Attack and Countermeasure on Interlock-based Device Pairing Schemes

Yongdong Wu, Binbin Chen, Zhigang Zhao and Yao Cheng

***Abstract*—In recent years, researchers have proposed several secure device pairing schemes that allow mobile devices in close proximity to establish a trusted communication channel between them without sharing any secret in advance. These schemes use the correlation of some physical measurements (magnetic field, acceleration, etc.) made independently by the two pairing devices to reconcile them. Their security against a Man-in-the-Middle (MitM) attacker relies on the difficulty for the MitM attacker to obtain a measurement data similar to the two pairing devices. As a key step in the reconciliation process, an interlock protocol is used in several recent schemes (e.g., Magpairing and ShaVe) to ensure that the measurement data is not leaked. However, the present paper points out that these schemes apply the interlock protocol improperly, making themselves vulnerable to MitM attacks. The analysis and experimental results show that the proposed MitM attack almost surely succeeds with very low computation overhead. We also propose countermeasures on the presented attack.**

***Index Terms*—Device pairing, interlock protocol, cipher operation mode, one-way function**

I. Introduction

With the advance of information and communication technologies, an increasing number of applications (e.g., mobile social network, mobile payment) are built upon the basis that two wireless devices in close proximity can securely communicate with each other. Some form of device pairing scheme is required to achieve such secure communication. One well-known example is the bluetooth pairing scheme which requires a user to manually input Personal Identification Number (PIN) into the bluetooth devices. However, such a manual approach could be inconvenient to use, especially under the input/output constraints on a mobile device.

In recent years, several novel proximity-based device pairing schemes have been developed. In these schemes, the genuine users are close to each other and the attacker is further away from them. Such a "near" authentication scenario is different from that of a "remote" authentication scenario, which will need to rely on some pre-established trusted information such as password or PIN, or even multi-factor authentication methods [1]. Instead, the security of these "near" authentication schemes depends on the assumption that the similar physical measurements made by the two nearby devices can serve as a source of secret between them. To achieve "near" authentication, the proximity-based device pairing schemes use different trusted auxiliary channels, such as audio-visual signal [2]–[6], correlated human behavior [7]–[9], shared vibration/acceleration [10]–[13], wireless signal strength [14]–[24], and body area network [25]–[27]. For a comprehensive survey, please refer to [28].

Proximity-based device pairing schemes include two main steps: a sampling step for the two devices to collect measurements at some auxiliary channels independently, and a reconciling step for them to reconcile their measurements to establish a shared key. For the sampling step, since the measurements are made by each device's local sensor (e.g., magnetometer, and vibrator) independently, some schemes introduce additional pre-processing logics to prepare the raw data so that the measurements obtained from the two devices can be better correlated. Even with such pre-processing, some measurement discrepancies between the devices inevitably exist, due to the difference in the auxiliary channels, the sensors, the measurement noise, the quantization errors, etc. Hence, the reconciling step needs to be able to let the devices agree on a shared key despite of such discrepancies.

In this paper, we focus on the reconciling step. Unlike the sampling step which varies across different proposed schemes (in regard of the auxiliary channels, the sensors, and the pre-processing techniques), the reconciling step can be a generic one that works for different schemes. There are different ways to design this step. One naïve method is that the devices exchange their measurements in cleartext and calculate the similarity or correlation value directly. Obviously, this straightforward method is vulnerable to Man-in-the-Middle (MitM) attack and hence is unable to generate a secure key between the devices. To enhance its security, some schemes [29], [30] exchange the measurement indexes such as sampling timestamp. The indexes are selected only if the indexed measurements incur low discrepancy among devices' measurements. As a cost of security enhancement over the naïve scheme, the index-sharing scheme may incur pairing errors. To reduce the error rate, some schemes (e.g., [31]–[33]) adopt Error Correcting Code (ECC) to encode the measurements or features extracted from the measurements into codewords and exchange the parity bits of the codewords in cleartext, incurring some information leakage. Afterwards, the recovered

Manuscript received ...; revised ... ; accepted October 10, 2017. Date of publication xxx; date of current version xxx. This research is partly supported by the NRF, Prime Minister's Office, Singapore under the Energy Programme and administrated by the EMA (EP Award No. NRF2014EWT-EIRP002-040); partly supported by the research grant for the Human-Centered Cyber-physical Systems Programme at ADSC from A∗STAR, Singapore; and partly supported by Guangdong Innovative and Entrepreneurial Research Team Program (No. 2014ZT05D238). The work of Y. Wu was done at Institute for Infocomm Research, A∗STAR, Singapore. The associate editor coordinating the review of this manuscript and approving it for publication was xxx

Y. Wu is with Institute for Infocomm Research, Singapore (e-mail: wuyd007@qq.com).

B. Chen is with Advanced Digital Sciences Center, Singapore (e-mail: Binbin.chen@adsc.com.sg).

Z. Zhao and Y. Cheng are with Institute for Infocomm Research, Singapore (e-mail: {zzhao,cheng_yao}@i2r.a-star.edu.sg).

Digital Object Identifier XXX.

codeword can be used in Password-Authenticated Key Exchange (PAKE) protocol [34] so as to build a strongly secure channel. Alternatively, fuzzy commitment/extractor schemes (e.g., [35]–[38]) replace Euclidean distance with Hamming distance in calculating the measurement similarity. To this end, they convert the Euclidean measurements into a binary feature sequence, incurring some measurement information loss.

In order to avoid information leakage and loss in the reconciling step, some pairing schemes (e.g., Magparing [39] and ShaVe [40], [41]) adopt a one-round key agreement protocol (e.g., Diffie-Hellman protocol [42]) and a two-round interlock protocol [43] to securely exchange measurements. If and only if the similarity of measurements is higher than a predefined threshold, the two devices conclude that there is no MitM attack and their agreed key is authenticated. Here the interlock protocol serves the critical role to expose a potential MitM attacker who compromises the anonymous key agreement protocol. Roughly speaking, in the interlock protocol, the two parties encrypt their messages using each other's key, then send only the first half of their encrypted messages to each other. Only after they receive each other's first message, they then send the second half of their encrypted messages. The interlock protocol works because one cannot decrypt an encrypted message by looking at its first half only. Thus, the MitM attacker will not be able to decrypt the first half-message and re-encrypt it using an unauthenticated key. If the attacker waits for the second half of a message, it is already too late to change the first half of the message. We call device pairing schemes that use interlock protocol in its reconciling step *interlock-based device pairing schemes*.

This paper points out a security flaw of such interlock-based device paring schemes. The identified security flaw allows an attacker to launch a successful MitM attack by changing the traffic. Specifically, the attacker can create manipulated measurement data that is highly correlated with the genuine device measurement. Hence, the devices will wrongly conclude that no attack exists. Using the same setting from the Magpairing paper [39], the analysis and experiments show that the attack almost surely succeeds to impersonate the communication parties while incurring very low computation overhead. In addition, this paper points out that the root cause of this security flaw is due to the violation of the one-wayness assumption made by the original security analysis in these schemes. Based on this, this flaw is fixed by properly ensuring the one-wayness in the schemes.

The remainder of this paper is organized as follows. Section II uses Magpairing as an example to introduce the interlock-based device pairing schemes and the threat model. Section III presents the new MitM attack that succeeds by exploiting the security flaw in the interlock-based device pairing schemes, and discusses the countermeasures for the new attack. Section IV evaluates the success probability and overhead for the new attacks. Finally, conclusion is drawn in Section V.

II. Interlock-based Device Pairing Schemes

The flaw revealed in this work exists in a general form of interlock-based device paring schemes that can be based on different types of physical measurements (e.g., vibration, wireless signal, magnetic signal, etc.), hence the revealed security flaw can have a broad impact. This section introduces the Magpairing scheme [39] as a concrete example to describe the revealed flaw. Other schemes, e.g., the widely-cited ShaVe scheme [40], [41] and those adopt its design (e.g., [44]–[46]) are all subject to the same flaw.

A. Magpairing scheme

In order to securely exchange information between two smartphones in close proximity that do not share any pre-established secret key in advance, the pairing scheme Magpairing [39] enables the smartphones to share an authenticated key by utilizing their similar magnetic field measurements which form a data array.

With reference to Fig.1, Magpairing scheme has three steps. The first step is the standard Diffie-Hellman key exchange protocol which creates unauthenticated keys (K_A and K_B) between the communication parties Alice and Bob. In order to ensure the authenticity of the communication channel, smartphones of both Alice and Bob sample the magnetic fields and carry on a pre-processing step [1] to transform the magnetic field readings into measurement data d_A and d_B.

The second step is to exchange the magnetic field measurements with the interlock protocol [43]. Specifically, Alice chooses a random Initialization Vector (IV) h_A, and encrypts the magnetic field measurements d_A into ciphertext

$$c_A = \mathcal{E}(K_A, d_A \oplus h_A) \tag{1}$$

where $\mathcal{E}(\cdot)$ is a block encryption function in Cipher Block Chaining (CBC) operation mode[2], and $x \oplus y$ is the exclusive-or operator between x and y. Then Alice sends a message A_1 including c_{A1} (the first half of ciphertext c_A) and h_{A1} (the first half of IV h_A) to Bob. Similarly, Bob creates an IV h_B and a ciphertext c_B. After receiving the message A_1, Bob sends message B_1 including the first halves of c_B and h_B to Alice. Afterwards, both Alice and Bob exchange the second halves of the ciphertexts and IVs.

The last step is to verify the similarity of magnetic field measurements. After assembling the ciphertext $c_A = c_{A1}|c_{A2}$ and IV $h_A = h_{A1}|h_{A2}$, Bob will recover the measurement

$$\tilde{d}_A = \mathcal{D}(K_B, c_A) \oplus h_A \tag{2}$$

where $\mathcal{D}(\cdot)$ is the block decryption algorithm corresponding to the encryption algorithm $\mathcal{E}(\cdot)$. Then Bob makes a decision based on a policy: if the Pearson's correlation value

$$r_B = corr(\tilde{d}_A, d_B) > r_0 \tag{3}$$

the decryption key K_B in Eq.(2) is equal to the encryption key K_A in Eq.(1), where r_0 is the predefined threshold. Similarly, Alice recovers Bob's measurement

$$\tilde{d}_B = \mathcal{D}(K_A, c_B) \oplus h_B \tag{4}$$

[1]For simplicity, we ignore the pre-processing step which is out of the scope of the present paper. We refer readers to the original paper [39] for details of this step.

[2]Strictly speaking, Eq.(1) and Eq.(2) are valid for the first ciphertext block only as the "IV" will be changed for all the other blocks in CBC mode. For the sake of exposition, the present paper adopts the same formula as Magpairing for encryption/decryption.

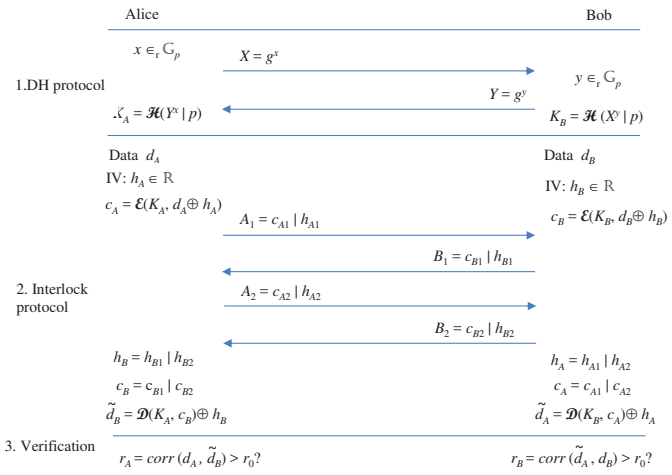

Fig. 1. Schema of Magpairing scheme [39], where p is a large prime, g is a generator of finite field $\mathbf{G}_p$, $\mathcal{H}(\cdot)$ is a one-way function, $x \oplus y$ is the exclusive-or of string x and y, and $x|y$ is the concatenation of string x and y, $c_A = c_{A1}|c_{A2}$, and $h_A = h_{A1}|h_{A2}$.

and then determines whether $K_A = K_B$ by checking the correlation value

$$r_A = corr(\tilde{d}_B, d_A) > r_0 \tag{5}$$

B. MitM implementation in near authentication

In an MitM attack, adversary Eve is able to easily sniffer/manipulate traffic and impersonate genuine users Alice and Bob by sitting between them. Hence most security protocols are required to be resilient to MitM attack. In the "near" authentication schemes, Eve is challenged in starting an MitM attack because he is further away from Alice and Bob. Nonetheless, Eve is still able to "sit" between them in several ways if Alice and Bob communicate with each other via wireless channels. For examples,

(1) If Alice and Bob communicate with each other via an access point, Eve can compromise the access point, or fake an access point so as to stay in the middle of them.

(2) If Alice and Bob have multiple communication channels, Eve can communicate with them via different channels. For instance, WiFi (IEEE 802.11 b/g) supports three independent channels (channel 1, channel 6, and channel 11). Eve (impersonating Bob) can communicate with Alice on channel 1, and at the same time he (impersonating Alice) can communicate with Bob with channel 6.

(3) Even when there is only one single, well-specified direct communication channel between Alice and Bob, the attack scenario can still be carried out in the following way with some assumption about Eve's capability. Specifically, assume Alice sends a message m_x to Bob, and Alice's wireless signal received by Bob is x. At the same time, Eve sends another message m_y to Bob, and Eve's wireless signal received by Bob is y. The total wireless signal received by Bob is $z = x + y$. If the energy of y is significantly higher than that of x (e.g., because Eve uses an emitter of higher transmission power and/or uses a directional antenna to concentrate its transmission power to Bob), Bob may obtain Eve's message m_y after the decoding. At the same time, although Eve also receives the combined signal from Alice and himself, since he knows his own signal, he can remove that to recover Alice's signal. Hence, Eve is still able to obtain Alice's message m_x. As a result, Bob obtains the message m_y from Eve and Eve obtains the message m_x from Alice. That is to say, Eve logically "sits" between Alice and Bob.

C. Prior MitM attacks to interlock protocol

As a generic and powerful building block, the security of interlock protocols have been studied previously, in particular, by [47], [48].

Bellovin and Merritt [47] presented an attack that will allow an MitM attacker to access sensitive (and invariant) information such as password if the genuine users/devices do not run the interlock protocol in parallel. For pairing scheme like Magpairing, interlock protocol is used to deliver time-variant private measurements. Hence, the access to information exchanged by interlock protocol itself does not constitute an effective attack, especially for the continuous authentication applications of device pairing schemes.

Ellison [48] discussed a dictionary attack to interlock protocol if the messages being exchanged have low entropy. In addition, Ellison also proposed a bit-by-bit message exchange protocol that can handle low-entropy messages in a more secure manner. For pairing schemes like Magpairing, the entropy of the physical measurements can be high enough to foil the dictionary attack. Also, the bit-by-bit countermeasure may be incur excessive communication overhead and delay for pairing schemes.

D. Security of Magpairing scheme under MitM attack

In the Magpairing scheme, the adversary Eve is assumed to be able to eavesdrop, change, delay, replay, inject and block any message in the communication channel, but unable to crack the devices and the crypto-algorithms. In addition, Magpairing assumes that Eve is far away from Alice (and Bob) such that Eve's measurement d_E has low correlation with any of Alice's measurement d_A and Bob's measurement d_B. Mathematically, Magpairing assumes that the Pearson's correlation values between the original measurements of the three parties satisfy:

$$\begin{cases} r_{AB} &= corr(d_A, d_B) > r_0 \\ r_{EA} &= corr(d_E, d_A) < r_0 \\ r_{EB} &= corr(d_E, d_B) < r_0 \end{cases} \tag{6}$$

That is to say, before the interlock protocol starts, Eve is unable to create any ciphertext such that Eq.(3) or Eq.(5) holds.

According to the security analysis in [39], Eve cannot create a new ciphertext c_E ($c_E \neq c_A$ and $c_E \neq c_B$) before receiving messages A_2 and B_2 in Fig.1 to make either Eq.(3) or Eq.(5) hold. Hence, Magpairing claims to be secure against MitM attack. In other words, if an MitM attack is launched, Magpairing claims that the correlation values between the recovered measurements and the original measurements satisfy:

$$\begin{cases} r_A &= corr(\tilde{d}_B, d_A) < r_0 \\ r_B &= corr(\tilde{d}_A, d_B) < r_0 \end{cases} \tag{7}$$

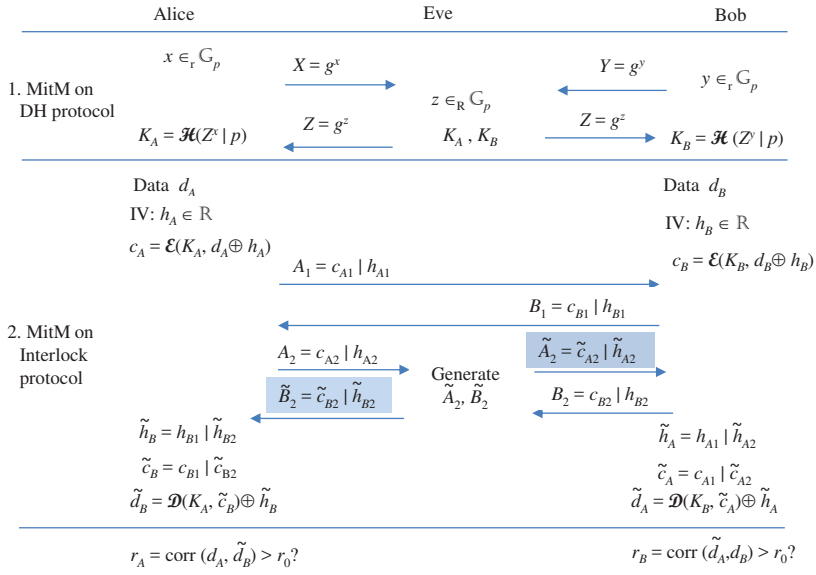

Fig. 2. MitM attack on Magpairing scheme [39]. The messages in the shadow boxes are faked by the attacker.

In reality, it is not surprising that some security protocols as even "provably secure" protocols may be broken [49]. Unfortunately, the above claim in Eq. (7) is not true under an MitM attack as Magpairing does not analyze the attack activities after Eve receives messages A_2 and B_2. Indeed, as we will present in the following, the interlock protocol does not guarantee the one-wayness of Eq.(2). In other words, by choosing a $\tilde{d}_A$ which is correlated to d_B, Eve is able to select a tuple $(K_B, \tilde{c}_A, \tilde{h}_A)$ such that Eq.(2) holds. Similarly, Eq.(4) is not one-way either. Section III will elaborate how Eve exploits this flaw to invalidate Eq.(7).

III. An Attack on Interlock-based Device Pairing Scheme and Countermeasures

According to the decision policy in step 3 of Magpairing scheme, if the recovered peer's magnetic measurement is highly correlated with the local measurement, the device will regard the negotiated key to be authenticated. Hence, an attacker's goal is to fake traffics to produce the high correlation value. Fig.2 illustrates how to realize the target, including the well-known attack on Diffle-Hellman key exchange protocol (see Subsection III-A) and tampering with the traffic in interlock protocol (see Subsections III-B and III-C).

A. MitM attack on Diffie-Hellman key exchange protocol

It is well-known that Diffle-Hellman key agreement protocol is not authenticated and vulnerable to MitM attack. This classic attack is illustrated in the step 1 of Fig.2, where the adversary Eve separately runs Diffle-Hellman key agreement protocol with Alice and Bob in the attack. After the attack is completed, Alice has a secret K_A, Bob has a secret K_B and Eve has both K_A and K_B. But $K_A = K_B$ with a negligible probability.

As assumed in the original Magpairing scheme [39] (see details in Subsection II-D), when Eve merely encrypts/decrypts the intercepted traffic with K_A and/or K_B, the legal participants are able to detect the conventional MitM attack on Diffie-Hellman protocol with Eq.(7). However, as we will present in the following two subsections, the design of device-pairing schemes actually allows Eve to manipulate the second halves of the encrypted messages in a way that the tampered messages can violate Eq.(7) hence cause an effective attack. We will first present the MitM attack in the simpler case with a single block, then extend the attack to the case with multiple blocks and show that it remains almost as effective as the single block case.

B. MitM attack for a single-block case

When the measurement is short, the encryption/decryption process is simple. In this case, the size of ciphertext c_A (or c_B) is the cipher blocksize n (*e.g.*, $n = 128$ for AES). This Subsection will elaborate the manipulation method on a single-block case.

1) Attack method: With reference to Fig.2, the Interlock protocol consists of two rounds. In the first round, Alice and Bob exchange their first halves of ciphertexts and IVs: $A_1 = c_{A1}|h_{A1}$ and $B_1 = c_{B1}|h_{B1}$. The attacker Eve merely stores and forwards the messages A_1 and B_1. But in the second round, the attacker will intercept the traffic and then replace them with faked ones, as shown in Fig.3. Specifically [3],

- *Step 1: Recovering measurements*. After intercepting the message $A_2 = c_{A2}|h_{A2}$ sent from Alice to Bob, Eve forms $c_A = c_{A1}|c_{A2}$ and $h_A = h_{A1}|h_{A2}$, and then recovers $d_A = \mathcal{D}(K_A, c_A) \oplus h_A$. Similarly, Eve forms c_B, h_B and then recovers $d_B = \mathcal{D}(K_B, c_B) \oplus h_B$.

[3]For ease of exposition, we assume that the order to send A_2 or B_2 is not restricted in the following. However, if A_2 must be sent ahead of B_2, d_B in Eq.(8) is approximated with d_A, otherwise, if B_2 must be sent ahead of A_2, d_A in Eq.(11) is approximated with d_B.

- *Step 2: Crafting the second half message*. Eve chooses a $\frac{n}{2}$-bit random number $\tilde{c}_{A2}$, forms a faked ciphertext block $\tilde{c}_A = c_{A1}|\tilde{c}_{A2}$, and calculates
$$\tilde{h}_{A1}|\tilde{h}_{A2} = \mathcal{D}(K_B, \tilde{c}_A) \oplus d_B \quad (8)$$
where $\tilde{h}_{A1}$ and $\tilde{h}_{A2}$ are of the same size $n/2$.
- *Step 3: Checking similarity*. Eve forms a faked ciphertext block $\tilde{c}_A = c_{A1}|\tilde{c}_{A2}$ and faked IV $\tilde{h}_A = h_{A1}|\tilde{h}_{A2}$. Then according to Eq.(2), Eve mimics Bob's behavior to recover Alice's magnetic field measurements
$$\tilde{d}_A = \mathcal{D}(K_B, \tilde{c}_A) \oplus \tilde{h}_A \quad (9)$$
and then computes Pearson's correlation value
$$r_B = corr(\tilde{d}_A, d_B) \quad (10)$$
If $r_B < r_0$, Eve repeats step 2: *Crafting the second half message*.
- *Step 4: Faking traffic*. Eve sends the faked message $\tilde{A}_2 = \tilde{c}_{A2}|\tilde{h}_{A2}$ to Bob.

Eve is able to impersonate Bob to cheat Alice in the same way except Eq.(8) is replaced with
$$\tilde{h}_{B1}|\tilde{h}_{B2} = \mathcal{D}(K_A, c_{B1}|\tilde{c}_{B2}) \oplus d_A \quad (11)$$

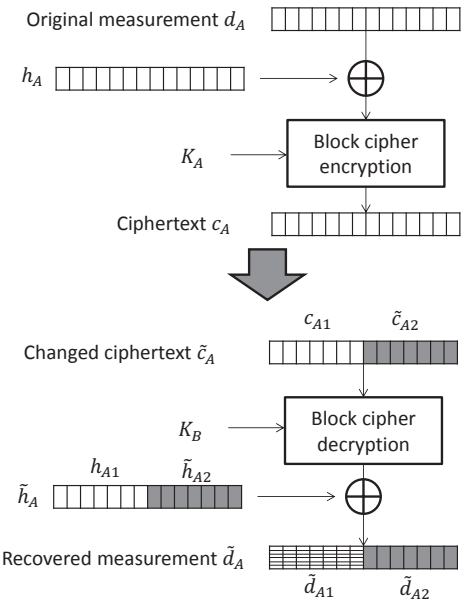

Fig. 3. Attacked data flow in CBC mode for one-block measurement, where the white blocks are intact, the solid gray blocks are intentionally manipulated, and the rest of the blocks are unintentionally changed.

Afterwards, Alice and Bob will continue the pairing process with the faked messages $\tilde{A}_2$ and $\tilde{B}_2$ till the completion of the pairing protocol. Nonetheless, even if they protect their communication channel with the generate keys K_A and K_B, Eve is able to intercept and decrypt the traffic.

Intuitively, the present attack works with a high probability because given any randomly chosen $\tilde{c}_{A2}$, by crafting a companion $\tilde{h}_{A2}$ based on Eq.(8), the attack ensures that the recovered second-half measurement, i.e., $\tilde{d}_{A2}$, will be a perfectly-matching one that the receiver is expecting. Although the first-half of the measurement will look like random value to the receiver, the combination of a perfect second half and a random first half will result in a high chance that the combined message will pass the overall correlation threshold checking. Also, note that Eve performs step 2 and step 3 above in a purely offline manner, and will only continue to the interlock session (in step 4) after it generates a good faked message. Hence, from Alice and Bob's point of view, they are unaware of the multiple retries that may happen in step 2 and step 3.

2) Analysis on attack probability: Rewriting Eq.(8) as
$$\mathcal{D}(K_B, \tilde{c}_A) = d_B \oplus (\tilde{h}_{A1}|\tilde{h}_{A2}) \quad (12)$$
with reference to Eq.(2), Eve mimics Bob's behavior to recover Alice's magnetic field measurements as
$$\begin{aligned} \tilde{d}_A &= \mathcal{D}(K_B, \tilde{c}_A) \oplus \tilde{h}_A \\ &= d_B \oplus (\tilde{h}_{A1}|\tilde{h}_{A2}) \oplus (h_{A1}|\tilde{h}_{A2}) \\ &= d_B \oplus ((\tilde{h}_{A1} \oplus h_{A1})|0) \end{aligned} \quad (13)$$
Denote the recovered data $\tilde{d}_A = \tilde{d}_{A1}|\tilde{d}_{A2}$ and Bob's measurement $d_B = d_{B1}|d_{B2}$, where the size of $\tilde{d}_{A1}, \tilde{d}_{A2}, d_{B1}$ and d_{B2} are $0.5n$. Then rewrite Eq.(13) into two parts as
$$\tilde{d}_{A1} = d_{B1} \oplus (\tilde{h}_{A1} \oplus h_{A1}) \quad (14)$$
and
$$\tilde{d}_{A2} = d_{B2} \oplus 0 = d_{B2} \quad (15)$$
Eq.(15) shows that the second half of the recovered data $\tilde{d}_A$ is identical to that of Bob's measurement[4]. That is to say, given that the second half of $\tilde{d}_A$ is equal to the second half of d_B, Eve is able to find a tuple $(K_B, c_{A1}|\tilde{c}_{A2}, h_{A1}|\tilde{h}_{A2})$ such that Eq.(2) holds, *i.e.*, one-wayness is violated.

Fig.4 is a screenshot taken from our proof-of-concept implementation (more details in Section IV) of the above attack process. As shown in the top-left boxes, the first half of faked ciphertext (and faked IV) is the same as that of true ciphertext (true IV respectively). But with the faked second halves, the measurement recovered from the faked data has the same second half as true data (right bottom box). That is to say, the faked data is correlated with the genuine measurement.

Assume the mean of $\tilde{d}_A$ and d_B are 0 as Pearson's correlation value is translation-invariant and scale-invariant, the Pearson's correlation value
$$\begin{aligned} r_B &= corr(\tilde{d}_A, d_B) = \frac{\tilde{d}_{A1} \cdot d_{B1} + \tilde{d}_{A2} \cdot d_{B2}}{\| \tilde{d}_A \| \cdot \| d_B \|} \\ &= \frac{\tilde{d}_{A1} \cdot d_{B1} + \| d_{B2} \|^2}{\| \tilde{d}_A \| \cdot \| d_B \|} \\ &= \frac{\tilde{d}_{A1} \cdot d_{B1}}{\| \tilde{d}_A \| \cdot \| d_B \|} + \frac{\| d_{B2} \|^2}{\| \tilde{d}_A \| \cdot \| d_B \|} \\ &= V + U \end{aligned} \quad (16)$$

[4]In the Magpairing scheme, the message is appended with user's identity which is not always possible to be verified, *e.g.*, in an ad-hoc environment, or non-direct communication channel. Moreover, even if it is possible to check identity, the protection is also very weak as the short identity verification is vulnerable to brute force attack.

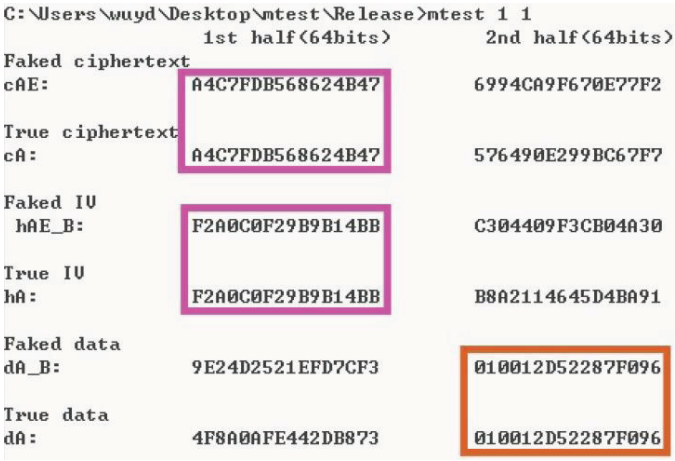

Fig. 4. The original data and faked data, where there is only one ciphertext block.

where $x \cdot y$ is the inner product of x and y, $\| x \| = \sqrt{x \cdot x}$, V and U are the first item and second item of Eq.(16) respectively. As $\tilde{d}_{A1}$ and d_{B1} are independent, the expected value $E(V) = 0$. Suppose $\| \tilde{d}_A \| \approx \| d_B \|$ and their elements are identically and independently distributed, the expected value $E(U) = 0.5$. Thus $E(r_B) = E(U+V) = 0.5$. Similarly, $E(r_A) = 0.5$.

Example 1: Assume each element of the measurement is uniformly distributed over bipolar [5] set $\{-1, 1\}$. Then

$$\begin{aligned} r_B &= \frac{\tilde{d}_{A1} \cdot d_{B1}}{\| \tilde{d}_A \| \cdot \| d_B \|} + \frac{\| d_{B2} \|^2}{\| \tilde{d}_A \| \cdot \| d_B \|} \\ &= \frac{\tilde{d}_{A1} \cdot d_{B1}}{n} + \frac{0.5n}{n} \\ &= \frac{v_1 + v_2 + \cdots + v_{0.5n}}{n} + 0.5 \end{aligned} \tag{17}$$

Suppose the AES cipher is used and the length of ciphertext is $n = 128$ bits, then

$$r_B = \frac{v_1 + v_2 + \cdots + v_{64}}{128} + 0.5 \tag{18}$$

where v_i $(i = 1, 2, \ldots, 64)$, the product of the ith element of $\tilde{d}_{A1}$ and d_{B1}, is uniformly and independently distributed over $\{-1, 1\}$. Hence, for any random variable v_i, its mean is 0 and variance is $\sigma_0^2 = (-1)^2 \times 0.5 + 1^2 \times 0.5 = 1$. According to central limit theorem,

$$V = \frac{v_1 + v_2 + \cdots + v_{64}}{128} \tag{19}$$

is approximately a normal distribution $\mathcal{N}(0, \sigma^2)$, where the variance $\sigma^2 = \sigma_0^2/256 = 1/256$. Therefore, the random variable r_B roughly follows a normal distribution $\mathcal{N}(0.5, 1/256)$. That is to say, the attack success probability

$$p_1 = P(r_B > r_0 = 0.5) \approx 0.5 \tag{20}$$

if Eve randomly chooses $\tilde{c}_{A2}$ once. Moreover, if Eve tries random $\tilde{c}_{A2}$ for t times, the attack succeeds with a probability

$$P_t = 1 - (1 - p_1)^t \approx 1 - 0.5^t \tag{21}$$

[5]The example message can be extended to bipolar array $\{a_0, a_1\}$ for any real number a_0 and a_1 as Pearson's correlation value is transit and scale invariant.

because the attacker wins as long as she has one trial that makes $r_B > 0.5$.

Therefore, an adversary is able to successfully impersonate the participants with a high probability by simply trying different $\tilde{c}_{A2}$ for a small number of times.

C. Extended MitM attack for a multiple-block case

The attack shown in Subsection III-B is viable because the second half of the IV can be arbitrarily selected by the adversary. Nonetheless, as IV is only applicable to the first n bits of the message, the success probability of the attack presented in Subsection III-B decreases with the number of the ciphertext blocks. For the ciphertext with multiple blocks, Eve has to extend the above attack.

1) Extended attack method: In the extended scheme, the MitM attack to Diffie-Hellman protocol is the same as those elaborated in Subsection III-A, and the first round of the interlock protocol of Magpairing is intact. However, after intercepting the second halves of all ciphertexts (*i.e.*, A_2 and B_2), Eve will launch the attack as shown in Fig.5. Specifically,

- *Step 1: Recovering measurements.* Eve recovers the original magnetic field measurements d_A and d_B, this is similar to the single block case in Subsection III-B.
- *Step 2: Crafting the second-half message.* Suppose there are l ciphertext blocks. Eve starts with the last block, chooses a random $\frac{n}{2}$-bit $\tilde{c}_{lA2}$, forms a faked cipher block $\tilde{c}_{lA} = c_{lA1} | \tilde{c}_{lA2}$, and calculates

$$\tilde{h}_{lA1} | \tilde{h}_{lA2} = \mathcal{D}(K_B, \tilde{c}_{lA}) \oplus d_{lB} \tag{22}$$

  Under the CBC mode, $\tilde{h}_{lA2}$ comes from the ciphertext of its previous block, i.e., $\tilde{c}_{jA2}$, where $j = l - 1$. Hence, when Eve tries to manipulate the decoded measurement of the lth block, she needs to make change to the ciphertext of the previous block as well.
  Now let us look at the block $j = l - 1$. To manipulate the value for the decode measurement from the jth block, Eve calculates

$$\tilde{h}_{jA1} | \tilde{h}_{jA2} = \mathcal{D}(K_B, \tilde{c}_{jA}) \oplus d_{jB} \tag{23}$$

  and sets the second half of the ciphertext of its previous block $\tilde{c}_{iA2} = \tilde{h}_{jA2}$, where $i = j - 1$.
  Eve repeats the same message crafting process for the remaining blocks, one at a time, from block $j - 1$, block $j - 2$, to the first block. Note that, for the first block, $\tilde{h}_{1A2}$ is the second half of the IV. Hence, we also denote it by $\tilde{h}_{A2}$.
- *Step 3: Checking similarity*. Eve forms $\tilde{h}_A = h_{A1} | \tilde{h}_{A2}$, and ciphertext $\tilde{c}_A = \tilde{c}_{1A} | \tilde{c}_{2A} | \cdots | \tilde{c}_{lA}$, where the faked ciphertext block $\tilde{c}_{jA} = c_{jA1} | \tilde{c}_{jA2}$, $j = 1, 2, \ldots, l$. Then according to Eq.(2), Eve mimics Bob to recover Alice's magnetic field measurements as

$$\tilde{d}_A = \mathcal{D}(K_B, \tilde{c}_A \oplus \tilde{h}_A) \tag{24}$$

  and calculates Pearson's correlation value

$$r_B = corr(\tilde{d}_A, d_B) \tag{25}$$

  If $r_B < r_0$, Eve repeats the attack from step 2.

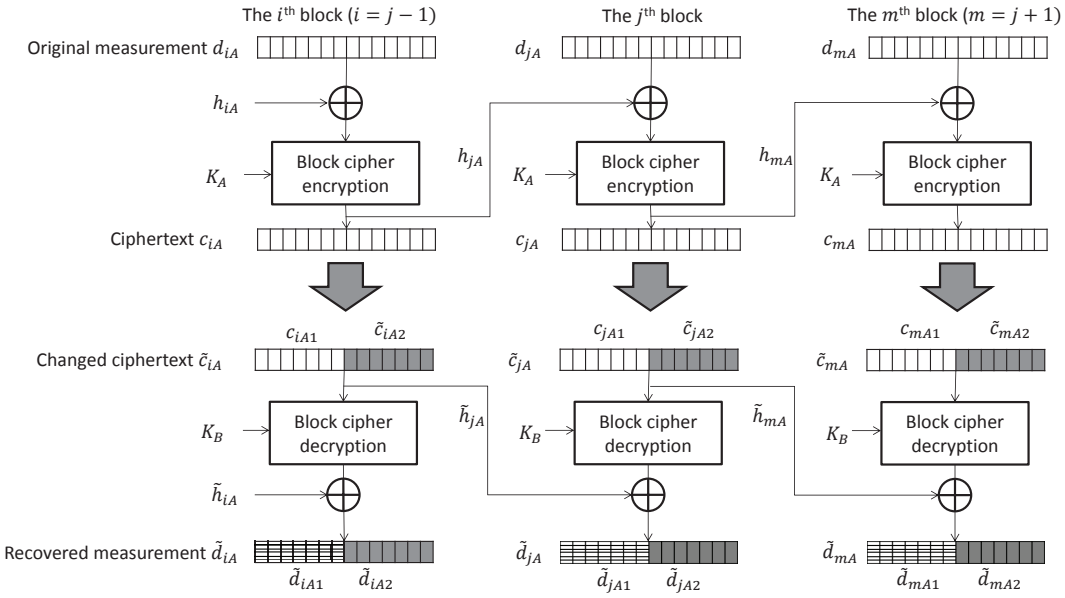

Fig. 5. Attacked data flow in CBC mode, where the white blocks (*e.g.*, c_{jA1}) are intact, the solid gray blocks (*e.g.*, $\tilde{c}_{jA2}$, and $\tilde{d}_{jA2}$) are intentionally manipulated, and the rest of blocks (*e.g.*, $\tilde{d}_{jA1}$) are unintentionally changed.

- *Step 4: Faking traffic*. As summarized in the second column of Table I, the faked traffic is

$$\tilde{A}_2 = \tilde{c}_{1A2}|\tilde{c}_{2A2}|\cdots|\tilde{c}_{lA2}|\tilde{h}_{A2} \tag{26}$$

and will be sent to Bob.

TABLE I
FAKED HALF-BLOCKS OF $\tilde{A}_2$

Original half-blocks	Faked one	Faking method
c_{lA2}	random	random
$c_{iA2}, i = l-1$	$\tilde{h}_{lA2}$	Eq.(22)
$c_{iA2}, i = l-2, \ldots, 1$	$\tilde{h}_{jA2}, j = i+1$	Eq.(23)
h_{A2}	$\tilde{h}_{1A2}$	Eq.(23)

Similarly, Eve will manipulate traffic B_2 sent from Bob to Alice. Alice and Bob will continue the rest steps of Magpairing after they receive the manipulated traffic.

2) Analysis on attack probability: Denote Bob's jth measurement block as $d_{jB} = d_{jB1}|d_{jB2}$, and the recovered plaintext block as $\tilde{d}_{jA} = \tilde{d}_{jA1}|\tilde{d}_{jA2}$, where the length of d_{jB1}, $\tilde{d}_{jA1}$, d_{jB2} and $\tilde{d}_{jA2}$ are $n/2$. Therefore, with reference to Eq.(14),

$$\tilde{d}_{jA1} = d_{jB1} \oplus (\tilde{h}_{jA1} \oplus h_{jA1}) \tag{27}$$

Meanwhile, similar to Eq.(15), we have

$$\tilde{d}_{jA2} = d_{jB2} \oplus 0 = d_{jB2} \tag{28}$$

Similar to Fig.4, Fig.6 is a screenshot of our attack process, where the ciphertext has two blocks. As shown in the left-top boxes, the first half of the faked ciphertext (and the faked IV) is the same as that of the true ciphertext (and the true IV respectively). But with the faked second half of the ciphertext, the recovered faked data has the same second half as the true data (right bottom box) such that the overall recovered measurement is highly correlated with his own measurement.

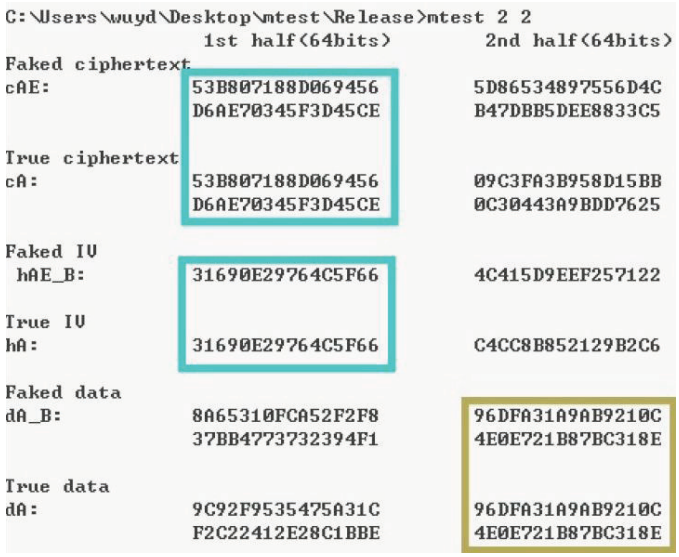

Fig. 6. The original data and faked counterparts, where the number of ciphertext blocks is 2.

Without loss of generality, assume the mean of $\tilde{d}_A$ and d_B are 0. Then Bob calculates Pearson's correlation value as

$$\begin{aligned} r_B &= corr(\tilde{d}_A, d_B) = \frac{\sum_{j=1}^{l}(\tilde{d}_{jA1} \cdot d_{jB1} + \tilde{d}_{jA2} \cdot d_{jB2})}{\| \tilde{d}_A \| \cdot \| d_B \|} \\ &= \frac{\sum_{j=1}^{l}(\tilde{d}_{jA1} \cdot d_{jB1})}{\| \tilde{d}_A \| \cdot \| d_B \|} + \frac{\sum_{j=1}^{l} \| d_{jB2} \|^2}{\| \tilde{d}_A \| \cdot \| d_B \|} \\ &= V + U \end{aligned} \tag{29}$$

where V and U are the first item and second item of Eq.(29) respectively. If all the elements in d_B are identically and

independently distributed, $E(U) = 0.50$, and $E(V) = 0$. Thus, $E(r_B) = 0.50$. Similarly, $E(r_B) = 0.50$ too.

Example 2: With the same assumption as example 1, each element of the measurement is uniformly distributed over $\{-1, 1\}$, the length of one ciphertext block is $n = 128$. Then

$$U = \frac{\sum_{j=1}^{l} \parallel d_{jB2} \parallel^2}{128l} = 0.50 \quad (30)$$

$$V = \frac{\sum_{j=1}^{l} (\tilde{d}_{jA1} \cdot d_{jB1})}{\parallel \tilde{d}_A \parallel \cdot \parallel d_B \parallel} = \frac{v_1 + v_2 + \cdots + v_{64l}}{128l} \quad (31)$$

where all v_i are uniformly and independently distributed over $\{-1, 1\}$. According to central limit theorem, random variable V approximately follows a normal distribution $\mathcal{N}(0, \sigma^2)$, where $\sigma^2 = \frac{\sigma_0^2}{256l} = \frac{1}{256l}$.

Then the attack success probability is the same as Eq.(20) for one attack trial on average, and Eq.(21) for t attack trials.

D. Attack extension to other cipher modes

Magpairing is vulnerable to the present attack because one-wayness requirement is not met in both Eq.(2) and Eq.(4) where CBC cipher mode is used. In fact, besides CBC operation mode, some other cipher modes including Cipher Feedback (CFB) mode, Output Feedback (OFB) mode, and Counter (CTR) mode, do not guarantee the one-wayness property either. Once the one-wayness requirement is not met, an attacker is able to craftily tamper with IV (or other block) such that legal parties fail to detect the MitM attack with Eq.(7). As shown in Fig.7, the attack has similar effect on different popular cipher modes.

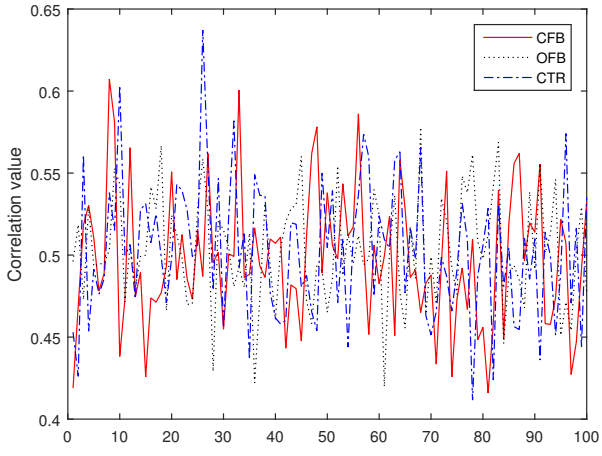

Fig. 7. The attack effect on different cipher modes. The ciphertext has 6 blocks, and each measurement value is of 2 bits.

E. Countermeasures

According to Eq.(7), the security of Magpairing scheme depends on the assertion that an attacker is unable to fake a message which is correlated to the genuine measurement. Thus, one simple countermeasure is to increase the threshold value r_0 to raise the bar for launching a successful attack. However, as shown in the experiments in [39], this countermeasure will increase the false rejection rate such that the usability of Magpairing scheme will be affected. Given that both Alice and Bob execute the interlock-based pairing protocol in parallel, there are two alternative countermeasures as follows.

1) Using message integrity code: In this countermeasure, Alice and Bob first exchange the message integrity codes $I_A = \mathcal{H}(d_A)$ and $I_B = \mathcal{H}(d_B)$ before carrying out the interlock protocol, where $\mathcal{H}(\cdot)$ is a one-way function. This step prevents Eve from changing the following traffic without being identified. Specifically, assume Eve is able to cheat Bob by impersonating Alice to defeat the countermeasure, i.e., knowing neither d_A nor d_B, Eve is able to send to Bob a message integrity code $\hat{I}_A = \mathcal{H}(\hat{d}_A)$ for some $\hat{d}_A$ before the interlock protocol starts; and Bob confirms that the recovered measurement $\tilde{d}_A$ matches $\hat{I}_A$ and is similar to his measurement d_B after the interlock protocol ends. Mathematically, Bob confirms that

$$\mathcal{H}(\tilde{d}_A) = \hat{I}_A = \mathcal{H}(\hat{d}_A)$$

Thus $\hat{d}_A = \tilde{d}_A$ with an overwhelming probability as $\mathcal{H}(\cdot)$ is a one-way function. Furthermore, Bob confirms that

$$corr(\hat{d}_A, d_B) = corr(\tilde{d}_A, d_B) = r_B > r_0 \quad (32)$$

with an overwhelming probability according to Eq.(3). Clearly, Eq.(32) is contradict with the above assumption that Eve knows neither d_A nor d_B before the execution of interlock protocol. Thus Eve cannot successfully impersonate Alice. Similarly, Eve cannot impersonate Bob.

2) Using ECB encryption mode: As Electronic Codebook (ECB) cipher mode does not employ IV in the encryption process, it can be used to defeat the present attack. Specifically, Alice generates a block-wise key $K_{jA} = \mathcal{H}(K_A, j)$ for the jth pliantext block, creates its ciphertext with ECB encryption mode. So does Bob. The rest of Magpairing protocol are intact.

As the key for each block is independent, each ciphertext block is also independent. Eve will need to attack each block independently. For ciphertext block $c_{jA} = c_{jA1}|c_{jA2}$, Eve tries to fake a block $\tilde{c}_{jA} = \tilde{c}_{jA1}|\tilde{c}_{jA2}$, and mimics Bob to calculate

$$\tilde{d}_{jA} = \mathcal{D}(K_{jB}, \tilde{c}_{jA1}|\tilde{c}_{jA2}) \quad (33)$$

As Eve knows neither d_A nor d_B before interlock protocol starts, he does not know how to select $\tilde{c}_{jA1}$, and may select the original c_{jA1} or a random one. However, for each manipulated $\tilde{c}_{jA2}$, Eve is able to calculate Eq.(33) to obtain $\tilde{d}_{jA}$, construct $\tilde{d}_A$ and calculate $r_B = corr(d_B, \tilde{d}_A)$ to check whether the attack succeeds or not.

A block cipher is believed to generate pseudo-random output, hence its output ciphertext is independent with Bob's measurement d_B for each faked $\tilde{c}_{jA2}$. Therefore, the correlation value $r_B = 0$ on average. Particularly, if each measurement item of d_B and d_A is uniformly and independently distributed over some constant set $\{a_0, a_1\}$, r_B approximately follows a normal distribution $\mathcal{N}(0, \frac{\sigma_0^2}{n}) = \mathcal{N}(0, \frac{1}{n})$ according to central limit theorem, where n is the number of measurement items.

Since the probability $P(r_B > r_0 = 0.5)$ is very low for any $n > 144$ according to Six Sigma doctrine, the probability that Eve can bypass this countermeasure is very low too.

IV. Evaluation of the Present MitM Attack

In this Section, we first examine the magnetic fields measured by two neighboring smartphones to verify the suitability of the threshold value recommended by the Magpairing scheme. Then, we present our proof-of-concept which implements the present attack to the reconciliation step of Magpairing scheme and evaluate its effectiveness with simulated measurements and real measurements.

A. Threshold value setting

In their original Magparing paper [39], Jin et al. recommend to use 0.5 as the correlation threshold value. In particular, their experiment shows that, after a series of pre-processing (including data synchronization based on a peak search, spatial alignment, mean value removal, and data reshaping), the average correlation is around 0.6 for 2 seconds of data collection period, which converges to around 0.7 when the data collection period is extended to 4 seconds or more. As reported by them, with 2 seconds of data collection time, the correlation can drop to as low as less than 0.4 in some experiments. Even for 5 seconds of data collection period, the correlation between two phones can still be as low as around 0.6. Hence, to ensure a decent success rate for the pairing, the threshold value cannot be set much higher than 0.5, especially if shorter data collection period is used.

We conduct our own experiments to independently verify the choice of the threshold value. In our experiments, we use two handphones of the same model (Galaxy S6 Edge) to sample the magnetic field. In our experiments, we vary different parameters, including the sampling rate (we found a sampling rate of 5 Hz produces the best result in our experiments), the way the raw data is pre-processed (specifically, we test the case that the strength of the magnetic field instead of a directional vector representation of the field is used), and different orientations/distance between the phones. When one handphone is right above another, we obtain best results. The corresponding measurement samples are illustrated in Fig.8. Due to environment interference and noise, the correlation value of the two phones' measurements has an average value of 0.62 and standard deviation 0.11. Our experiment result verify that setting a correlation threshold higher than 0.5 can substantially increase the pairing failure rate.

We also measure the correlation when the two handphones are 1 meter away from each another. The raw samples in one experiment are shown in Fig.9. For the 5000 experiments we conduct for this setting, the average correlation value between the two phones' measurements is 0.43 and the standard deviation is 0.02. Hence, the threshold $r_0 = 0.5$ is proper in the Magpairing scheme [39] to detect an attacker as close by as 1 meter.

Based on the recommendation from the original Magpairing paper and our own independent experiment results, we use the threshold value of $r_0 = 0.5$ for our following experiments.

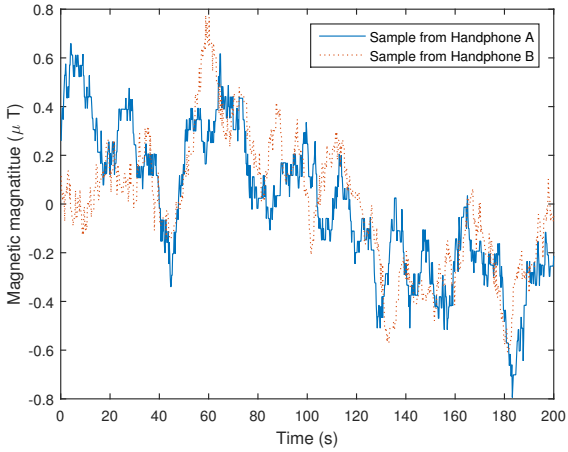

Fig. 8. The amplitude of magnetic fields (mean is set to 0) from two neighboring handphones.

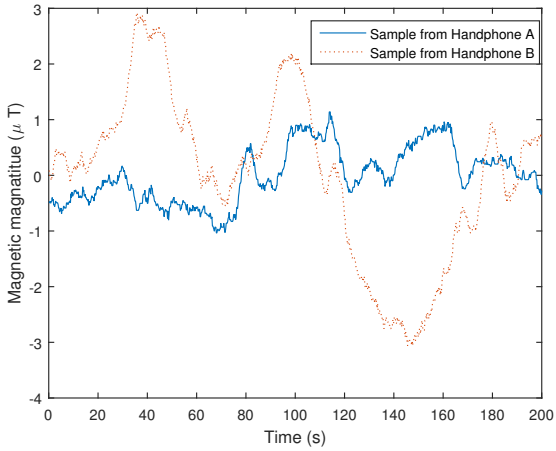

Fig. 9. The amplitude of magnetic fields (mean is set to 0) from two separated handphones.

B. Proof-of-concept implementation

In order to evaluate the effectiveness and performance overhead of the present attack, a proof-of-concept was implemented in C/C++ language[6], where AES-CBC functions in Openssl 0.9.8d library (*https://www.openssl.org/source/*) is used for data protection. In the simulation, Alice is the sender and Bob is the receiver. The workflow of the proof-of-concept for the simulation purpose is as follows.

- Both Alice and Bob are assumed to have two random initialization vectors, and different random keys which are the outputs of the MitM attack to Diffie-Hellman key exchange protocol. Besides, they have the same random measurements in the simulations (see Subsection IV-C and Subsection IV-D), or different real measurements in the experiments (see Subsection IV-E). The attacker Eve knows their keys, but neither initialization vectors nor measurements.

[6]The source code and executable of our implementation are accessible from the website *https://www.dropbox.com/s/zcwfap5u3aooj01/mtest.zip?dl=0*.

- Alice encrypts her measurement with AES cipher, her 128-bit key and initialization vector.
- After obtaining the ciphertext generated by Alice, Eve fakes the 2nd-half of each ciphertext block, from the last block to the first one, as those addressed in Table I.
- Bob decrypts the faked blocks to obtain Alice's measurement, and then calculates the correlation value between his measurement and the obtained Alice's measurement.

We conducted a series of simulations with the proof-of-concept on a Dell Precision 3620 (Intel Core i7-6700 CPU @3.4GHz, 64-bit Windows 7) PC. As a base line, we also carried on experiments with a naive attack scheme, where the adversary has the keys of Alice and Bob (similar to attack to the Diffie-Hellman key exchange protocol addressed in Subsection III-A), but does not modify the inter-lock protocol. The following subsections introduce the experiments according to different measurement types.

C. Results for simulated binary measurement setting

We first study the case where the measured value is represented in binary form. Here, we will also compare the measurement results from our experiments with our theoretical analysis from Section III.

1) Single cipher-block: Fig.10 shows the correlation values from 100 trials of our attack and those from 100 trials of naive attacks, when there is a single ciphertext block. As analyzed in Magpairing scheme, the naive attack has much smaller correlation value (dashed line in Fig.10) than the threshold of 0.5, hence the threshold is reasonable when only the naive attack is considered. However, in the present attack, the correlation values are significantly higher.

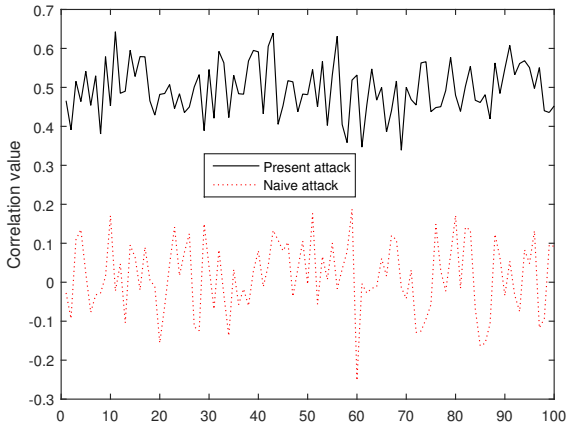

Fig. 10. The correlation value obtained in 100 trials of our attacks on Magpairing scheme [39] when the message is only one block (*i.e.*, $n = 128$ bits), compared with the result from the naive attack.

Fig.11 plots the probability density function of the correlation values from both of empirical evaluation and theoretical analysis. Our experiment shows that for a single trial, the average value of the obtained correlation value is 0.4999 with a standard deviation of 0.0628, which is consistent with the normal distribution $\mathcal{N}(0.5, 1/256) = \mathcal{N}(0.5, 0.0625^2)$ as shown in our analysis. This confirms that our present attack has around 0.5 of probability to succeed with a randomly selected seed. The attack almost surely succeeds with a few rounds of local searching, which can be done locally before the attacker sends the second half message to a victim.

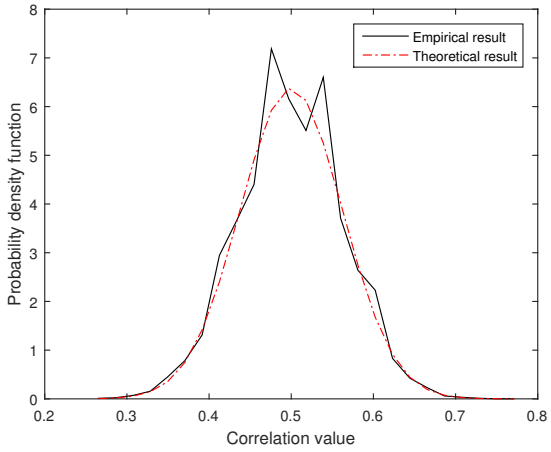

Fig. 11. The probability density function for the correlation value of our attack on Magpairing scheme [39].

2) Multiple cipher-blocks: If there are multiple ciphertext blocks, and the attacks are launched. As shown in the Fig.12, the naive attack still can only obtain small correlation values below the threshold, while the present attack can obtain the correlation values with average 0.5000, and standard deviation 0.0257, which are consistent with the distribution $\mathcal{N}(0.5, \frac{1}{256l}) = \mathcal{N}(0.5, 0.0255^2)$ obtained in our analysis where $l = 6$. In comparison with Fig.10, the correction value of Fig.12 has smaller fluctuation because the standard derivation is reduced with the increased number of blocks. As shown in Fig.13, the theoretical correlation value and empirical correlation value have the similar distribution. Hence, the present attack is also effective for long message setting.

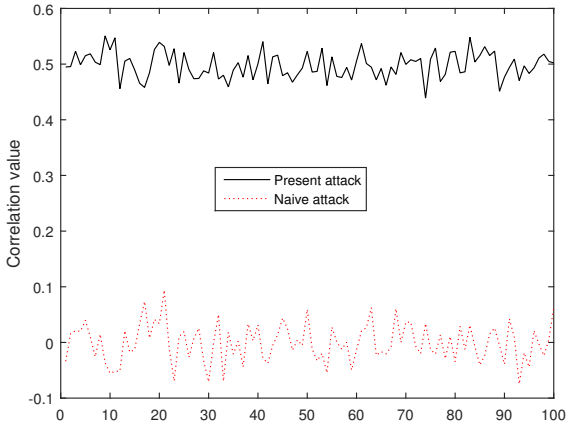

Fig. 12. The correlation value of the attack on Magpairing scheme [39], when the number of AES blocks is 6.

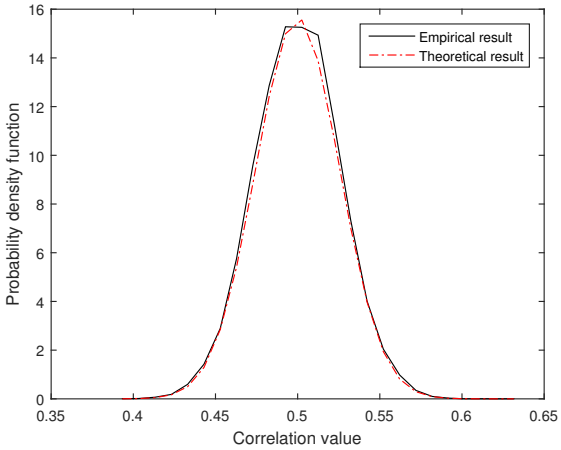

Fig. 13. The probability density function of the correlation value of the attack on Magpairing scheme [39], when the number of AES blocks is 6.

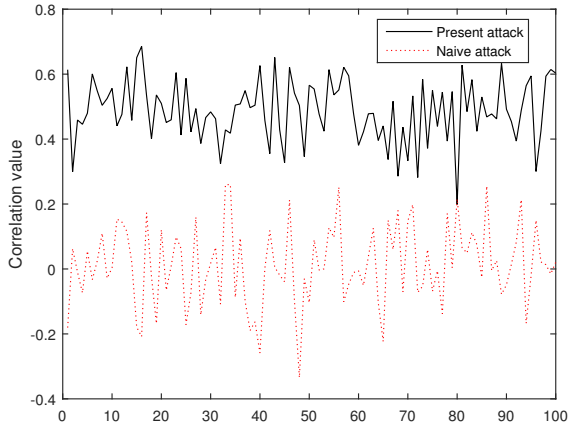

Fig. 14. The correlation values obtained by the attack on Magpairing scheme [39], where the size of each element is 2-bit and there is a single ciphertext block, as compared to that obtained by the naive attack.

D. Results for simulated real-value measurement setting

If the measurement elements are not bipolar, Eve performs the attack with the same method elaborated in Subsection III-A. However, it is not easy to derive the closed-form of the attack probability because the probability distribution of V and/or U in Eq.(16) is hard to describe. Hence, we perform experiments to evaluate the attack probability.

1) Single cipher-block: We first study the setting where each measurement value is of 2-bit. When our attack is launched, as shown in Fig.14, correlation value has the average value 0.4997 and standard derivation 0.0999. In comparison with Fig.10, the correlation value has smaller fluctuation because of the extra bits used to represent the measurement value. We also plot the result for the naive attack, which is consistently below the threshold of 0.5. Fig.15 illustrates the attack rate against the correlation threshold value. As shown, the attack success rate decreases when the threshold increases. However, the attack is still possible when the threshold is 0.7 even with a single trial. Subsection IV-E will show that the attack probability will increase quickly with the number of trials.

2) Multiple cipher-blocks: Now we consider the case when the ciphertext has 6 blocks, and each measurement value is of 4-bit. Fig.16 shows the correlation values obtained by our attack in 100 independent experiments, which have an average value 0.4998 and a standard derivation 0.0581. Fig.17 shows the cumulative distribution function of the correlation values obtained by our attack. They confirm that our attack is effective under this setting as well.

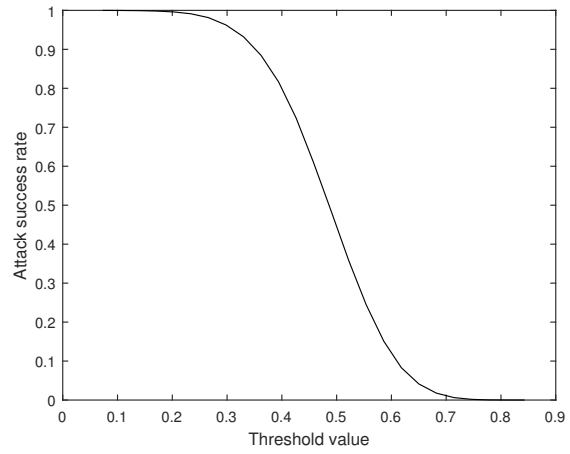

Fig. 15. The attack success rate vs the threshold of correlation value with a single attack trial.

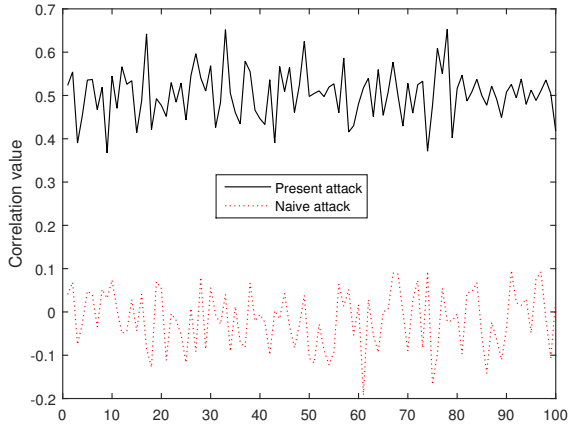

Fig. 16. The correlation values obtained by the attack on Magpairing scheme [39], where the size of each element is 4 bits and the number of ciphertext blocks is 6, as compared to that obtained by a naive attack.

E. Results for real measurement setting

In the above experiments, the measurements are generated from a pseudo-number generator, and are the same for both Alice and Bob. In this subsection, we adopt the real magnetic measurements sampled by two neighboring handphones, where each item of the measurement is of 8-bit, and the number of ciphertext blocks is $l = 31$.

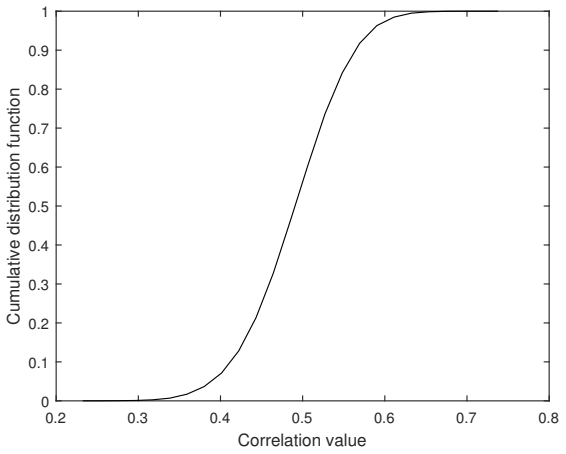

Fig. 17. The correlation value distribution of simulation on attacking Magpairing scheme [39].

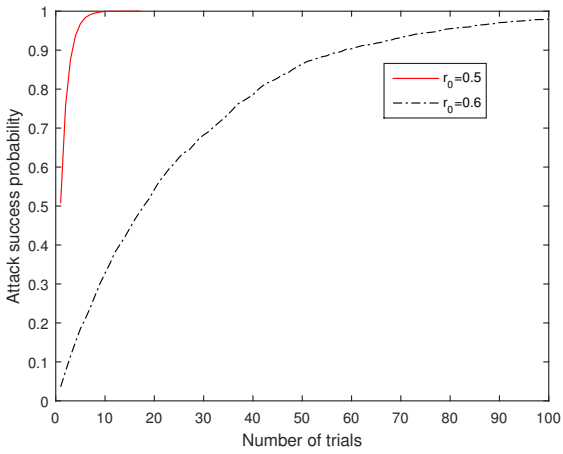

Fig. 18. The attack success probability function for the number of trials needed before the first one succeeds for different threshold values.

In the first experiment with real measurements, both Alice and Bob have the real measurements which have a high correlation value 0.8256. After obtaining the ciphertext generated from Alice, Eve randomly chooses a half AES cipher-block as indicated in step 2 of Subsection III-C1, and fakes 2nd-half of Alice's ciphertext as indicated in Table I. After receiving the tampered ciphertext, Bob calculates the correction value which is similar to Fig.16, where the mean is 0.4970 and standard derivation is 0.0366, and the cumulative distribution function of the correlation value is similar to Fig.17.

In the second experiment with real measurements, the real measurements from the handphones have a marginal correlation value 0.5580. With the same process as the previous experiment, the faked correction value is similar to Fig.16. where the mean is 0.4971 and standard derivation is 0.0367. The cumulative distribution function of the correlation value is similar to Fig.17.

According to these two experiments, we know that the similarity of the original measurements has minor impact on the attack success probability. Meanwhile, we know that the attacker is able to break the Magpairing scheme with a probability 50% for any single trial. Hence, by trying the attack for several times, the attacker is able to invalidate the verification process in Magpairing scheme with an overwhelming probability, as shown in Fig.18.

F. Time needed for launching the attack

In order to realize the real-time attack on Magpairing, Eve should quickly fake the traffic of the 2nd round in interlock protocol. Since the attack incurs most time for the setting of real-value measurements with multiple cipher-blocks, we will present our experimental results for the same setting as Subsection IV-D2. On the Dell Precision 3620 PC (Intel Core i7-6700 CPU @3.4GHz, 64-bit Windows 7), it takes 29.1 μs on average to produce one attack result shown in Fig.17. If an attack trial cannot produce a correlation value which is above the threshold value, the attacker will start a new trial. Fig.18 plots the cumulative distribution function for the number of trials needed before the first one succeeds. As shown, since each trial is independent, the number of trials follows a geometric distribution with success probability around 0.5. It can be seen that our attack succeeds with probability greater than 99% with no more than 8 trials and take less than 250 μs. The success probability is greater than 99.9% with no more than 10 trials and take less than 300 μs. In summary, our attack can be launched in real time, by using common off-the-shelf computing device.

With regard to Fig.15, if the threshold r_0 is increased, the attack success probability will be decreased for each trial. However, if the attacker increases the number of attack trials, the attack success rate can be high. For instance, if the threshold is 0.6, according to Fig.18, if Eve tries the attack simulation 100 times, he has a success rate is 98% after spending about $100 \times 29.1\mu s = 2910\mu s$ calculation time.

V. Conclusion

Secure device pairing is an important building block for device-to-device communication if the devices do not share a secret in advance. Recent schemes like Magpairing and ShaVe leverage the similarity of physical measurements (over some trusted auxiliary channel) made by devices in close proximity, and they use an interlock-based approach to enable the secure pairing process.

This paper discloses a security flaw in their measurement exchange and authentication process, and presents an effective attack that exploits this security flaw. According to the experiments with the developed proof-of-concept, the experimental results are in concert with the theoretical analysis, and the attack succeeds with an over-whelming probability for both simulated measurements and real measurements. In addition, the paper discuss several countermeasures to defeat the presented attack.

References

[1] D. Wang, and P. Wang, "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound," IEEE Trans. on Dependable and Secure Computing, 2017.

[2] R. Prasad and N. Saxena, "Efficient Device Pairing using 'Human-Comparable' Synchronized Audiovisual Patterns," *in Proc International Conference on Applied Cryptography and Network Security*, Lecture Notes in Computer Science (LNCS) 5037, pp. 328-345, 2008.

[3] Y. Wu, F. Bao, and R. H. Deng, "Secure Human Communications Based on Biometrics Signals," *in Proc IFIP International Information Security Conference*, pp.205-221, 2005.

[4] N. Saxena, J.-E. Ekberg, K. Kostiainen, and N. Asokan, "Secure Device Pairing Based on a Visual Channel: Design and Usability Study," IEEE Trans. on Information Forensics and Security, 6(1):28-38, 2011.

[5] T. Perkovic, M. Cagalj, T. Mastelic, N. Saxena, and D. Begusic, "Secure Initialization of Multiple Constrained Wireless Devices for an Unaided User," IEEE Trans. on Mobile Computing, 11(2):337-351, 2012.

[6] S. Schmid, G. Corbellini, S. Mangold, and T. R. Gross, "LED-to-LED Visible Light Communication Networks," *in Proc ACM International symposium on Mobile ad hoc networking and computing*, pp.1-9, 2013.

[7] O. Chagnaadorj, and J. Tanaka, "MimicGesture: Secure Device Pairing with Accelerometer-Based Gesture Input," *in Proc Ubiquitous Information Technology and Applications*, Lecture Notes in Electrical Engineering 214, pp.59-67, 2013.

[8] L. Li, X. Zhao, and G. Xue, "A Proximity Authentication System for Smartphones", IEEE Trans. on Dependable and Secure Computing, 13(6):605-616, 2016.

[9] I. Ahmed, Y. Ye, S. Bhattacharyay, N. Asokan, G. Jacucci, P. Nurmi, and S. Tarkoma, "Checksum Gestures: Continuous Gestures as an Out-of-Band Channel for Secure Pairing," *in Proc ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp.391-401, 2015.

[10] T. Yonezawa, J. Nakazawa, and H. Tokuda, "Vinteraction: Vibration-based Information Transfer for Smart Devices," *in Proc International Conference on Mobile Computing and Ubiquitous Networking*, pp.155-160, 2015.

[11] D. Bichler, G. Stromberg, M. Huemer, and M. Low, "Key Generation Based on Acceleration Data of Shaking Processes," *in Proc International Conference on Ubiquitous Computing*, pp 304-317, 2007.

[12] A. Studer, T. Passaro, and L. Bauer, "Don't Bump, Shake on It: The Exploitation of a Popular Accelerometer-based Smart Phone Exchange and Its Secure Replacement," *in Proc ACM Annual Computer Security Applications Conference*, pp.333-342, 2011.

[13] N. Roy, and R. R. Choudhury, "Ripple II: Faster Communication through Physical Vibration," *in Proc USENIX Symposium on Networked Systems Design and Implementation*, pp.671-685, 2016.

[14] T. J. Pierson, X. Liang, R.d Peterson, and D. Kotz, "WANDA: Securely Introducing Mobile Devices," *in Proc IEEE Conference on Computer Communications*, pp. 1-9, 2016.

[15] S. Sun, Y. Wu, B.S. Lim, and H.D. Nguyen, "A High Bit-Rate Shared Key Generator with Time-Frequency Features of Wireless Channels," *in Proc IEEE Global Communications Conference*, 2017.

[16] L. Cai, K. Zeng, H. Chen, and P. Mohapatra, "Good Neighbor: Ad-hoc Pairing of Nearby Wireless Devices by Multiple Antennas," *in Proc Network and Distributed System Security Symposium*, 2011.

[17] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy:Extracting a Secret Key from an Unauthenticated Wireless Channel," *in Proc ACM international conference on Mobile Computing and Networking*, pp. 128-139, 2008.

[18] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers," IEEE Trans. on Communications, 64(6):2578-2588, 2016.

[19] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and Practical Secret Key Extraction by Exploiting Channel Response," *in Proc IEEE International Conference on Computer Communications*, pp.3048-3056, 2013.

[20] Y. Ding, J. Zhang, and V. F. Fusco, "Retrodirective-Assisted Secure Wireless Key Establishment," IEEE Trans. on Communications, 65(1):320-334, 2017.

[21] W. Xi, X. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast Secret Key Extraction Protocol For D2D Communication," *in Proc IEEE International Symposium of Quality of Service*, pp.350-359, 2014.

[22] E. Gaebel, N. Zhang, W. Lou, and Y. T. Hou, "Looks Good To Me: Authentication for Augmented Reality," *in Proc ACM International Workshop on Trustworthy Embedded Devices*, pp.57-67, 2016.

[23] W. Wang, Z. Wang, W. T. Zhu, and L. Wang, "WAVE: Secure Wireless Pairing Exploiting Human Body Movements," *in Proc IEEE Trustcom/BigDataSE/ISPA*, pp.1243-1248, 2015.

[24] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-Based Security Techniques for Mobile Users in Wireless Networks," IEEE Trans. on Information Forensics and Security, 8(12):2089-2100, 2013.

[25] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body Area Network Authentication Exploiting Channel Characteristics," IEEE Journal on Selected Areas in Communications, 31(9):1803-1816, 2013.

[26] L. Shi, J. Yuan, S. Yu, and M. Li, "MASK-BAN: Movement-Aided Authenticated Secret Key Extraction Utilizing Channel Characteristics in Body Area Networks," IEEE Internet of Things Journal, 2(1):52-62, 2015,

[27] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. L. Huang, "Body Area Network Security: Robust Key Establishment Using Human Body Channel," *in Proc USENIX Workshop on Health Security and Privacy*, 2012.

[28] M. K. Chong, R. Mayrhofer, and H. Gellersen, "A Survey of User Interaction for Spontaneous Device Association," ACM Computing Surveys, vol. 47, vol. 1, Article 8, 2014.

[29] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie-Talkie: Motion-Assisted Automatic Key Generation for Secure On-Body Device Communication," *in Proc ACM/IEEE International Conference on Information Processing in Sensor Networks*, pp.1-12, 2016.

[30] M. F. Haroun, and T. A. Gulliver, "Secret Key Generation Using Chaotic Signals Over Frequency Selective Fading Channels," IEEE Trans. on Information Forensics and Security, 10(8):1764-1775, 2015.

[31] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: Proximity-based Secure Pairing using Ambient Wireless Signals," *in Proc ACM International conference on Mobile systems, applications, and services*, pp.211-224,2011.

[32] L. Yang, W. Wang, and Q. Zhang, "Secret from Muscle: Enabling Secure Pairing with Electromyography," ACM Conference on Embedded Network Sensor Systems, pp.28-41, 2016.

[33] D. Schurmann, A. Brusch, S. Sigg, and L. Wolf, "BANDANA - Body Area Network Device-to-device Authentication using Natural gAit," *in Proc IEEE Conference on Pervasive Computing and Communications*, 2017.

[34] J. Katz, R. Ostrovsky, and M. Yung, "Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords," *in Proc EUROCRYPT*, LNCS 2045, pp. 475-494, 2001.

[35] A. Juels, and M. Wattenberg, "A Fuzzy Commitment Scheme," *in Proc ACM Conference on Comp. and Comm. Security*, pp. 28-36, 1999.

[36] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors:How to Generate Strong Keys from Biometrics and Other Noisy Data," SIAM J. Comput., 38(1):97-139, 2008.

[37] R. Canetti, B. Fuller, O. Paneth, and L. Reyzin, "Key Derivation From Noisy Sources With More Errors Than Entropy," IACR Cryptology ePrint Archive, paper 243, 2014.

[38] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, A. D. Smith, "Reusable Fuzzy Extractors for Low-Entropy Distributions," *in Proc EUROCRYPT*, LNCS 9665, pp. 117-146, 2016.

[39] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra, "MagPairing: Pairing Smartphones in Close Proximity Using Magnetometers," IEEE Trans. on Information Forensics and Security, 11(6):1306-1320, 2016.

[40] R. Mayrhofer, and H. Gellersen, "Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices," IEEE Trans. on Mobile Computing, 8(6):792-806, 2009.

[41] R. Mayrhofer, and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," *in Proc International Conference on Pervasive*, LNCS 4480, pp. 144-161, 2007.

[42] W. Diffie, and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. on Information Theory, 22(6):644-654, 1976.

[43] R. L. Rivest, and A. Shamir, "How to Expose an Eavesdropper," Communications of the ACM, 27(4):393-394, 1984.

[44] D. Liu, J. Chen, Q. Deng, A. Konate, and Z. Tian, "Secure pairing with wearable devices by using ambient sound and light," Wuhan University Journal of Natural Sciences, 22(4):329-336, August 2017.

[45] R. Mayrhofer and H. Gellersen, "Shake well before use: two implementations for implicit context authentication," *in Adjunct Proc. Ubicomp*, pp. 72-75, 2007.

[46] R. Mayrhofer, and H. Gellersen, "Spontaneous mobile device authentication based on sensor data," Information Security Technical Report, vol. 13, pp. 136-150, August 2008.

[47] S. M. Bellovin, and M. Merritt, "An Attack on the Interlock Protocol When Used for Authentication," IEEE Trans. on Information Theory, 40(1):273-275, 1994.

[48] C. M. Ellison, "Establishing Identity Without Certification Authorities," *in Proc USENIX UNIX Security Symposium*, pp.67-76, 1996.

[49] D. Wang, H. Cheng, D. He, and P. Wang, "On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices," IEEE Systems Journal, 2017.