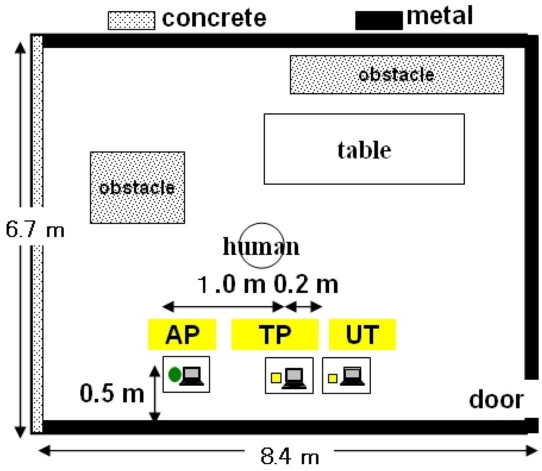

Fig. 4. Experimental environment.

In a similar way, $I(Y_{AP}; L_{UT}|L_E)$ – the amount of information AP and UT can share securely (based on L_{UT}) – is lower-bounded by

$$I(Y_{AP}; L_{UT}|L_E) \geq I(Y_{UT}; L_{AP}) - I(Y_{AP}; L_E). \quad (2)$$

5 Experimental Results

The following experimental results show a high potential of this protocol for obtaining unconditionally secure key agreement. Using these results, we compute the information quantities presented in the previous section. In particular, we precisely compute an upper bound on the average rate, at which AP and UT can exchange secret keys using the protocol from Section 3.3. The experimental data are kindly provided by the Wave Engineering Laboratory, Advanced Telecommunication Research Institute International (ATR), Japan. The environment (corresponding to a standard office) in which the data was collected is shown in Fig 4.

The measurements and computations were performed as described in the protocol Probing. The RSSI profiles R_{AP}, R_{UT} were measured and then the levels $L = \{1, \cdots N_p\}^{N_p}$ and the key candidates $Y = \{0,1\}^{N_p}$ were computed. The same values for E were computed analogously as if E was a user in the protocol Probing sending no packets but just intercepting. The parameters were chosen as follows: $N_p = 384$ and $N_t = 500$.

After the computations described in Step 2 of the protocol Probing, we obtained the following error rates: the error rate p_x between Y_{AP} of the level x at AP and Y_{UT} of the corresponding packet at UT; and the analogous values for Y_{UT} and Y_{AP}; Y_E and Y_{UT}; Y_E and Y_{AP}.

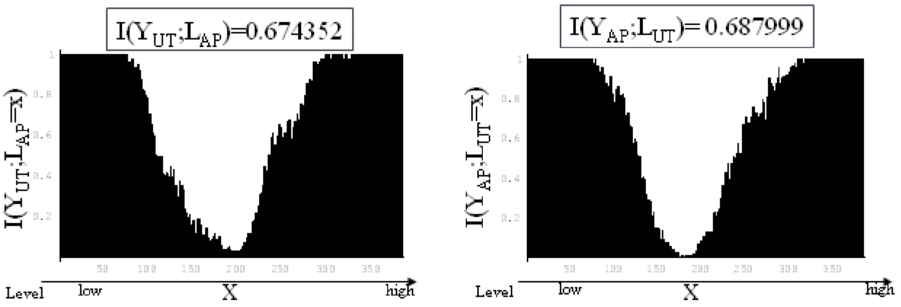

Fig. 5. Mutual information between data of AP and UT.

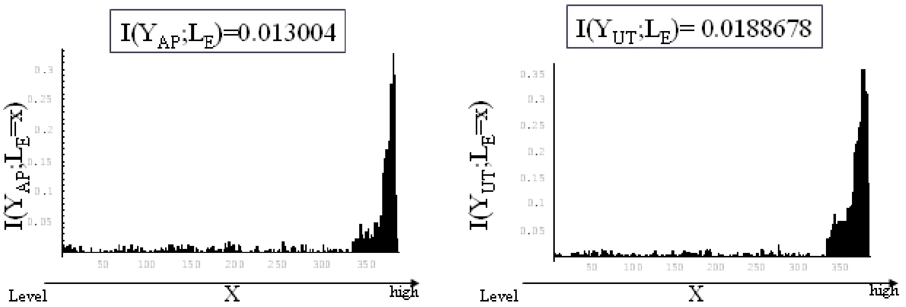

Fig. 6. Mutual information between data of AP, UT and E.

These rates are used to estimate $I(Y_{UT}; L_{AP} = x)$, $I(Y_{AP}; L_{UT} = x)$, $I(Y_{UT}; L_E = x)$ and $I(Y_{AP}; L_E = x)$, respectively using the following equation:

$$I(Y; L = x) = 1 + p_x \log_2 p_x + (1 - p_x) \log_2(1 - p_x). \qquad (3)$$

In other words, for the sake of simplicity, we assume that the error rate is the same for the same level and, in addition that the “channels” defined by each level x are binary symmetric.

Then, we compute:

$$I(Y; L) = \frac{1}{N_p} \sum_{x=1}^{N_p} I(Y; L = x). \qquad (4)$$

In Fig. 5 and 6, we provide the graphs for $I(Y|L = x)$ depending on the level x computed according to (3), and the corresponding value of $I(Y; L)$ computed using (4) is given above each graph. Considering Fig. 5, we note that due to the nature of our encoding into level sets L, the middle levels turn out to be the most noisy. Fig 6 allows us to conclude that in this particular example, the highest levels of L (and so, the largest values of RSSI profiles R) provide the adversary with most of information on Y_{AP} an Y_{UT}. We note that different levels appear to leak different information to the eavesdropper. This raises an interesting open question: whether excluding the more "leaking" levels (in a proper way) in Step 4 of Protocol Key-Agree can increase security and efficiency? What values are more "leaking" should be defined by experimental checking on adversary's capabilities. A related question is finding a better encoding for RSSI profiles.

Using (1) and (2), we compute:

$$I(Y_{UT}; L_{AP}|L_E) \geq 0.674 - 0.019 = 0.655, \text{ and} \tag{5}$$

$$I(Y_{AP}; L_{UT}|L_E) \geq 0.688 - 0.013 = 0.675. \tag{6}$$

The above estimates show that $I(Y_{UT}; L_{AP}|L_E)$ and $I(Y_{AP}; L_{UT}|L_E)$ are substantially large such the protocol Key-Agree may in principle be efficient and practical. However, it is not secure so far, because the parties must make sure that E is left with only a negligible information on the common key.

Let us estimate the impact of privacy amplification. Suppose that AP and UT obtain the key by hashing their resulting Y's using 2-universal hash function [6]. After completion of the protocol, they publicly agree on using the function $g(\cdot)$ which is chosen uniformly at random from a family of 2-universal functions $G : \{0,1\}^{N_p} \rightarrow \{0,1\}^r$.

According to the privacy amplification theorem [2, Corollary 4], from E's point of view, the uncertainty of the key K given his measurement ${L_E}^t$ and the function in G is the following:

$$H(K|G, L_E^t) \geq r - \frac{2^{r-cN_p}}{\ln 2}, \text{ where} \tag{7}$$

$$c \geq H_2(Y_{UT}|L_E) - H_2(Y_{UT}|L_{AP}). \tag{8}$$

is the Rényi information which is contained in L_E^t. The Rényi information is defined as a counterpart of the Rényi entropy [19]: $H_2(X) = -\log \sum_{x \in \mathcal{X}} P_X(x)^2$. For the binary variable X distributed according to the Bernoulli distribution with probability p, we have: $H_2(X) = -\log\left(p^2 + (1-p)^2\right)$. Equation (8) easily follows by: 1) observing that Equations (1) and (2) hold for the Rényi information as well and 2) assuming that error patterns are uniformly distributed from E's point of view as long as he does not learn L_E^t.

Using (7), (8) and the previously computed error probabilities, we obtain $I_R(Y_{UT}; L_{AP}|L_E) \geq 0.967 - 0.259 = 0.708$. And then $I_R(Y_{AP}; L_{UT}|L_E) \geq 0.977 - 0.250 = 0.727$ can be computed in the same way. It may seem surprising that the above estimates are better than those of (5) and (6). The reason is that they contain tighter upper bounds than the former ones.

We conclude that by taking r smaller than $0.7N_p$, the right part of (7) can be made negligible. This means that the protocol Key-Agree indeed has a high potential for achieving unconditionally secure key agreement at the same time being both efficient and practical.

6 Concluding Remarks

We presented the practical scheme elaborating on [1] which is shown to provide unconditional security for wireless networks users under a number of reasonable assumptions. The most important one is that the eavesdropper does not obtain more information on the data exchanged by the parties than a certain threshold. The main problem of a network security administrator is to set up such threshold properly. The analysis of our experimental results have shown that for the considered system, one can ensure that the legitimate parties can share a key which is secure in the information-theoretical sense.

Our recommendation is to use this system in a protected environment such as offices with restricted access. This would make sure that the adversary does not near himself to the players' antennas or install an intercepting receiver (a "bug"). This would also simplify the security analysis (and make the scheme more efficient), as the eavesdropper could only intercept from outside the office.

The following two issues on optimizing the system are to be highlighted: First of all, note that the encoding RSSI profiles into the level sets used in the protocol Probing provide us with a very rough estimate. This is because the actual error rate might be quite different for the same level in different RSSI profiles. Therefore, it is important to provide a better technique for the error rate estimation. For the second: Note that E must not be able to obtain a side information on the error pattern themselves. As an example, suppose that the environment is a merely cube (made of some material with known electromagnetic properties) containing only AP, UT and E inside. Then, E may perform a simulation for radio wave propagation and succeed in guessing the error pattern with AP and UT. Clearly, the real environment has a complex shape and properties, besides the radiation patterns are chosen at random and their number is quite big (2^{48}) that excludes a successful a priori guessing. Nevertheless, for the real key agreement system, one must provide: 1) the argument that the error patterns are sufficiently random; 2) a true random generator for the directional antenna.

Some channels do not allow for unconditionally secure key agreement [15]. In our case, this will happen if the adversary obtains too much information on the players' error patterns.

Methods for protection against active attacks were investigated in [16].

In the light of the above discussion, the ultimate goal of our current research is to build a fully functional and secure hard/software prototype of this key agreement system for radio communication network. The following particular open questions are interesting at the current stage:

- Providing a more adequate estimation on the channel noise characteristics.
- Providing protection against active attacks.
- Improving the error-correction stage using specifically designed codes, for instance the LDPC codes of [5].
- Improving the privacy amplification stage. An ideal solution would be to combine error-correction and privacy amplification, for instance, using the extractors proposed in [7].

References

1. T. Aono, K. Higuchi, T. Ohira, B.Komiyama, H. Sasaoka, Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels. IEEE Trans. on Antennas and Propagation, vol. 53, no. 11, pp. 3776–3784, 2005.
2. C. H. Bennett, G. Brassard, C. Crépeau, U. Maurer, "Generalized Privacy Amplification", IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, 1995.
3. C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion", SIAM J. on Computing, no. 17(2), pp. 210–229, 1988.
4. J. Barros, M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," Proc. ISIT '06, pp. 356–360, 2006.
5. M. Bloch, A. Thangaraj, S.W. McLaughlin, J.-M. Merolla, "LDPC-based secret key agreement over the Gaussian wiretap channel," Proc. ISIT '06, pp. 1179–1183, 2006.
6. J.L. Carter, M.N. Wegman, "Universal Classes of hash functions. J. of Comp. and System Sciences", vol. 18., Elsevier, pp. 143–154, 1979.
7. Y. Dodis, J. Katz, L. Reyzin, and A. Smith, "Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets," Accepted to *CRYPTO '06*.
8. J.E. Hershey, A.A. Hassan, R. Yarlagadda, "Unconventional Cryptographic Keying Variable Management", IEEE. Trans. Commun., vol. 43, no. 1, pp. 3–6, Jan 1995.
9. J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby, "A Pseudorandom Generator from any one-way function, SIAM J. on Comp., vol. 28, no. 4., pp. 1364–1396, 1999.
10. R. Impagliazzo, L. Levin and M. Luby, "Pseudo-random Generation from One-Way Functions," *Proc. 21st ACM STOC*, pp. 12–24, 1989.
11. H. Imai, M.G. Rahman, K. Kobara, "Wireless Communications Security," Artech House, 2005.
12. H. Kawakami, T. Ohira, "Electrically Steerable Passive Array Radiator (ESPAR) Antennas," *IEEE Antennas and Propagation Magazine*, vol. 47, no. 2, April 2005.
13. U. Maurer, "Secret Key Agreement by Public Discussion IEEE Transaction on Information Theory", vol. 39, no. 3, pp. 733–742, 1993.
14. U. Maurer, S. Wolf, "Secret-key agreement over unauthenticated public channels – Part I: Definitions and a completeness result", IEEE Trans. Inf. Theory, vol. 49, no. 4, pp. 822-831, 2003.
15. U. Maurer, S. Wolf, "Secret-key agreement over unauthenticated public channels – Part II: The Simulatability ", IEEE Trans. Inf. Theory, vol. 49, no. 4, pp. 832-838, 2003.
16. U. Maurer, S. Wolf, "Secret-key agreement over unauthenticated public channels – Part III: Privacy Amplification", IEEE Trans. Inf. Theory, vol. 49, no. 4, pp. 839-851, 2003.
17. F.J. MacWilliams, N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, 1977.
18. T. Ohira and J. Cheng, "Analog smart antennas," *Adaptive Antenna Arrays*, pp. 184–204, 2004.
19. A. Rényi, "Probability theory," *North-Holland, Amsterdam*, 1970.
20. A. D. Wyner, "The Wiretap Channel," Bell Syst. Tech. J. vol. 54, no. 8, pp. 1355–1387, 1975.