Differential Secret Sharing in Wireless Networks

Lei Miao
Dept. of Electrical and Computer Engineering Technology
Farmingdale State College, Farmingdale, NY 11735
lei.miao@farmingdale.edu

***Abstract*—This paper utilizes the principle of reciprocity in electromagnetic wave propagation as well as the variations of the wireless channel state to share secrets in wireless networks. In particular, a novel secret sharing mechanism is proposed to share secret bits between two wireless users. Using the Central Limit Theorem, we show that the proposed approach can provide performance guarantee when only limited stochastic information is available. A few properties of the proposed approach are identified to optimize the secret sharing process. Simulation results indicate that compared with [3], the proposed mechanism can share secret bits 3-4 times faster with higher probability of success.**

Keywords: secret sharing, wireless communications, principle of reciprocity

I. Introduction

There is an intriguing information security problem in wireless communications: suppose that Alice and Bob are two legitimate wireless users, and Eve is an eavesdropper; how can we guarantee that the confidential information exchanged between Alice and Bob is protected against Eve who can also receive all the transmitted packets? The most common way of achieving security is cryptography. Most wireless networks have adopted symmetric-key cryptography. Symmetric-key cryptography encrypts and decrypts messages using a single shared private key which must be securely exchanged initially. Therefore, secret sharing is crucial to the information security of wireless communications, especially in Machine to Machine (M2M) networks where human intervention is either minimal or does not exist at all.

This paper proposes a novel secret sharing policy between Alice and Bob, utilizing the differential information of their common observations on the wireless channel state. The organization of the paper is as follows: in Section II, we discuss the related work of secret sharing and formulate the problem; in Section III, we introduce our main result; finally, we conclude in Section IV.

II. Related Work and Problem Formulation

Electromagnetic wave propagation has a property known as the principle of reciprocity [1]: if two antennas radiate identical signals at about the same time, the excitation of each antenna by the signal originated from the other antenna will generate almost identical outputs. Utilizing this property, some work focused on extracting information from Alice and Bob's common observations on the wireless channel state [2] [3] [4]. In particular, Alice and Bob send *probes* to each other at a regular rate. The channel state is then obtained from these probes, and secrets are shared based on the similarity of the channel state information. Whether a secret bit can be successfully shared is probabilistic. We use probability of error to denote the probability that a secret bit is shared unsuccessfully. In [3], a secret bit is shared between Alice and Bob only after a number of consecutive channel estimates are all above or below pre-established thresholds. This approach has two obvious drawbacks: *i)* consecutive probes that are above or below the reference levels may not always exist and *ii)* unused probes are essentially wasted. In addition, the approach in [3] does not specify how a specific error probability can be guaranteed. Furthermore, the error probability in [3] can only be derived when the wireless channel characteristics are fully known.

Conventional physical layer security solutions often bypass secret keys by designing smart transmit coding strategies. What is different in this paper is that we exploit physical layer properties, i.e., wireless channel state, to extract secret keys over a public channel.

We assume that the channel state information between Alice and Bob is estimated by short probes: waveforms known to both Alice and Bob. Specifically, Alice initiates the probes at a constant rate, and Bob sends a probe to Alice τ seconds after receiving each probe from her. During the transmission, the probes are distorted by the wireless channel and are also affected by noises. Upon the reception of each probe, Alice and Bob can then estimate the instantaneous channel state. It is widely accepted that the time-variant channel response of the wireless channel can be modeled as a complex Gaussian random process. In this paper, we consider the magnitude response at a fixed frequency f_0 as the channel state function $h(t)$. Let $h_a(i)$ and $h_b(i)$ be the channel estimates of the *i-th* probe received by Alice and Bob respectively. Because of the principle of reciprocity, $h_a(i)$ and $h_b(i)$ are highly correlated when τ is sufficiently small. This is the basis of how we can extract common information from the channel estimates.

In this paper, we will focus on the procedure of sharing one bit of secret between Alice and Bob. Specifically, Alice will accumulate a sequence of channel estimates and send some probe information to Bob. Bob will then extract the secret bit from the probe information. Alice will restart the same process to share the next secret bit. Our questions are: *what probe information shall Alice send to Bob and how does Bob decode the secret bit from the probe information?* Essentially, we need to come up with a good secret sharing policy that fully utilizes the probe information and also incurs low probability of error.

We use E_i to denote the difference between $h_a(i)$ and $h_b(i)$, i.e.,

$$E_i = h_a(i) - h_b(i)$$

We have the following assumption:

Assumption 1: E_i, $i = 1, 2, 3, \ldots$ are i.i.d. random variables, and each random variable has mean μ and variance σ^2.

Note that the above assumption does not rely on the probability distribution function of random variable E_i; instead, only the mean and variance of E_i are assumed to be known. They can be obtained via statistical methods.

III. Differential Secret Sharing

In this section, we propose a novel Differential Secret Sharing (DSS) mechanism that addresses the issues in [3]. We denote:

$2N$: the number of channel estimates *exchanged* between Alice and Bob before sharing each secret bit.

$2n$: the number of channel estimates actually *used by* Alice and Bob to share each secret bit.

We first present the basic idea of the secret sharing mechanism:

Step 1: Alice decides the secret bit (0 or 1) from the 2N (N is a control variable) number of channel estimates and then picks n *(n is another control variable) largest channel estimates and* n *smallest channel estimates from the* $2N$ *estimates,* $1 \le n \le N$.

Step 2: Alice sends a sequence S of the $2n$ *indices to Bob such that*

$$\begin{aligned} h_a(S(1)) &\le h_a(S(2)) \le \cdots \le h_a(S(2n)), \\ &\quad \text{if 1 is picked in } \textit{Step 1}; \\ h_a(S(1)) &\ge h_a(S(2)) \ge \cdots \ge h_a(S(2n)), \\ &\quad \text{if 0 is picked in } \textit{Step 1}. \end{aligned} \tag{1}$$

where $S(i)$ is the *ith* index in S, $i = 1, \ldots, 2n$.

Step 3: Bob decodes the secret bit using (2) below.

$$Q(S,n) = \begin{cases} 1, & \text{if } \sum_{i=1}^{n} h_b(S(i)) < \sum_{i=n+1}^{2n} h_b(S(i)) \\ 0, & \text{if } \sum_{i=1}^{n} h_b(S(i)) > \sum_{i=n+1}^{2n} h_b(S(i)) \end{cases} \tag{2}$$

Note that in Step 1, Alice may use very simple rules to determine the random secret bit. For example: choose bit 1 if $h_a(1) < h_a(2N)$, and bit 0 otherwise.

Notice that $Q(S,n)$ may not always be the same secret bit generated by Alice. When this happens, Bob encounters a decoding error. As we will show next, the error probability depends on n and some other factors. We use $P_e(n)$ to denote the error probability of decoding at Bob when $2n$ probes are used to share the secret bit. When the pdf of E_i is known, we may derive the exact form of $P_e(n)$, using which we can then find the best n that minimizes the error probability. In general, not all $2N$ channel estimates are always needed to share the secret bit. In this paper, we are more interested in providing a guaranteed maximum error probability when the pdf of E_i is unknown. This is the focus of the rest of the section. Before we derive the error probability, we first introduce another assumption and show that Eve cannot precisely figure out the information bit from the above procedure.

Assumption 2: Eve is more than $\lambda/2$ (λ is the wavelength of the wireless signal) away from Alice and Bob.

It has been shown in [5] that under Assumption 2, the probe signals received by Eve are uncorrelated with $h(t)$. Although Eve can overhear the probe signals sent by Alice and Bob, the signals received by her are completely different. Therefore, Eve cannot decode the information bit using sequence S, even if the DSS mechanism is known to her.

We now derive the error probability of the DSS mechanism.

Lemma 3.1: For sufficiently large integers N and n, $1 \ll n \le N$,

$$P_e(n) \approx \frac{1}{2}[1 - \mathrm{erf}(\frac{D_n}{\sqrt{4n}\sigma})] \tag{3}$$

where

$$D_n = |\sum_{i=1}^{n} h_a(S(i)) - \sum_{i=n+1}^{2n} h_a(S(i))| \tag{4}$$

Proof: The probability of error is

$$P_e(n) = P\{B = 1|A = 0\}P\{A = 0\}$$
$$+P\{B = 0|A = 1\}P\{A = 1\}$$

where $\{A = 0\}$, $\{A = 1\}, \{B = 0\}$, and $\{B = 1\}$ are the events "Alice generates 0", "Alice generates 1", "Bob calculates 0", and "Bob calculates 1", respectively. Assuming that Alice generates "1" or "0" with equal probability, and due to the symmetric property of the policy,

$$P_e(n) = P\{B = 1|A = 0\} = P\{B = 0|A = 1\}$$

Without loss of generality, let us calculate $P\{B = 1|A = 0\}$. First,

$$\begin{aligned} &\sum_{i=1}^{n} h_b(S(i)) - \sum_{i=n+1}^{2n} h_b(S(i)) \\ = &\sum_{i=1}^{n}[h_a(S(i)) - E_i] - \sum_{i=n+1}^{2n}[h_a(S(i)) - E_i] \\ = &\sum_{i=1}^{n} h_a(S(i)) - \sum_{i=n+1}^{2n} h_a(S(i)) + E \end{aligned} \tag{5}$$

where $E = -\sum_{i=1}^{n} E_i + \sum_{i=n+1}^{2n} E_i$. Because n is sufficiently large, we invoke the Central Limit Theorem and get

$$\sum_{i=1}^{n} E_i \xrightarrow{d} N(n\mu, n\sigma^2) \text{ and } \sum_{i=n+1}^{2n} E_i \xrightarrow{d} N(n\mu, n\sigma^2).$$

Therefore,

$$E \xrightarrow{d} N(0, 2n\sigma^2) \tag{6}$$

Since Alice generates "0", from (1), we have

$$\sum_{i=1}^{n} h_a(S(i)) - \sum_{i=n+1}^{2n} h_a(S(i)) \ge 0 \tag{7}$$

Because Bob decodes the message, and gets "1", we have

$$\sum_{i=1}^{n} h_b(S(i)) - \sum_{i=n+1}^{2n} h_b(S(i)) < 0 \qquad (8)$$

Combining (5), (7), and (8), we have

$$P_e(n) \approx P\{E < -|\sum_{i=1}^{n} h_a(S(i)) - \sum_{i=n+1}^{2n} h_a(S(i))|\}$$
$$= \frac{1}{2}[1 - \mathrm{erf}(\frac{D_n}{\sqrt{4n}\sigma})] \quad \blacksquare$$

Lemma 3.1 shows that when n is sufficiently large, the error probability can be calculated by Alice, using her channel estimates, n, and the variance of random variable E_i. This property is attractive because it does not require the exact distribution of E_i and $h_a(i)$.

In order to take advantage of this nice property, we modify the secret sharing mechanism so that it can now guarantee that the error probability is below a given threshold P_e:

Step 1: Alice and Bob keep sending each other channel probes until Alice has 2N (N is a control variable) channel estimates and there exists integer n^* that satisfies:

$$n^* = \arg\max_{n\in\{\overline{n},\ldots,N\}} (\frac{D_n}{\sqrt{n}}) \text{ and} \qquad (9)$$

$$\frac{D_{n^*}}{\sqrt{n^*}} \geq 2\sigma\,\mathrm{erf}^{-1}(1-2P_e)), \qquad (10)$$

where $\overline{n}$ is a sufficiently large positive integer

Steps 2 and 3: the same as *Steps 2 and 3* above, except that we now use n^*.

Note that $\overline{n}$ is a sufficiently large known positive integer. We would like n to be always greater than $\overline{n}$ so that (3) applies to all $n \in \{\overline{n},\ldots,N\}$, including n^*. It implies that in order to achieve guaranteed error probability, at least $2\overline{n}$ channel estimates are used to share the secret bit and $N \geq \overline{n}$. Notice that the above secret sharing mechanism does not specify how many initial channel probes ($2N$) have to exchanged; it is up to the specific implementation to determine it. For example, Alice may initially exchange $2N = 2(\overline{n} + C)$ (C is a constant positive integer) channel probes with Bob and then check if there exists n^* that satisfies both (9) and (10). If yes, Alice will proceed to Steps 2 and 3 above; otherwise, she will accumulate more channel probes and try to find n^* again.

Next, we will show three properties of the above secret sharing mechanism:

i) the lowest error probability can be obtained when (9) and (10) are satisfied and it is less than P_e

ii) in order to find n^*, we do not have to check all $n \in \{\overline{n},\ldots,N\}$.

iii) any arbitrarily low P_e can be satisfied by increasing $2N$, the amount of channel probes Alice and Bob exchange.

We now work on Property $i)$. n^* is the value in $\{\overline{n},\ldots,N\}$ that minimizes (3). One way of finding n^* is to compare $P_e(n)$ for all $n \in \{\overline{n},\ldots,N\}$. Nonetheless, the lemma below shows that n^* can be easily found without the need of dealing with the error function at all.

Lemma 3.2: $n^* = \arg\max_{n\in\{\overline{n},\ldots,N\}} (\frac{D_n}{\sqrt{n}})$.

Proof: Because

$$\frac{D_{n^*}}{\sqrt{n^*}} \geq \frac{D_n}{\sqrt{n}}, n = \overline{n},\ldots,N$$

we have

$$\frac{D_{n^*}}{\sqrt{4n^*}\sigma} \geq \frac{D_n}{\sqrt{4n}\sigma}, n = \overline{n},\ldots,N$$

Since erf(x) is a strictly increasing function, we obtain

$$\mathrm{erf}(\frac{D_{n^*}}{\sqrt{4n^*}\sigma}) \geq \mathrm{erf}(\frac{D_n}{\sqrt{4n}\sigma}), n = \overline{n},\ldots,N$$

Invoking (3),

$$P_e(n^*) = \frac{1}{2}[1 - \mathrm{erf}(\frac{D_{n^*}}{\sqrt{4n^*}\sigma})]$$
$$\leq \frac{1}{2}[1 - \mathrm{erf}(\frac{D_n}{\sqrt{4n}\sigma})] = P_e(n),\ n = \overline{n},\ldots,N \quad \blacksquare$$

Lemma 3.2 uses the monotonicity property of the erf function to show that the optimal number of probes that minimizes the error probability can be easily found by comparing the values of $\frac{D_n}{\sqrt{n}}$, for each $n \in \{\overline{n},\ldots,N\}$. The smallest n that provides the largest $\frac{D_n}{\sqrt{n}}$ is the optimal number. This result is important because it asserts that determining the set of channel estimates for minimum error probability requires neither complicated calculations nor any stochastic information. It also confirms that using all $2N$ number of channel estimates may not minimize the error probability. Using n^* in (3) and letting $P_e(n^*) \leq P_e$, we obtain (10). This completes the discussion of Property *i)*.

We now discuss Property *ii)*. As we can see from the above, finding n^* may still require lots of comparisons. The lemma below shows that in some scenarios, the number of comparisons could be less.

Lemma 3.3: $n^* \leq k$, $k \in \{\overline{n},\ldots,N-1\}$, if

$$\frac{D_{k+1}}{D_k} \leq 1 + \frac{1}{\sqrt{Nk}+k}$$

Proof: Invoking Lemma 3.2, we need to show that

$$\frac{D_k}{\sqrt{k}} \geq \frac{D_n}{\sqrt{n}},\ \text{for } n = k+1,\ldots,N.$$

Because

$$\frac{D_{k+1}}{D_k} \leq 1 + \frac{1}{\sqrt{Nk}+k},$$

we have

$$D_{k+1} - D_k \leq D_k \frac{1}{\sqrt{Nk}+k}. \qquad (11)$$

By definition of D_n in (4), we obtain

$$D_{n+2} - D_{n+1} \leq D_{n+1} - D_n, \forall n \in \{\overline{n},\ldots,N-2\} \qquad (12)$$

Combining (11) and (12), we have

$$\begin{aligned} D_n - D_k &\leq (n-k)(D_{k+1} - D_k) \\ &= D_k \frac{n-k}{\sqrt{Nk}+k},\ n = k+1,\ldots,N \end{aligned}$$

i.e.,

$$\frac{D_n}{D_k} \le 1 + \frac{n-k}{\sqrt{Nk}+k} \le 1 + \frac{n-k}{\sqrt{nk}+k} = \frac{\sqrt{n}}{\sqrt{k}} \;\blacksquare$$

Lemma 3.3 shows that when the difference between D_k and D_{k+1} is small enough, we do not have to take $n = k+1, \dots, N$ into consideration. In this case, we only need to consider $\{\overline{n}, \dots, k\}$ for n^*.

We now discuss Property *iii)*. The next result shows that arbitrarily low P_e can be satisfied when Alice and Bob exchange a large number of probes.

Lemma 3.4: When $N \to \infty$, $P_e(n^*) \to 0$.

Proof: Assume there are two thresholds h^+ and h^- that lie within the possible range of channel states, and $h^+ \;> h^-$. Let

$$c = h^+ \; - h^- \; .$$

When $2N$, the number of probes Alice and Bob accumulate goes to infinity, $2n^{'}$, the number of probes that are above h^+ and below h^- also goes to infinity. Then, we have

$$\begin{aligned}\lim_{N\to\infty} P_e(n^*) &= \lim_{N\to\infty} \frac{1}{2}[1-\mathrm{erf}(\frac{D_{n^*}}{\sqrt{4n^*}\sigma})] \\ &\le \lim_{N\to\infty} P_e(n^{'}) = \lim_{n^{'}\to\infty} \frac{1}{2}[1-\mathrm{erf}(\frac{n^{'}c}{\sqrt{4n^{'}}\sigma})] \\ &= \frac{1}{2}[1-\mathrm{erf}(\infty)] = 0 \;\blacksquare\end{aligned}$$

In practice, we are interested in knowing how quickly a secret bit can be successfully shared between Alice and Bob. In our proposed secret sharing mechanism, we let $N \ge \overline{n}$ in order to use the Central Limit Theorem to derive the error probability without relying on the exact distribution of E_i. Nonetheless, it is important to note that when the exact distribution of E_i is known, the requirement of $N \ge \overline{n}$ may be relaxed. For example, when E_i is zero-mean Gaussian with variance σ^2, (6) and (3) are true even for small n.

In Fig. 1, we show the typical number of probes needed for various error probability requirements in correlated Rayleigh fading channels, under the assumption that E_i is Gaussian. Rayleigh fading process is simulated using the autoregressive method studied in [6]. In particular, the autoregressive model order is set to 100, the maximum doppler frequency is set to 400Hz, the symbol rate is set to 3k baud, and a bias of 10^{-8} is used to condition the Yule–Walker equations. The number of probes needed for each error probability in Fig. 1 is the average value of 1000 secret bit sharing procedures. Notice that the maximum number of probes required in Fig. 1 is only 47. Since the probing rate typically is at least a few kilo Hz [3], our simulation results essentially show that the differential secret sharing approach proposed in this paper can significantly reduce the error probability while keeping a fast secret generation rate.

In Table 1, we show the simulations results of DSS, compared with the approach in [3]. Specifically, we run simulation to share 1 million bits in the above Rayleigh fading channel. When implementing the approach in [3], we let system parameters $q_{\pm}$ = mean of channel state $\pm\, 0.8\sigma$, and we chose m to be 5 and 7. When implementing DSS, the error probability was set to below 10^{-7}. The results show that DSS is able to achieve zero percent of error while the approach in [3] cannot. Compared with the $m = 7$ case, DSS also requires much less number of average probes per bit, indicating that DSS can share secrets at a rate 3-4 times faster.

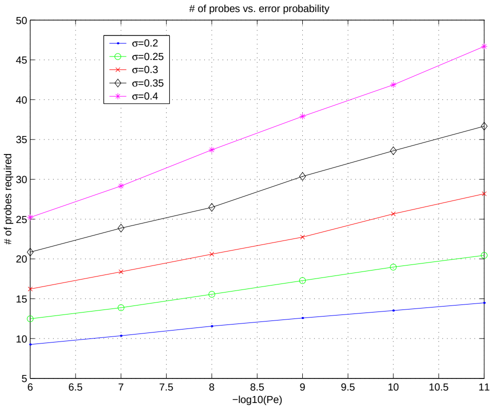

Fig. 1. Number of probes needed for various error probabilities

	$m=5$	$m=7$	DSS
% of error, $\sigma = 0.3$	0.053	0.0022	0
% of error, $\sigma = 0.4$	0.171	0.0134	0
avg. probes / bit, $\sigma = 0.3$	25.87	71.73	18.30
avg. probes / bit, $\sigma = 0.4$	34.03	107.49	29.58

Table 1: Performance comparison between [3] and DSS (1 million bits)

IV. Conclusions

In this paper, we propose a novel secret sharing mechanism that utilizes two wireless users' common observations on the wireless channel state. The differential information of the channel estimates fully utilizes the channel probes and provides us a way to accurately calculate the error probability. Simulation results show that compared with the approach in [3], DSS shares secrets faster and more reliably. The nice properties of DSS make it suitable for M2M applications, especially in the scenarios that extremely low error probability is required in order to share secrets among multiple devices.

References

[1] C. A. Balanis, *Antenna Theory: Analysis and Design*, 2nd ed. New York: John Wiley and Sons, 1997.

[2] R. Wilson, D. Tse, and R. A. Scholtz, “Channel identification: Secret sharing using reciprocity in ultrawideband channels,” *IEEE Trans. on Information Forensics and Security*, vol. 2, pp. 364–375, 2007.

[3] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: extracting a secret key from an unauthenticated wireless channel,” in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, San Francisco, CA, USA, 2008.

[4] B. A.-S. A. Kiayias, A. Mercado, and B. Yener, “Robust key generation from signal envelopes in wireless networks,” in *Proceedings of the 14th ACM conference on Computer and communications security*, Alexandria, Virginia, USA, 2007.

[5] W. . C. Jakes, *Microwave Mobile Communications*. Wiley, 1974.

[6] K. E. Baddour and N. C. Beaulieu, “Autoregressive modeling for fading channel simulation,” *IEEE Trans. on Wireless Communications*, vol. 4, pp. 1650–1662, 2005.