Secure Inductive-Coupled Near Field Communication at Physical Layer

Rong Jin, Member, IEEE, and Kai Zeng, Member, IEEE

Abstract—Near field communication (NFC) is widely used today in many useful applications, such as contactless payment, identification, and file exchange. Due to the limitations on computation, power, and cost of NFC devices, NFC systems often lack encryption or are weakly encrypted, leaving them exposed to security attacks. One solution for this problem is to install strong cryptographic protocols on NFC devices. However, it involves upgrading and revoking deployed NFC devices, which is costly and impractical. Moreover, encryption algorithms are usually considered expensive for resource constrained NFC devices in terms of computation overhead and energy consumption. Aiming at a solution to tackle the security threat without revoking or changing the insecure NFC devices, this paper investigates whether the recent advance of physical layer security can be applied as a means to secure NFC. A detailed analysis is performed to reveal two unique challenges brought by NFC’s data transmission mechanism. A practical solution, SecNFC, through special waveform design at the initiator is proposed. Extensive simulations and concept-proof experiments are conducted to evaluate the performance of our solution. Both simulation and experimental results show that SecNFC can efficiently prevent NFC from eavesdropping with a slight and tolerable decoding performance degradation at the initiator.

Index Terms—Near field communication, inductive coupling, physical layer security, waveform design, confidentiality.

I. INTRODUCTION

NEAR Field Communication (NFC) provides convenient proximity radio communication technology for many useful applications [1]–[4], including contactless payment, identification, and file exchange with NFC tags or posters. Although the communication range of NFC is short, NFC alone does not prevent data modification and eavesdropping [1], [5]. Unfortunately, ISO standard defines no security mechanism for NFC [6].

Manuscript received October 14, 2017; revised February 21, 2018; accepted April 10, 2018. Date of publication May 3, 2018; date of current version June 6, 2018. This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2016JCTD203, in part by the SAST Fund under Grant SAST2016087, and in part by the U.S. National Science Foundation under Grant CNS-1619073 and Grant CNS-1464487. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Chip-Hong Chang. (Corresponding author: Kai Zeng.)

R. Jin is with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: jinrong@hust.edu.cn).

K. Zeng is with the Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA 20230 USA (e-mail: kzeng2@gmu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2018.2832983

One suggested solution to secure NFC is to generate a shared key between NFC devices using standard key agreement protocols, such as Diffie-Hellman (DH) key agreement protocol [1], [7]–[9], and apply symmetric key encryption. However, NFC is aiming at ultra low power and low cost in communication, so traditional key agreement protocols, such as Diffie-Hellman key agreement, are still considered costly in terms of computational overhead and energy consumption [10]–[13]. Moreover, to install strong cryptographic protocols for NFC involves upgrading and revoking largely deployed NFC devices, which are lack of encryption or weakly encrypted [14]–[16]. Since NFC devices and facilities have already been widely deployed and will be increasingly distributed, adding or upgrading cryptographic mechanisms on them tends to be costly and impractical.

Inspired by recent advance of friendly jamming, this paper explores physical layer security approach to provide confidentiality communication between an initiator and a passive target device by randomizing the initiator’s waveform without relying on cryptographic encryption. Note that in today’s NFC systems, the initiator transmits a constant carrier waveform \(c(t)\), and the target multiplies this waveform by its data \(x\) through load modulation, producing \(xc(t)\). The intuition is that we can change the initiator’s constant carrier waveform \(c(t)\) into random carrier waveform \(r(t)\). The eavesdropper does not know the randomized carrier waveform \(r(t)\), so it cannot extract data from what it overhears. In contrast, the initiator is the one who generates the random noise, and thus is able to decode the information by removing the noise effect. In this way, no modification to deployed target devices is required.

However, there are two challenges needing to be solved before existing physical layer security schemes such as friendly jamming [17] or RF Cloak [18] can be applied to an NFC system.

(Problem 1) There is a voltage jump in the middle of the analog waveform representation of a binary bit (a falling edge for ‘1’ and a rising edge for ‘0’) resulting from NFC’s Manchester coding along with synchronization offset. The eavesdropper can focus on this detail to decode the signal.

(Problem 2) In the data transmission of NFC, the initiator and the target’s coils are mutually coupled through common magnetic flux. This makes NFC different from other wireless communication in that NFC follows “multiplication” law rather than common superposition law. For friendly jamming, increasing the intensity of jamming signal decreases the SNR (signal to noise ratio) at the eavesdropper. Therefore it
is effective to simply send very strong jamming signal to “override” the original communication. But for NFC, increasing the intensity of randomized carrier waveform does not affect the SNR, which brings significant difficulty in achieving high security strength.

Aiming at a practical secure solution, this paper proposes SecNFC. To tackle the mentioned problems, we propose to not only randomize the amplitude of initiator’s carrier waveform but also perform a waveform design to change the standard NFC modulation to RZ (return to zero) coding by introducing power-off period at specific part of the signal. The new waveform representation covers both voltage jump in the middle of a bit and the voltage level difference between the first half bit and the second half bit, so as to avoid these information being used by the eavesdropper. For the initiator, the power-off period is a fraction of a bit duration. It can simply discard it, and the decoding will be unaffected.

We conduct simulations and experiments to demonstrate the effectiveness of SecNFC, which is simple, energy efficient, practical, and secure. The basic idea of SecNFC comes from our earlier work presented in conference [19], which has established basic mathematical model, solution to address (problem 1), simulations and concept-proof experiments to validate that the target can respond normally to randomized carrier waveform. Comparing with our earlier work, (a) this paper presents a detailed analysis to the two special problems brought by NFC’s data transmission mechanism. (b) this paper significantly enhances the solution, SecNFC by developing a practical solution to address both (problem 1) and (problem 2). (c) this paper discusses the other security threats besides eavesdropping threat.

Our main contributions are as follows:
- We investigate physical layer security approach to secure NFC and present a detailed analysis to the special problems brought by NFC’s data transmission mechanism.
- We apply a method, SecNFC, to secure inductively-coupled NFC from eavesdropping without relying on cryptographic encryption nor any change to the targets.
- We demonstrate the effectiveness and security of SecNFC by extensive simulations.
- We build a testbed based on USRP software defined radio and conduct proof-of-concept experiments to evaluate the effectiveness and security strength of SecNFC in a real-world environment.

II. RELATED WORK

In this section, we discuss the related work on symmetric key encryption methods, eavesdropper detection scheme and other physical layer security schemes, respectively.

A. Symmetric Key Encryption Methods

Some existing works suggest using symmetric key cryptography to secure the NFC to protect against eavesdroppers [1], [5]. It is mentioned that standard key agreement protocols like Diffie-Hellman based on RSA or Elliptic Curves may be used to establish symmetric keys between NFC devices. Many works [7], [8], [11] focus on key establishment protocols for NFC. However, these solutions involve upgrading and revoking non-encrypted and weak-encrypted NFC devices that are already deployed, which is costly and impractical. Moreover, standard key agreement protocols have extensive computational overhead and energy consumption. They are not preferable for resource constrained NFC devices.

B. Eavesdropper Detection Scheme

An eavesdropper detection method for inductive coupled communication is presented in [20]. Due to coupling, the presence of an eavesdropper detunes the transfer function between the legitimate users. This detuning can be detected to reveal the presence of the eavesdropper. This method is based on the assumption that the initiator and the target both know the main statistical parameters of the channel (transfer function and noise power) in the absence of the eavesdropper. However, in practical systems, due to the ad hoc communication between mobile devices, obtaining knowledge of the channel precisely in prior can be difficult. Moreover, there may be several unknown conducting objects proximate to the communication system, such as other nearby NFC equipments. Finally, the scheme targets on detecting eavesdropping not preventing it.

C. Other Physical Layer Security Schemes

Our work belongs to the class of physical layer security mechanisms with full duplex radios.

Some works propose to use “friendly jamming” to protect the plain text [17], [21]–[23]. For example, a technique called IMD (Implantable Medical Device) shield [17] was proposed, which exploits jamming to provide access control to an IMD. The IMD shield is a small radio device that employs two antennas for concurrent jamming and receiving. The receive antenna is physically connected to a transmit jam-and-receive chain, so that when sending a jamming signal, the jam chain can inject an antidotesignal to the receiving antenna to cancel the jamming signal.

Similar to our work, some other works propose to randomize the carrier waveform. Examples are Noisy Reader proposal [12] and RF-Cloak proposal [18] proposed for securing backscattered RFID communications. In Noisy Reader, two random values are used to replace the constant waveform in each transmitted bit to disturb the voltage level. In RF-Cloak, to further destroy the bit pattern in RFID, large number of random values are used in each transmitted bit. Other physical layer based security solutions to eavesdropping attacks, such as the noisy tag [13], require modifying the cards to use physical layer signals to exchange a key with the initiator.

As presented in introduction, none of the existing physical layer solutions has paid attention to and was able to tackle the unique challenges brought by NFC’s data transmission mechanism. We have studied friendly jamming and RF-Cloak schemes numerically. The results indicate that, in the case of friendly jamming the BER (bit error rate) at the eavesdropper is only about 2% on average for syn offset decoder and 40% on average for optimal decoder no matter how we increase the noise level; in the case of RF-Cloak the BER at the
eavesdropper is only about 8% on average for syn offset decoder and 40% on average for optimal decoder. These BERs are far from 50% (a random guess).

To the best of our knowledge, this is the first work to propose a practical physical layer based secure solution to confidential communication between NFC initiator and target devices without relying on cryptographic encryption nor modification on the target devices.

III. NFC PRELIMINARY

NFC is based on inductive coupling [24], [25], where loosely coupled inductive circuits share power and data over a distance of a few centimeters. Typical NFC happens between an active NFC device and a passive one. The former creates an RF field for data transmission, while the latter uses the RF field generated by the former, instead of creating its own RF field.

In communication, the active NFC device sends out a signal to the passive NFC device. If the devices are close enough to each other, the passive NFC device becomes powered by the active device’s signal. In this way, the active NFC device is also called initiator, and the passive NFC device is called target as shown in Fig. 1.

A. Difference Between Near Field and Far Field

NFC systems differ from other wireless communications in that most conventional wireless RF systems use an antenna to generate and transmit a propagated electromagnetic wave. In these types of systems all of the transmission energy is designed to radiate into free space. This type of transmission is referred to as “far-field.”

According to Maxwell’s equation for a radiating wire, the power density of far-field transmissions attenuates or rolls off at a rate proportional to the inverse of the range to the second power (1/r^2) or −20 dB per decade. This slow attenuation over distance allows far-field transmissions to communicate effectively over a long range.

NFC systems are designed to contain transmission energy within the localized magnetic field. This magnetic field energy resonates around the communication system, but does not radiate into free space. This type of transmission is referred to as “near-field”. The power density of near-field transmissions is extremely restrictive and attenuates or rolls off at a rate proportional to the inverse of the range to the sixth power (1/r^6) or −60 dB per decade.

B. Mathematical Model

To communicate, the initiator continuously transmits a high power RF signal c(t) = c0 cos(2πfΔt + θ), and the target modulates the signal with its data through a mechanism called load modulation. In particular, the target switches a load resistor off and on at its own antenna. The target’s action affects the transmitted signal at the initiator through inductive coupling. The output at the initiator y(t) (voltage between A and B in Fig. 1) is

\[ y(t)_{\text{load-off}} = G^{\text{off}} c(t) + w(t) \]
\[ y(t)_{\text{load-on}} = G^{\text{on}} c(t) + w(t) \]

where \( G^{\text{off}} \) and \( G^{\text{on}} \) represent the transfer functions of the impedance states of load off and on.\(^1\) \( w(t) \) denotes the wireless channel noise.

It is common practice to describe wireless systems in baseband, which is after removing the carrier frequency. Hence, in the rest of this paper, we focus on the baseband signals. For the simplicity of illustration, we also ignore channel noise in the following method description.

In current NFC systems, the baseband signal is a constant waveform \( c_0 \). We replace \( c(t) \) by \( c_0 \) in (1) to get the baseband representations under two impedance states:

\[ y(t)_{\text{load-off}} = G^{\text{off}} c_0 \]
\[ y(t)_{\text{load-on}} = G^{\text{on}} c_0 \]

When the load resistor is on, the target absorbs energy from the initiator’s magnetic field. This power consumption causes voltage drop at the antenna of the initiator, thus \( G^{\text{on}} < G^{\text{off}} \) and resulting \( y(t)_{\text{load-on}} < y(t)_{\text{load-off}} \). This high/low voltage relationship is used to modulate bits. Taking a widely used NFC system FeliCa [26] as an example, it uses 10% ASK and Manchester coding, high voltage level followed by a low voltage level represents a ‘1’, and vice versa as shown in Fig. 2 (a) blue lines. Because the target’s bits have equal probability of being ‘0’ or ‘1’, in the following deduction, we take an example that the target transmitting a bit ‘1’ to the initiator.

\[ Y^{\text{left}} = y(t)_{\text{load-off}} = G^{\text{off}} c_0 \]
\[ Y^{\text{right}} = y(t)_{\text{load-on}} = G^{\text{on}} c_0 \]

where \( Y^{\text{left}} \) denotes the first half bit and \( Y^{\text{right}} \) denotes the second half bit; and the decoding relies on comparing the voltage level between them.

\[ \text{bit} = 1 \text{ if } \Delta Y > 0 \]

where \( \Delta Y = Y^{\text{left}} - Y^{\text{right}} \).

\(^1\)The explicit expression of the transfer function is complicated, which relates to the capacitance, resistance, load impedance of the circuits of the initiator, the target, the eavesdropper, and other standby NFC enabled devices as well as the mutual impedances of each other among them. The derivation is in [20]. Nevertheless, transfer functions can be considered unchanged within the communication duration once the environmental configuration is prescribed.
JIN AND ZENG: SECURE INDUCTIVE-COUPLED NEAR FIELD COMMUNICATION AT PHYSICAL LAYER

C. Eavesdropping Model

The eavesdropper, who inserts its antenna into the system for eavesdropping [20], [27], observes the same voltage level relationship at its own antenna.

\[ Y_{\text{left}}^{e} = y_e(t)|_{\text{load:off}} = G_{\text{off}}^{e} c_0 \]
\[ Y_{\text{right}}^{e} = y_e(t)|_{\text{load:on}} = G_{\text{on}}^{e} c_0 \]

where \( y_e(t) \) is the output at the eavesdropper (voltage between E and F in Fig. 1). \( G_{\text{off}}^{e} \) and \( G_{\text{on}}^{e} \), \( Y_{\text{left}}^{e} \) and \( Y_{\text{right}}^{e} \) represent the corresponding transfer functions, the first and the second half bit with respect to the eavesdropper. It can decode modulated bits in the same way as the initiator does.

\[ \text{bit} = 1 \text{ if } \Delta Y_e > 0 \]

where \( \Delta Y_e = Y_{\text{left}}^{e} - Y_{\text{right}}^{e} \).

IV. SECNFC: PHYSICAL LAYER SECURITY ON NFC

This section introduces the basic idea of applying physical layer security approach on secure NFC, discusses the unique challenges brought by NFC’s data transmission mechanism and presents our solution.

A. System Setting and Security Model

In this paper, we consider a typical NFC scenario, where the initiator wants to read information from the target securely through inductive coupling. The target is assumed to be an ordinary off-the-shelf NFC tag or card. The initiator and the target do not have a shared secret key or any shared information in prior. For the convenience of method introduction, we make following system configuration assumptions.

1) Personal Tag: We assume that the target is a personal NFC tag, which is embedded in some personal owned material object (such as card, ticket or car key). In this case, illegitimate initiator is difficult to interrogate the target alone to obtain or reveal the same information as the legitimate initiator does.

2) Adversary Model: We aim at addressing eavesdropping only attacks against NFC. In this attack, an attacker listening on the wireless medium intercepts the RF signals between legitimate NFC devices. The adversary may seek to obtain confidential information contained in the NFC tag. In the simplest case, he can learn the ID of the card, threatening...
the privacy of the party carrying the card and opening doors for cloning attacks. Second, the adversary can obtain sensitive data transmitted by the card, such as biometric information and passwords. Further, the eavesdropper can intercept the cryptographic nonce transmitted by the card, and use it to reverse engineer the encryption and extract the secret key.

We assume a very powerful attacker possessing a high quality wireless channel in eavesdropping. It may be in any location with respect to the legitimate NFC devices. The attacker may use standard or custom-built hardware, and capture baseband and RF signals with high sensitivity and sampling rate. In this case, it can detect the slightest synchronization offset. The attacker also has powerful computational ability to store all the overheard signals and conduct sophisticated signal processing or data analysis.

3) What About Active Attacks?: Aside from passive eavesdropping, active scanning attacks [28], [29] are also frequently discussed in the RFID literature. In active attacks, an adversary repeatedly queries an RFID card in an attempt to infer the secret key from the responses or obtain confidential information.

We ignore active attacks in this paper because active attacks are relatively easier to address for personal tags: (1) they have a shorter range [1] since the attacker needs to power the tag. An active adversary needs to be within a few centimeters from the tag whereas a passive eavesdropper can be more than 4 meters away [30]. (2) active attacks are easier to be detected and stopped because they require the adversary to transmit its own signal [1].

4) Scope of Application: One example fitting in with our system configuration is the vehicle immobilizer [14], an anti-theft device which prevents the engine of the vehicle from starting unless the corresponding transponder is present. Such a transponder is a passive RFID tag which is embedded in the car key and wirelessly authenticates to the vehicle. It prevents a perpetrator from hot-wiring the vehicle or starting the car by forcing the mechanical lock. However, the cipher used in RFID-based anti-theft devices for modern cars has recently been broken in under 6 minutes based on eavesdropped information. Some other realistic applications include ID Cards, Access Management, Campus or Citizen cards, Micropayment (Mobile wallet, contactless payment, cashless payment), Event ticketing, Car or Bike rentals, etc.

It must be noted that just because we make a personal tag assumption doesn’t mean that our scheme, SecNFC is only suitable for such system configuration. On the contrary, SecNFC is fully capable of being applied to public tags. In such cases, we need not only to prevent information stolen by passive attackers, but also to counter unauthorized information access by active attackers. Thus, security consideration should include soundness of tag authentication, the ability to resist to adversaries aiming at identifying, tracing, or linking tags. These factors are not our focus in this paper, and were modeled [28], [29] and investigated by many research works with emphasis. In these scenarios, although SecNFC cannot prevent active attacks, SecNFC is still valuable of providing partial security against passive attacks.

We shall clarify that SecNFC is not aiming to replace cryptographic encryption. It can provide secure communication at physical layer when high layer data encryption is not available, however, it does not necessarily exclude encryption at higher layers. Even if there is data encryption at higher layers, security keys could be compromised or need to be updated frequently. In these scenarios, SecNFC is still very useful to secure the communication at physical layer to hide the real signals from the attacker or reduce key recovery risk.

5) Basic Design Principle: In the design of SecNFC, we only modify the initiator and keep the target unchanged. This is because target devices are normally embedded NFC tags and cards, which have already been widely deployed and planned to be increasingly distributed. Revoking and upgrading them are costly and impractical. While the initiator devices are normally well-resourced programmable intelligent devices, such as smartphones, e-ticketing reader. In this case, we can program SecNFC on the initiator device. When reading NFC tags, smartcards or exchange information with other NFC enabled smart devices, the NFC system can choose SecNFC instead of conventional NFC applications without making any change on both current initiator and target devices, making our solution a simple, effective and easy to implement security protection for NFC.

B. Basic Idea

As can be seen from equations (3) and (5) that the signal received by the initiator or the eavesdropper is equal to the carrier waveform multiplying the transfer function. The intuition is that we can change the initiator’s constant carrier waveform $c_0$ into random amplitude scaling carrier waveform $r(t)$ for each half bit to confuse the eavesdropper.

$$r(t) = a_1 \quad 0 < t < T/2$$
$$r(t) = a_2 \quad T/2 < t < T$$

where $T$ is the bit duration; $a_1$ and $a_2$ are random samples. In this case, (5) turns to

$$Y_{left} = G_{e}^{off} a_1$$
$$Y_{right} = G_{e}^{on} a_2$$

Fig. 2 (a) illustrates how this scheme works under ideal cases. There is a possibility that randomized carrier waveform changes the voltage level relationship. The first half bit becomes smaller than that of the second half bit: $\Delta Y_e < 0$ for bit = ‘1’. The eavesdropper does not know the randomized carrier waveform $r(t)$, and will decode a ‘1’ as a ‘0’ if it measures the voltage level of the overheard signals (as shown in Fig.2 (a) red lines).

In contrast, the initiator is the one who generates the random amplitude scaling carrier waveform $r(t)$, and thus is able to decode the bits by removing the noise effect.

C. Challenges

Note that contrary to traditional wireless communication that use far-field models of electromagnetic waves, inductive
c) Synchronization Offset in NFC: It must be pointed out that, although the target is mutually coupled with and absorbs the energy from the initiator, the target’s clock cannot be directly extracted from the incident sine carrier wave of the oscillator. Because in data transmission, there are intervals in which no power is transmitted from initiator and no carrier is received [31]. This would cause the clock signal from carrier to become intermittent. In common sense, logic block is preferred to be driven by a consecutive system clock. As a result, the target is designed to have its own internal clock generator block called clock recovery circuit [31]–[33].

It is well known that strict time synchronization between two distributed clocks is difficult in practice [34], [35]. There are residue synchronization offsets between them. A major factor causing synchronization offset is known as clock skew [36]. In communication, one device oscillates at a slightly different frequency than the other device, causing the clocks to tick at different rates. The phenomenon of clocks ticking at different rates, creating an ever widening gap in perceived time is known as clock drift. The difference between two clocks at any point in time is called clock skew and is due to both clock drift and the possibility that the clocks may have been set differently on different machines.

The frequency deviation of clock recovery circuit for NFC working at 13.56MHz has been studied in [31]–[33]. The frequency deviation is inevitable and may be different in different devices, and can be affected by environmental factors such as temperature and circuit aging.

b) Eavesdropper can make use of the synchronization offset to decode the signal: Normally, the level of synchronization offset will not affect the initiator’s bit decoding in NFC as long as it is significantly smaller than a bit duration [37], [38], whose effect is usually ignored. However, to secure NFC at physical layer, its effect must be considered.

Under the basic scheme, once there is a slight synchronization offset between the initiator and the target, the eavesdropper can exploit it to compromise the bits. To decode a bit, the eavesdropper focuses only on the voltage jump caused by the target’s action of turning load on or off in the middle of a bit. Fig. 2 (b) shows the randomized signal under non-perfect synchronization. It can be seen that, with the existence of synchronization offset, the eavesdropper can determine that a bit is ‘1’ if it observes a falling edge of voltage level transition in the middle of the bit. Similarly, it can distinguish that a bit is ‘0’ if it observes a rising edge.

c) Increasing randomness of the carrier cannot solve the problem: RF-Cloak [18] proposes to use more random values to hide the transmitted bit. This will make the transmitted waveform looks more irregular. However, this proposal cannot fundamentally solve the problem. Fig. 2 (c) illustrates the signal if the initiator simply increases the number of random values to hide the transmitted bit, where the frequency of random values introduced is set to 2MHz as used by RF-Cloak. It can be seen that despite the increase of randomness in waveform, the received signal still exhibits a rising or falling edge in the middle of a bit.

To destroy the voltage jump caused by the Manchester coding, the RF signal should be completely destroyed, i.e. the frequency of random values should be much higher than the carrier frequency (13.56MHz). But in this case, the initiator itself would become unable to decode.

2) Problem 2: Friendly Jamming Not Working for NFC: For traditional EM (electromagnetic) wave based wireless communication, the received signal at the eavesdropper follows superposition law. For example, in friendly jamming, the jamming signal from the receiver is independently added to the plain text from the transmitter at the receiving end of the eavesdropper as shown in Fig. 3. Increasing the intensity of jamming signal decreases the SNR at the eavesdropper. Therefore, it is
effective to simply send very strong jamming signal to override the original communication to achieve a high decoding BER at the eavesdropper.

However, it is not the case for NFC. In an NFC system, the initiator and the target are coupled together to form a circuitry link; the energy absorbed at the load of the target is proportional to the energy provided by the initiator’s carrier waveform as shown in Fig. 1. As can be seen in (8) that NFC follows “multiplication” law; in which case, the received signal at the eavesdropper is equal to the product of the signals from two communicating parties. Let’s assume that the eavesdropper still compares the voltage level difference to decode. The bit detection indicator of bit ‘1’ can be deduced from (8) as

\[ \Delta Y_e = G_{e \parallel} \alpha_1 - G_{e \parallel} \alpha_2 \]

We use \( f(x) \) to denote the power density function of \( \Delta Y_e \), \( \mu \) to denote the mean of the pre-set random distribution of the amplitude of the carrier waveform, the mean of \( f(x) \) can be derived from (9) as

\[ E[\Delta Y_e] = (G_{e \parallel} - G_{e \parallel}) \mu > 0 \]

We have

\[
BER = Pr(bit = 1)Pr(\Delta Y_e < 0|bit = 1) \\
+ Pr(bit = 0)Pr(\Delta Y_e > 1|bit = 0)
\]

\[ = Pr(\Delta Y_e < 0|bit = 1) = \int_{-\infty}^{0} f(x)dx \]

\[ < \int_{-\infty}^{(G_{e \parallel} - G_{e \parallel})\mu} f(x)dx = 50\% \]

where \( Pr(bit = 1), Pr(bit = 0) \) denote the probabilities of the occurrence of bit ‘1’ and bit ‘0’, and \( Pr(bit = 1) = Pr(bit = 0) = 1/2 \). It can be seen that no matter how we tune the random distribution, the BER can never reach 50%. Especially, increasing the intensity of randomized carrier waveform \( r(t) \) does not affect the shape of \( f(x) \) and results in the same BER.

In order for the readers to better understand this concept, we give an example: suppose that the initiator randomizes the amplitude of the carrier waveform \( r(t) \) to be uniformly distributed\(^4\) in \([0, \beta]\).\(^5\) Since there is no prior knowledge of \( r(t) \), the eavesdropper still attempts to decode the bit by the voltage level difference. The bit detection indicator \( \Delta Y_e \) (the sum of two uniform distributions) follows trapezoidal distribution [39]. As illustrated in Fig. 4, the BER at the eavesdropper equals to the shadowed area

\[ BER = \frac{G_{e \parallel} \beta}{2 G_{e \parallel} \beta} \approx 41\% \]

It can be seen from (12) that the BER depends only on the ratio between the transfer functions of the state impedances of load off and load on. According to ISO/IEC 18092 standard, this ratio is a constant, \( G_{e \parallel} / G_{e \parallel} = G_{e \parallel} / G_{e \parallel} \approx 0.82 \).

Thus, no matter how we increase the noise level \( \beta \), the security strength is unchangeable with the BER at the eavesdropper approximate to 41%, which is far from a perfect security system (A perfectly secure system should maintain a 50% bit error rate at the eavesdropper, equivalent to a random guess).

D. Solution

This subsection introduces SecNFC, a physical layer security solution specially designed for NFC.

1) Waveform Design: Introducing Power-Off Period: As pointed out in subsection IV-C, for problem 1, we need to hide the voltage jump caused by synchronization offset to ensure that the eavesdropper cannot decode. However, the initiator and the target are distributed devices; it is practically impossible for the initiator to simply compensate the time difference between their internal clocks. For problem 2, we need to make an eavesdropper obtain a high BER to achieve a high security strength. However, as can be seen from (12) that simply increasing the noise level is ineffective.

To tackle these two problems, SecNFC proposes to introduce \textit{power-off period} (equivalent as sending no signal) at specific area to cover the voltage jumps and the voltage level differences.\(^6\) The information produced by the target’s action of turning load on or off will be eliminated completely, including the voltage jump and the voltage level information. At the same time, we remain the other part of the carrier waveform so that the initiator itself will still be able to decode.

\( a) \) Where to introduce power-off period: (a) To hide the voltage jump, the power-off period is introduced around the transition time point when the target turns load on or off. As shown in Fig. 2(d), there will be no rising or falling edge observable for the eavesdropper, so that the eavesdropper has no clue to exploit the synchronization offset to decode.

\( b) \) To hide the voltage level difference, the power-off period is also introduced at the second half bit. Since the voltage level

\(^4\)Random amplitudes drawn different distributions, such as folded normal distribution, come up with very similar results.

\(^5\)In the case of \([\beta_0, \beta] \), \( \beta_0 \neq 0 \), eavesdropper gets a even lower BER.

\(^6\)As mentioned in subsection IV-C, the target has been adequately charged before communicating with the initiator. The target also has its own internal clock circuit. Therefore, the target would not went down with temporal power off.
difference now is always a positive value,
\[ \Delta Y_e = Y_{e}^{\text{left}} > 0 \]  
(13)
if the eavesdropper still decodes the bit by the voltage level difference, it will decode every bit as ‘1’ (as shown in Fig. 2(d)). In this case, the BER at the eavesdropper is 50% 
\[
BER = Pr(\text{bit} = 1)Pr(\Delta Y_e < 0|\text{bit} = 1)
+ Pr(\text{bit} = 0)Pr(\Delta Y_e > 1|\text{bit} = 0)
= \frac{1}{2} \times 1 + \frac{1}{2} \times 0 = 50\%
\]  
(14)
To conclude, SecNFC initiator sends random signal \( r(t) \) as follows. The initiator now generates only one random sample \( \alpha \) per bit. The samples are then to match the resolution of the digital-to-analog converter. For each bit, the initiator uses \( \alpha \) as the amplitude of the first half bit. It introduces power-off period at the second half bit with extended time length to cover the middle part of the bit. In this case, (7) turns to
\[
r(t) = \alpha \ \delta < t < T/2 - \delta \\
r(t) = 0 \ \text{otherwise}
\]  
(15)
where \( r(t) = 0 \) denotes the time period that SecNFC turns off the power. \( \delta \) denotes the extended time length of the power-off period.

b) Protect the secrecy of probability distribution: It is important to note that if an attacker could learn (through statistical methods most probably, by analyzing the stored interrogations of a specific information (e.g. an ID) between initiator and the target on many occasions) the probability density function (PDF) of the random distribution \( f_0(x) \) from which the random amplitude is drawn, he can make use of the knowledge to decode some of the bits.

Let’s take uniform distribution (whose boundaries are denoted by \( a \) and \( b \) as an example. If the bit is ‘1’, the load is off at the target side for the first half bit. The corresponding voltage level observed at the eavesdropper \( Y_{e}^{\text{left}} \) is in the range of \( [V_{\text{on}}^{\text{off}}, V_{\text{off}}^{\text{on}}] = [aG_{e}^{\text{off}}, bG_{e}^{\text{off}}] \). If the bit is ‘0’, the load is on at the target side for the first half bit. The corresponding voltage level observed at the eavesdropper \( Y_{e}^{\text{left}} \) is in the range of \( [V_{\text{on}}^{\text{on}}, V_{\text{off}}^{\text{high}}] = [aG_{e}^{\text{on}}, bG_{e}^{\text{on}}] \).

As shown in Fig. 5, since \( G_{e}^{\text{on}} < G_{e}^{\text{off}} \), we have \( V_{\text{on}}^{\text{off}} > V_{\text{on}}^{\text{on}} \) and \( V_{\text{off}}^{\text{high}} > V_{\text{off}}^{\text{on}} \). If the eavesdropper observes a voltage level \( Y_{e}^{\text{left}} \) in the range of \( [V_{\text{on}}^{\text{on}}, V_{\text{off}}^{\text{on}}] \), he can make sure that the load cannot be off, and thus decode the corresponding bit as ‘0’. Similarly, if the eavesdropper observes a voltage level \( Y_{e}^{\text{left}} \) in the range of \( [V_{\text{on}}^{\text{high}}, V_{\text{off}}^{\text{high}}] \), he can make sure that the load cannot be on, and thus decode the corresponding bit as ‘1’.

This promotes us to set up a protection scheme to prevent the eavesdropper from knowing the probability distribution \( f_0(x) \) when necessary. One suggested scheme could be “distribution hopping”. SecNFC randomly switches from one distribution to another every few bits by (1) changing the mean and variance of a distribution (for example, from \([0.5 \ 2]\) to \([4 \ 6]\), etc), (2) changing the type of distribution (for example, from uniform distribution to folded normal distribution, lognormal distribution, etc), (3) using compound distributions (for example, the sum of a uniform distribution and a folded normal distribution) to confuse the eavesdropper. Once the eavesdropper cannot accurately determine the probability distribution curve \( f_0(x) \), this attacking scheme can be well avoided.

c) Notices: It should be noted that the initiator does not know whether the random synchronization offsets put forward or backward the voltage jumps in prior; thus \( \delta \) has to be set longer than the estimated synchronization offset.

It should also be noted that if SecNFC misjudges the time-interval of state impedance of load off or load on, the protocol can be break down. Since ISO/IEC 18092 standard defines a range for this value, the specific modulation waveform may differ from device to device. Therefore, it is not appropriate to define specific beginning and ending time points of random signal and power-off period.

To solve this problem, an on-line rough synchronization is needed. We notice that although the modulation waveform may differ from device to device, the specific modulation waveform is relative stable within the same device and the same frame. Therefore, we can use the preamble (a preamble consisting of 48 zeros is defined by ISO/IEC 18092 standard for each transmitted frame) to make an estimation to the waveform and dynamically adjust the specific time points of sending random signal and introducing power-off period accordingly.

2) How Does the SecNFC Initiator Decode: The goal of the SecNFC initiator’s decoder is to retrieve the target’s bit stream \( x, [x(1), x(2), \ldots, x(n), \ldots] \) from the received signal \( y(t) \). Refer to equation (15), the initiator’s baseband signal exemplified by bit ‘1’ can be written as

\[
Y_{e}^{\text{left}} = G_{e}^{\text{off}} \alpha \\
Y_{e}^{\text{right}} = 0
\]  
(16)
Since the initiator is receiving at the same time while transmitting, it can hear its own transmission. This phenomenon is commonly referred to as self interference. The initiator first divides \( Y_{e}^{\text{left}} \) by \( a/c_{0} \) to cancel the noise effect to get the retrieved voltage level \( Y_{e}^{\text{left}} \) with constant carrier waveform \( c_{0} \) (as shown in Fig. 6 blue lines).

\[
Y_{e}^{\text{left}} = Y_{e}^{\text{left}}c_{0}/a
\]  
(17)
Note that SecNFC changes the standard NFC modulation to RZ (return to zero) coding. The initiator needs to decode the bit based only on the first half bit. We find this is possible.
As shown in Fig. 6, the initiator can use the bit representation in preamble as reference to make an estimation to the mid-level threshold \( Y_{\text{mid}} \).

\[
Y_{\text{mid}} = \frac{c_0(G_{\text{off}} + G_{\text{on}})}{2}
\]  

(18)

Instead of extracting the voltage level difference, the initiator compares the retrieved voltage level \( Y_{\text{left}} \) with mid-level threshold \( Y_{\text{mid}} \) to decode.

\[
\begin{align*}
\text{bit} &= 1 \quad \text{if} \quad Y_{\text{left}} > Y_{\text{mid}} \\
\text{bit} &= 0 \quad \text{if} \quad Y_{\text{left}} < Y_{\text{mid}}
\end{align*}
\]

(19)

**How about the BER at the initiator:** It must be pointed out that replacing the constant carrier waveform with SecNFC’s random carrier waveform decreases the channel capacity, because (1) introducing power-off period at the second half bit shorten the effective time duration of communication by half. (2) dividing a noisy received signal by \( r(t) \) can potentially increase the noise variance, due to the random structure of \( r(t) \). Readers may worry that SecNFC’s modulation would present a high BER at the initiator.

Notice that NFC is different from traditional wireless communication in original intention. Traditional far field wireless communication aims at massive data transmission. It is designed to make full use of the channel capacity to achieve a high bit rate. The modulation methods are often multi-bits-per-symbol, such as QPSK. Since there is little redundancy, the decrease of channel capacity could leads to a rapid increase of decoding BER.

Things are different for NFC. On one hand, the two communicating parties are close to each other to have high quality wireless channel. On the other hand, NFC is specially designed for contactless payment (electronic ticket, smartcards and mobile payment), social networking (sharing contacts, photos, videos or files), and bootstrapping other connections (NFC offers a low-speed connection with simple setup that can be used to bootstrap more capable wireless connections). These applications have very small data transmission requirements. Thus, NFC is designed to sacrifice data transmission ability to achieve what is more important in the concept of design: low power consumption. Many works have reported that current bit rate of NFC is much smaller than the channel capacity [40]–[43] with the potential of using multi-bits-per-symbol modulation schemes. Therefore, with optimization to the initiator’s transmitting and receiving circuit, the decoding BER would not be affected, as long as the degraded channel capacity is still larger than the bit rate.

V. DISCUSSIONS

This section discusses other security threats.

A. SecNFC Is Immune to MIMO Eavesdropper

The major limitation of physical layer security approach in other EM wave based wireless communication is that a MIMO eavesdropper can separate the transmitted signals from two communicating parties to break the security scheme [22]. For example, in friendly jamming, a simple way for MIMO eavesdropper to compromise the conversation is to use beam-forming techniques to separate two signals: plain text from the transmitter and self-generated noise from the receiver and extract only the former one as shown in Fig. 3.

In NFC, the nature of interaction between devices changes fundamentally. It must be noticed that between the two communicating NFC devices, the initiator is the only one actively transmitting RF signal, while the target is a passive device. To communicate, the target is loosely coupled to the communicating NFC devices, the initiator is the only one fundamentally. It must be noticed that between the two communicating NFC devices, the initiator is the only one actively transmitting RF signal, while the target is a passive device. To communicate, the target is loosely coupled to the initiator as shown in Fig. 1. In this way, the target becomes “part of the initiator’s circuit” in an NFC system, similar to a transformer circuit, where the initiator is “primary coil” part and the target is “secondary coil” part. Since there is only one signal produced by a combined circuit of both the initiator and the target, MIMO technique is not useful in this case to separate the target’s signal from the initiator’s signal.

B. SecNFC Is Immune to Far-Field Jamming

The change of the nature of interaction between NFC devices also changes the way an NFC system being interfered. Since NFC devices do not receive electromagnetic waves, an active attacker has to couple with the initiator in the same way that the initiator couples with the target. That is by generating a changing magnetic field in the air and passing it through the coil of the initiator as shown in Fig. 7.

The energy of wireless interference in the initiator is drawn from the primary coil of the attacker. As introduced in Section III-A, the power density of near-field transmissions is non-propagating and extremely restrictive. An active attacker would have to be standing next to the initiator, by enclosing the initiator inside the attacker’s magnetic “bubble”, to interfere with the wireless transmissions between...
the initiator and the target. This makes the NFC immune to active interference from a distance.\(^9\)

C. SecNFC Can Detect Close-Range Active Attacks

It has been summarized in a well cited survey [1] that possible close-range active attacks are data corruption, data modification and data insertion, and they are detectable due to the NFC’s full-duplex ability.

For data corruption and data modification, NFC devices can counter these attacks because they can check the RF field, while they are transmitting data. If an NFC device does this, it will be able to detect the attack. The power which is needed to corrupt the data is significantly bigger than the power which can be detected by the NFC device. Thus, every such attack should be detectable.

For data insertion, there are two possible countermeasures. One is that the answering device answers with no delay. In this case the attacker cannot be faster than the legitimate device. The attacker can be as fast as the legitimate device, but if two devices answer at the same time no correct data is received. The second possible countermeasure is listening by the answering device to the channel during the time, it is open and the staring point of the transmission. The device could then detect an attacker, who wants to insert data.

Finally, due to the interference range limitation, once an active attack is detected, the users can simply change the position of NFC devices (typically mobile phones) maintaining a distance from the interference source.

D. Eavesdropping is Practical Security Threat to NFC

On one hand, NFC has inherent advantages of being immune to MIMO eavesdropper and detectability of active attack. On the other hand, existing works [1], [5], [18], [44], [45] have identified that passive attack is major threat to NFC.

Intuitively, NFC should be inherently secure because of the short communication range and the properties of the RF modulation. However, the authors in [44] showed that it is always possible to eavesdrop NFC at some range, partially determined by the antenna signal gain. The RF signal from the initiator has to be strong enough to induce sufficient voltage to power up the target. The eavesdropping equipment may not have the same constraints. It may have a better antenna designed for best possible gain, and it does not need to be integrated in a mobile phone or tag. It may also have power supply, filters, signal amplifiers and other circuitry optimizing the receiving capabilities. Generally, NFC’s operating range is within 4cm, while eavesdropping range is up to 10m.

For example, it seems possible to make a device able to eavesdrop and store information transmitted between a contactless card and an automatic teller machine (ATM), similar to how magnetic strip card skimmers are working today. Although VISA and MasterCard may provide a well designed security solution protecting their application, NFC may still be a weakness. Attackers can use other NFC applications with low or no security as backdoors in order to launch attacks against the Visa or MasterCard applications. This motivates the need for some kind of NFC security protocol.

Based on above reasons, we believe that our solution, SecNFC, addresses a real world problem that threatens the security of NFC systems.

E. SecNFC can Detect Active Eavesdropping Attacks

Recent advance on RFID security [46] has identified a new type of attack, which is called active eavesdropping attack. Unlike the conventional eavesdropping attack where the adversary merely intercepts the signals transmitted between the two communicating parties, the active eavesdropper is able to broadcast its own signal, and because of the special properties of load modulation used in RFID systems, the active eavesdroppers received signal is a sum of the response to both its own signal and the legitimate initiator’s signal. Therefore, its decoding ability can be improved, leading to more harmful and easier attacks on the existing RFID systems.

This attacking scheme also presents practical threat against physical layer security schemes who randomized carrier wave form \(r(t)\). As modeled by [46], let’s consider an adversarial initiator who is able to transmit its own continuous wave signal \(c(t)\) outside the frequency band of the legitimate initiator. Due to the fact that under load modulation, the tag cannot distinguish different frequencies and simply sets the impedance in its circuitry to either low or high to reflect a bit of 1 or 0. In this case, the adversarial initiator’s received signal is a weighted sum of the response to both its own signal and the legitimate initiator’s signal.

\[
y_r(t) = r(t)x + c(t)x
\]  

(20)

Since \(c(t)\) and \(r(t)\) are transmitted over different band, a simple way to attack physical layer security schemes is to filter out \(r(t)x\) to obtain only \(c(t)x\) (by assuming the power of \(c(t)\) is sufficiently large), and uses normal way to decode.

For active eavesdropping attack, our solution SecNFC can make good use of the power-off period to detect the attack. Legitimate initiator can continuously monitor the RF signal at the second half bit over the whole data transmission band. Once he detects a suspicious signal, (due to the distance advantage, the adversarial initiator requires to generate a
relative strong signal in order for itself to decode. Thus, it is no need to worry that the suspicious signal might be too weak to be detectable) the legitimate initiator detects the attack and can stop the data transmission immediately.

VI. NUMERICAL RESULTS

In this section, we conduct numerical simulations to evaluate our method. We take Felica as a simulation example. It uses Manchester coding at 212 kbit/s. We set the inevitable synchronization offset to at most 10% of a bit duration. In order to destroy the trace of synchronization offset, we set the extended time length of the power-off period $\delta$ to 15% of a bit duration for SecNFC.

We set the eavesdropper’s sampling rate to 100Mbits/s. It down converts RF signal by a frequency mixer and uses a low pass filter to get the baseband signal. We set the eavesdropper’s SNR to 20dB.

To decode bit information from the baseband signal, the eavesdropper may use one of the following strategies.

1) Optimal decoder. It uses a maximum likelihood decoder (called optimal decoder derived in [18]). Optimal decoder synthetically considers all sample points within a bit duration to decode. It determines whether the bit is a ‘1’ or ‘0’ by observing the voltage level relationship between the first half and the second one. A high-low voltage is decoded as a ‘1’, and a low-high voltage is decoded as a ‘0’.

2) Syn offset decoder. It exploits synchronization offset to decode as introduced in Section IV-C (called Syn offset decoder). Syn offset decoder pays attention to a few sample points around the middle of a bit, and ignores all irrelevant sample points. It determines whether the bit is a ‘1’ or ‘0’ by observing voltage level transition. A falling edge is decoded as a ‘1’, and a rising edge is decoded as a ‘0’.

We use the bit error rate (BER) experienced by the eavesdropper as our security metric. A perfectly secure system should maintain a 50% bit error rate at the eavesdropper, equivalent to a random guess. In the simulation, we generate a 10,000-bit random message as the target’s reply to the initiator. The cumulative distribution function (CDF) curve is obtained based on 1000 random runs.

A. Evaluation of Basic Modulation Scheme

We first test the basic scheme of using random carrier waveform to confuse the eavesdropper as introduced in section IV-B. In this case, during the target’s reply, the initiator continuously transmits a random amplitude scaling carrier waveform for each half bit ($a_1$ for the first half bit, $a_2$ for the second half bit). The random samples are set to follow uniform distribution with mean value equals to $c_0$ ($r(t) \in [0, 2c_0]$).

Fig. 8 (a) plots the CDF of the eavesdropper’s BERs. For syn offset decoder, the BER at the eavesdropper is only about 2% on average, which indicates that the basic scheme is completely compromised. In this case, the eavesdropper intercepts nearly all of the information from the target. For optimal decoder, the BER at the eavesdropper is about 40% on average, which indicates that the basic scheme is not very secure. In this case, the eavesdropper can intercept portion of the information from the target.

The results demonstrate that applying the basic idea of randomizing the amplitude of carrier waveform on NFC does not work. There are weaknesses can be exploited by both syn offset decoder and optimal decoder.

B. Evaluation of RF-Cloak Proposal

Then, we test RF-Cloak proposal of using large number of random values to disturb the carrier waveform. In this case, the initiator increases the number of random values from 1 to 4 for each half bit. We keep the other simulation parameters unchanged.

1) Security Strength: Fig. 8 (b) plots the CDF of the eavesdropper’s BER. It can be seen that for syn offset decoder, the increase of BER is very limited. The BER at the eavesdropper still remains at a very low level of only about 8% on average. For optimal decoder, the BER at the eavesdropper is almost unchanged.

The results demonstrate that increasing the number of random values does little to improve the security. The BERs are still far from 50%.

2) Complexity: Using large number of random values also increases the complexity of the signal processing at the initiator. As a result, RF-Cloak is more costly than SecNFC in terms of memory and energy.

RF-Cloak needs to generate 2M random values for 1 second; that is 16M bit data assuming 8 bits a value. The random values must be stored in memory for the initiator’s decoding. According to Nyquist theorem, the sampling rate of the initiator’s receiver should be at least 4MHz, that is another 32M bit receiving data. Totally, the temporary memory cost for the application should be at least 48M bits. Similarly, we can estimate that SecNFC requires only 10M bit memory for the same application.

Moreover, sampling rate is approximately proportional to the energy consumption [47] in digital processing devices. Since RF-Cloak requires much higher sampling rate (4MHz) than SecNFC (848kHz), the energy cost of RF-Cloak is about five times that of SecNFC.

C. Evaluation of Friendly Jamming Proposal

Then, we investigate whether friendly jamming proposal of increasing the intensity of randomized carrier waveform can affect the security strength. We vary the mean value of the random amplitude scaling from $C_0$ to 10 $C_0$.

Fig. 8 (c) shows the average eavesdropper’s BER as a function of noise level. For each point, we take the average of 1000 runs. It can be seen that the BERs at the eavesdropper are almost unchanged for both syn offset decoder and optimal decoder.

10We simply use a very fast sampling rate with an affordable calculation complexity. Note that our tested eavesdropper’s sampling rate is more than double the carrier frequency (13.56MHz). According to Nyquist theorem, the eavesdropper would gain no more information with faster sampling rate.

11We simply choose one random value among the four for each half bit, and use the same way as previous to decode.
This result conforms with the conclusion in section IV-C that simply increasing the intensity of randomized carrier waveform equally increases the voltage level difference, and thus will not make any difference to the eavesdropper.

D. Evaluation of SecNFC’s Modulation Scheme

Next, we evaluate the effectiveness of our solution, SecNFC’s modulation scheme, against eavesdropping. In this case, during the target’s reply, the initiator continuously transmits random amplitude scaling noise as well as power-off period, which has been introduced in section IV-D.

Fig. 9 (a) plots the CDF of the eavesdropper’s BERs of SecNFC. For optimal decoder, the eavesdropper’s BER is about 50% on average; and the minimum BER is 46%. For syn offset decoder, the eavesdropper’s BER is about 50% on average; and the minimum BER is 45%. Both results are very close to random guesses. Thus, it can be concluded that SecNFC is secure against both optimal decoder and syn offset decoder.

E. Impact of Extended Time Length of Power-Off Period on BER

We then vary the extended time length of power-off period $\delta$ from 0% to 15% to test the performance.

Fig. 9 (b) shows the average BER as a function of $\delta$. For each point, we take the average of 1000 simulations.

It can be seen from the figure that when $\delta < 10\%$, the time length is not long enough to cover up the synchronization offset (at most 10%), resulting a low BER using syn offset decoder. For $\delta > 10\%$, SecNFC works well. The eavesdropper will get an average 50% BER for both optimal decoder and syn offset decoder. This result conforms with the discussion in section IV-D that $\delta$ has to be set longer than the estimated synchronization offset.

F. SecNFC Initiator’s BER

In this subsection, we evaluate how SecNFC affects the decoding at the legitimate initiator. We use the method introduced in section IV-D.2 to decode the bits. We set SNR at the initiator to 30dB. In this simulation, we generate a 100,000-bit random message as the target’s reply to the initiator in each run. We conduct 1000 random runs.

Fig. 9(c) plots the CDF of the BERs at the initiator. The initiator has an average decoding BER of about 0.02% and a maximum decoding BER of 0.03%. An average BER of 0.03% is quite common and considered negligible in NFC systems. For reference, the figure also shows the BER using a constant waveform. It can be seen from the figure that there is only a small BER increment by using SecNFC’s modulation instead of constant waveform. That is, replacing the constant waveform with SecNFC’s modulation does not bring significant impact on the initiator’s decoding.

G. Robustness of SecNFC Against Low-Power Interference

By far, we have focused our attention on passive attack. In this subsection, we test our protocol against low-power interference that could come from either intended adversaries or unintended sources like microwaves.
Fig. 10 plots the BER at the initiator with respect to different strength of external interference. The result shows that SecNFC is robust. The BER is negligible (less than 0.5%) when the jamming signal level is less than -7dB. For reference, the figure also shows the BER using a constant waveform. It can be seen from the figure that there is only a small BER increment (less than 2% BER increment for arbitrary SNR point) by using SecNFC’s modulation instead of constant waveform. That is, replacing the constant waveform with SecNFC’s modulation does not bring significant impact on the robustness of the initiator’s decoding.

As pointed out in section V that high-power interferences are detectable due to the NFC’s full-duplex ability. Once an interference is detected, the users can simply change the position of NFC devices (typically mobile phones) maintaining a distance from the interference source.

VII. EXPERIMENTS

We conduct experiments to prove the concept of SecNFC. We use off-the-shelf Felica NFC tags as the target. We use software defined radios, USRP N210, as the initiator. Another USRP is used to simulate the eavesdropper. We use BasicTX and BasicRX Daughter board operating in the 1-250 MHz frequency range to send and receive RF signals at 13.56MHz. We use an amplifier (mini circuit ZKL-2R5) to boost the output power of USRP. The sample rate is set to 20MHz. The antennas are the DLPRFID-ANT antennas. The equipments used in the experiment are shown in Fig. 11. We put the initiator and the target close to each other. We then put the eavesdropper’s antenna close to the target (about 10cm away), so it can hear clearly on the communication.

A. Effectiveness of SecNFC

In this experiment, we are aiming at validating the concept of SecNFC. For comparison, we test 3 following cases: (1) standard NFC system, (2) basic scheme as introduced in Section IV-B, (3) SecNFC scheme as introduced in Section IV-D. For case (2) and (3), we set the amplitude of the carrier waveform $r(t)$ to be uniformly distributed between $[0, 0.5]$.

Fig. 12 plots the snapshots of the received signal at the eavesdropper for the 3 cases:

1. Fig. 12(a) shows the standard NFC system, where the initiator transmits constant carrier waveform.
2. Fig. 12(b) shows the basic scheme, where the initiator transmits random amplitude scaling carrier waveform.
3. Fig. 12(c) shows the SecNFC scheme, where the initiator not only randomize the amplitude but also introduce power-off period.

If this value is set too small, the signal energy of some bits might be too weak for the initiator itself to decode. As a result, the BER at the initiator would be high. Our experimental experience show that 0.5 is appropriate.
...scenario for the eavesdropper, i.e. a random guess guarantees BER to be always smaller than 50%, which indicates the worst-case scenario for the eavesdropper, i.e. a random guess.

This can simply flip the decoding (changes all '0' to '1' and all '1' to '0'). This subtracting it by 100% whenever it exceeds 50% because that the eavesdropper

An illustration of the truncated signal, bit sequence $[110100]$ can be decoded by comparing the voltage level between the first half bit and the second half bit.

Fig. 12(b) shows the basic scheme, where the initiator transmits random amplitude scaling carrier waveform. It can be seen from the figure that for the same truncated signal, random amplitude noise opportunistically changes the voltage level relationships of the 1st, 4th and 5th bits (as shown in blue numbers) to opposites. The eavesdropper would make mistakes if it still decodes the signal by measuring the voltage levels of the overheard signals. However, this scheme has weakness when there exists a synchronization offset between the initiator and the target. A smart eavesdropper can still determine that the bit is actually ‘0’(‘1’), if it observes a rising edge (falling edge) in the middle of the bit. It can also be seen from the figure that the eavesdropper corrects all of the mistaken bits (as shown in red numbers) in this case.

Fig. 12(c) shows SecNFC scheme, where the initiator not only randomize the amplitude but also perform a waveform design to change the standard NFC modulation to RZ coding by introducing power-off period at specific part of the signal. It can be seen from the figure that the new waveform representation covers both voltage jump in the middle of a bit and the voltage level difference between the first half bit and the second half bit, so as to avoid these information being used by the eavesdropper. For the same truncated signal, the eavesdropper can no longer recognize the waveforms and would mistake all ‘0’ to ‘1’.

**B. Robustness of SecNFC**

In this experiment, we statistically test the security of SecNFC on 6 different Felica tags (labelled from A to F) in a real-world configuration. The initiator interrogates the target while the eavesdropper listens and stores the overheard signal in a computer and infers the bit sequence by both optimal decoder and syn offset decoder off-line. For each interrogation, we count the eavesdropper’s BER on 1000-bits. We perform the interrogations 10 times and calculate the average BER.

Table 1 shows the result. It can be seen that our proposed scheme, SecNFC, randomizes the original waveform and causes high BER at the eavesdropper for all 6 tags. The BERs are from 45% to 54% with the average of 49.7% for optimal decoder. The BERs are from 44% to 56% with the average of 49.3% for synchronization offset decoder. The average BERs are very close to 50%.

For reference, we also test the basic scheme and record the BER in Table 1. The BERs are from 34% to 43% with the average of 37.8% for optimal decoder. This conforms with the discussion in Section IV-C.2 that the basic scheme offers imperfect security, residue information can be extracted by comparing the voltage level difference, our proposed method increases the BER by 11.9% on average in this case. For synchronization offset, the BERs are from 5% to 13% with the average of 9.3%; our proposed method increases the BER by 40% on average in this case. The results validate that SecNFC solves the unique challenges in NFC as pointed out in Section IV-C, and results in enhanced security strength than the basic scheme for all of the tested cases.

To further test the decoding performance at the initiator, we use the method introduced in Section IV-D.2 to cancel the noise effect and retrieve the target’s bit stream. It can be seen in Table 1 that the initiator’s BERs are less than 0.2% with an average of 0.1%. The result validates that SecNFC is robust and would not cause the problem of high BER at legitimate initiator.

**VIII. Conclusion**

In order to secure NFC from eavesdropping attack without revoking or changing the deployed NFC devices, this paper explores physical layer security approach to provide confidential communication between an initiator and a passive target device by randomizing the initiator’s waveform without relying on cryptographic encryption. A detailed analysis is performed to reveal two unique challenges brought by NFC’s data transmission mechanism (1) There is a voltage jump in the middle of the analog waveform representation of a binary bit resulting from NFC’s Manchester coding along with synchronization offset. The eavesdropper can focus on this detail to compromise the bit. (2) NFC follows “multiplication” law rather than common superposition law. This unique transmitting-receiving relationship brings significant difficulty in achieving high security strength.

A practical solution, SecNFC, through a special waveform design is proposed. SecNFC uses a novel idea of introducing power-off period in part of the bit duration to cover the voltage jumps and the voltage level differences. For the initiator, it can simply discard the power-off portion and uses the remaining part to decode.

We conducted extensive simulations to evaluate the effectiveness of SecNFC. The results show that the eavesdropper’s BER is about 50% on average (equal to a random guess) for either of the attacking methods of exploiting synchronization offset or comparing voltage level difference; at the same time, the initiator itself has a very low decoding BER of about 0.02% on average. We also conduct concept-proof experiments to validate our solution. The results have indicated that the average BERs are very close to 50%.

SecNFC is simple, energy efficient, practical, and secure.

**Future Work:** Our physical layer solution, SecNFC is promising to be further extended to RFID systems that also
uses load modulation in data transmission. However, MIMO eavesdropper presents a practical threat to an RFID system currently due to its far-field radiation characteristic. To tackle the threat from MIMO techniques will be our future work.

REFERENCES


Rong Jin received the B.E., M.E., and Ph.D. degrees in electronic and information engineering from the Huazhong University of Science and Technology (HUST), China, in 2006, 2008, and 2012, respectively. He was a Post-Doctoral Scholar with the Department of Computer and Information Science, University of Michigan-Dearborn, from 2012 to 2014. He is currently a Lecturer with the School of Electronics Information and Communications, HUST. His research interests include microwave remote sensing, antenna array, electromagnetics, and physical layer wireless network security.

Kai Zeng received the Ph.D. degree in electrical and computer engineering from the Worcester Polytechnic Institute in 2008. He was a Post-Doctoral Scholar with the Department of Computer Science, University of California at Davis, Davis, from 2008 to 2011. He was with the Department of Computer Science, University of Michigan-Dearborn, from 2011 to 2014, as an Assistant Professor. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, also with the Department of Computer Science, and also with the Center for Secure Information Systems, George Mason University. His current research interests are in cyber-physical system security and privacy, physical layer security, network forensics, and cognitive radio networks. He was a recipient of the U.S. National Science Foundation Faculty Early Career Development award in 2012. He was also a recipient of the Excellence in Postdoctoral Research Award, UCD, in 2011, and Sigma Xi Outstanding Ph.D. Dissertation Award, WPI, in 2008. He is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.