Securing Emerging Short Range Wireless Communications: The State of the Art

KUI Ren, QIAN Wang, DI Ma, AND XIAOHUA JIA

Abstract

As an emerging advanced short-range communication technology, near field communication (NFC) is undergoing a fast rate of expansion with many promising benefits including low power, small size, and peer-to-peer communication, without incurring complex network configuration overhead. However, current NFC technologies suffer from one practical limitation: almost all NFC-enabled applications require built-in NFC chipsets, and as a result such low levels of penetration of NFC hardware has stymied its applications on most mobile devices in the market, for example, smartphone and tablet platforms. In addition, from the security perspective the confidentiality of the transmitted data has not been satisfactorily addressed by current NFC technologies, which do not incorporate any security at the physical or MAC layers by assuming that the extremely short range of communication itself has offered a degree of protection physically.

Therefore, great interest has been aroused in the practicality and security enhancement of NFC technologies. In this article we discuss alternative NFC technologies, with an emphasis on barcode-based NFC and acoustics-based NFC, which are compatible with legacy devices and existing infrastructure and can provide a high level of security guarantee. Following a brief overview of barcode-based and acoustics-based short-range communications respectively, for each technology we present the major technical hurdles to be overcome and the state-of-the-art, and finally offer a vision of the future research issues on these two promising technologies.

Introduction

Near-Field Communication (NFC) is an emerging wireless technology designed for low-power communication between devices within close proximity (e.g. a few centimeters) [1]. The close communication range, as a result of fast decaying magnetic induction between the antennas of NFC transmitter and receiver, is a distinctive trait of NFC and brings several key advantages. First, due to the physical collocation of the transmitter/receiver, NFC does not require cumbersome network configuration and can be used as out-of-band channels for secure device pairing without resorting to a Public Key Infrastructure (PKI) or trusted third parties. Second, it offers a natural, physical protection against various attacks, particularly malicious eavesdropping. Due to these silent features, NFC is expected to revolutionize a range of mobile applications, from contactless payment and ticketing access control, to peripheral pairing for smart devices. It is estimated that the NFC market will grow to 34 billion by 2016.

However, the widespread use of NFC is hindered by the fact that only a limited number of smartphone/tablet platforms have built-in NFC chipsets. Moreover, in order to support NFC on the existing industrial infrastructure like POS terminals, it typically requires costly hardware and software upgrades, due to the need for additional NFC chipsets and radio stack. As of 2012, it is estimated that only three to five percent of smartphones worldwide and 12 percent of smartphones in the U.S. have NFC support. For instance, the popular iPhone has no NFC support. Moreover, while NFC does not incorporate any security at the physical or MAC layers by assuming that the extremely short range of communication in itself has offered a degree of physical protection, several recent findings have brought the security of NFC into question. Account details of Google Wallet could easily be hacked into and changed. In [2] the eavesdropping distance of NFC is empirically measured to be 30 cm using an oscilloscope. Recent experimental studies shows that, with a specially designed portable NFC sniffer, it is possible to eavesdrop NFC transmissions from up to 240 cm away, which is at least an order of magnitude further than the intended NFC communication distance. These results have seriously challenged the general perception that NFC is immune to eavesdropping. Recently, the NFC forum proposed that NFCIP-1 and NFC-SEC-01 specifications adopt the Diffie-Hellman key exchange protocol to enhance data confidentiality. However, most existing NFC applications are designed for short-duration rapid data exchange, and the lengthy key exchange process might dominate the entire NFC communication session, compromising the user experience.

Recently, great interest has been aroused in the practicality and security enhancement of
As a potential alternative to radio frequency communication, visible light communication has recently received significant attention. It has several advantages over RF technology such as security against eavesdropping and not generating RF interference. NFC technologies. To this end, researchers are highly motivated to design secure NFC for off-the-shelf devices. This article discusses new alternative NFC technologies, with an emphasis on barcode-based NFC and acoustics-based NFC, which are compatible with legacy devices (non-NFC smartphones or even feature phones) and existing infrastructure (e.g. POS terminals) while providing a high level of security guarantee. The key idea of resulting designs is to leverage visible light channel and acoustic channel to realize NFC systems with fine performance and security assurance. For each technology, we will first give a brief overview of its applications in short-range communications. Then we discuss the major technical hurdles in the design of such NFC-like systems and the most recent advances, which achieve compatibility with legacy devices, NFC-comparable throughput, better security guarantees, and great usability and robustness. Finally, we offer a vision of future research issues along the direction of designing more dependable and secure NFC systems.

**SYSTEM MODEL AND ASSUMPTIONS**

In the short-range communication system, we assume that the sender and the receiver are both off-the-shelf smartphones, which are assumed to have no priori knowledge of any secret information before the communication. Like today’s devices, an off-the-shelf smartphone has a built-in speaker and microphone pair and is equipped with a color screen and a front-facing camera. The barcode-based NFC system works on top of a duplex visible light communication (VLC) channel using the color screen and the front-facing camera as the sender and the receiver to ‘talk’ to each other simultaneously. The data to be transmitted are encoded as a stream of images and displayed on the sender’s screen while the receiver uses the camera to record and decode the stream. Note that the barcode-based communication system is designed to work on different mobile platforms without specific requirement on the screen size and camera resolution, but a better specification usually leads to higher communication throughput. Like the barcode-based NFC, to eliminate the need for any specialized NFC hardware, the acoustics-based NFC system uses the microphones and speakers on mobile phones as the senders and the receivers, respectively. We model the channel between the smartphones as a Line-of-Sight (LOS) channel, and it is approximated by the frequency-selective fading function.

In both systems, we mainly consider a passive attacker whose objective is to obtain the exchanged data information during the short-range transmissions. In the barcode-based NFC system, the communication privacy and security depends on the characterization of the screen geometric model or, for example, the control of the direction and distance of the screen-camera link. In the acoustics-based NFC system, multiple-sensor eavesdroppers may try to separate the data signal from its recorded mixture signals. The eavesdroppers are allowed to place their sensors (microphones) at any fixed locations in priori to the acoustic NFC communication.

**ROBUST AND DEPENDABLE BARCODE-BASED NFC FOR SMARTPHONES**

As a potential alternative to radio frequency (RF) communication, visible light communication (VLC) has recently received significant attention. It has several advantages over RF technology such as security against eavesdropping and not generating RF interference. Most existing VLC approaches use LEDs for digital communication [3]. Recently, PixNet [4] is employing the LCD-camera pair to build wireless links. Based on OFDM and advanced computer vision techniques, high throughput over a long distance can be achieved by these methods. However, they are mainly designed for large LCD monitors and high-speed cameras, and thus are not suitable for smartphone platforms [5]. Due to the popularity of smartphones and tablets, numerous applications have been developed to scan/read barcodes using cameras equipped on smart devices. However, due to the limited capacity of a single barcode, its applications are limited to storing a very small piece of information such as a website address, short personal information, coupons, and so on. Moreover, the decoding algorithms of existing barcodes requires expensive operations such as corner detection and image transformation, especially for high density barcodes. Finally, from a security perspective, barcodes are susceptible to eavesdropping attacks due to their visual nature. The fundamental design principles of 2D barcodes also make it difficult to establish a secure communication channel due to the one-way barcode exchange.

**DESIGN CHALLENGES FOR BARCODE-BASED NFC**

Due to the high directionality of narrow light beams, VLC can potentially enable secure and interference-free wireless links, and serve as a good alternative to implement the functionality of NFC. In barcode-based NFC, information can be encoded as a stream of images and played on smartphone/computer screens while the receiver uses a camera to record and then decodes the video stream.

However, the major challenges in building a barcode-based NFC system are caused by the poor image quality and the constrained computation power of smartphones. First, smartphones have a small screen size and low resolution compared to large LCD monitors. Consequently, neighboring pixels displaying different colors often blur on the borderline. Secondly, the relative movement between devices introduces more blur effect in the captured images, making it hard to obtain high decoding rates. Moreover, the capture rate of camera on smartphones requires the system to capture and process a barcode image within around 30 ms [5]. This requirement imposes another design challenge on most smartphone platforms in the market. Finally, due to the inherent directionality, the visible light communication (VLC)
channel of barcode exchanges yields interesting security properties. The security of barcode-based NFC needs to be analyzed using carefully designed security models.

**The State-of-the-Art on Barcode-Based NFC**

To achieve barcode streaming for smartphone systems, in 2012 Hao et al. [5] designed COBRA, the first practical VLC system with high throughput communication in dynamic environments. In the system, the sender encodes data into color barcodes and displays on the screen at certain frequency. The authors developed a new color barcode design that can significantly accelerate the decoding process. On the sender end, the use of color barcode, which includes three types of area, i.e., corner trackers, timing reference blocks, and code area, can achieve high capacity and fast decoding speed.

Based on the color barcode design, COBRA utilizes adaptive configuration and blur-aware color ordering to mitigate the blur effect. Observing that smaller block size causes more blur in the captured image, the sender adaptively changes the block size based on the current level of mobility. In addition, since blur usually occurs along the border of blocks of different colors, the sender optimizes the order of color blocks in a barcode to minimize the total border length of different colors. On the receiver end, corner trackers utilizes a unique pattern placed in each corner of the smart border to accelerate corner detection. Finally, special blocks surrounding the code area are added and used as timing references (TR) to locate each block in the code area faster and more accurately.

While COBRA enables high-throughput ad hoc communications over smartphones, it is designed based on highly customized barcodes that have not been widely adopted in practice. In addition, COBRA achieves only one-way communication, which limits its scope of application. Finally, from the perspective of security, the system needs to be formally analyzed under carefully-defined models, taking into account unique characteristics of VLC. To address these concerns, recently Zhang et al. [6] proposed SBVLC, another barcode-based NFC system that achieves two-way communication and uses the widely-used QR codes, due to its high information density per code and low sensitivity to varying lighting conditions and angles. In the system, the sender divides the data string into several data chunks, whose size depends on the maximum storage capacity of a single barcode and the rate of the employed error correcting codes (ECC). By adding sequence numbers in the headers, data chunks are formatted to packages, which are encoded by ECC to frame blocks processed to generate barcodes. The receiver starts the decoding process as soon as the first barcode frame is captured by its front-facing camera. Fig. 1 shows the flowchart of 2D barcode streaming.

By realizing duplex two-way communication using front-facing cameras as transmitters, SBVLC aims to provide real time communication for practical use of barcode-based NFC. To this end, the authors carefully select the optimal system parameters: determine the proper ECC level by statistical test of QR version 1-20, choose the frame refresh rate cap as half of the camera capture rate by channel robustness test, and determine the ideal frame refresh rate by screen refresh rate and camera capture rate test. Because multiple camera frame images may be generated for the same QR code, an efficient QR filter is constructed to remove duplicated QR frame images. Similarly to COBRA, a color screen is utilized to improve the barcode capacity, letting the sender display the QR codes in blue and red alternating order such that any two consecutive QR codes are in different colors.

Based on SBVLC, the authors proposed an all-or-nothing streaming protocol using secret sharing, and analyzed the security using screen geometric models. In Fig. 2, by the property of all-or-nothing, the eavesdropper has to “see” both screens in order to recover the message. Assuming the distance between two smartphones is around 10 cm, an eavesdropper must be in the shadowed area to simultaneously “see” both phone screens. This shadowed area is bounded as a minimum ball \( B(O, d_{safe}) \), where the origin \( O \) denotes the middle of two phones and \( d_{safe} = (4/\tan(\epsilon)) \) cm. With the widest smartphone visible angle \( \epsilon = 2^\circ \), the safe distance for data confidentiality \( d_{save} = 114 \) cm. And obviously, any adversary within the ball can be easily detected. The security of the basic scheme can be further enhanced by combining it with proactive rotation mechanisms.
Geometric security model of barcode-based NFC.

**Figure 2.** Geometric security model of barcode-based NFC.

**Future Research Issues**

The ultimate goal of barcode-based NFC is to provide dependable and secure high-throughput short-range communications for power-constrained smartphones. To achieve this goal, there is still much room for improving the state-of-the-art from the performance and security aspects.

**Full-Duplex Two-Way Communication** — A full-duplex communication system allows communication to occur in both directions simultaneously between smartphones, so it is desirable to extend barcode-based NFC to support full-duplex barcode-based communication. The first design challenge is the following: when screens and cameras of two devices are facing each other, a refreshing screen may cause reflection from the other screen, causing significant noise to the front-facing camera. To address this problem, novel noise canceling techniques should be investigated to mitigate the blur introduced by the effect of reflections. Another design challenge is the following: when full-duplex communication is realized, the barcode area and the scan window both have to occupy parts of the full screen, making barcode detection and extraction more difficult. This motivates future researchers to design a new suite of color barcodes, blur-aware color ordering and enhancement, corner detection, and barcode extraction techniques.

**2D Barcode Authentication** — Due to the lack of authenticity checking in existing 2D barcodes, barcode-based communication is vulnerable to various attacks, including buffer overflow, SQL injections, phishing, social network attacks, and so on. It is necessary to analyze the security threats of malicious 2D barcodes by evaluating the existing popular smartphone-based QR code scanning applications. Based on the analytical and experimental results, authenticated 2D barcodes may be designed by embedding specially-designed authentication information (e.g., digital signature) into the barcodes to protect the message integrity and verify the authenticity of the issuer of 2D barcodes. The carrying of a large amount of authentication information, which is much larger than the current data capacity of 2D barcodes, also motivates researchers to design novel barcode design with high capacity.

**Analysis Under More Practical Security Model** — Different from existing radio technologies, the direction and distance of a screen-camera link of barcode-based data streaming can be easily controlled. Motivated by this observation, it is necessary to develop a more sound and practical security model for barcode-based communication, taking into account camera resolutions, screen view angles, screen brightness, and user-induced motions. Based on the 2D/3D geometric model and single/multi-receiver adversarial models, a systematic security study of the barcode-based mobile communication system is also required. Moreover, the characterization of various conditions under which the established communication channel is secure against sophisticated eavesdropping attacks can be another research direction.

**Dependable and Secure Acoustics-Based NFC**

**A Brief View of Acoustics-Based Short-Range Communications**

As a unique wireless technology for short-range and long-range communication, acoustic communication has received continuous and extensive attention in recent years. As such, it has been widely used in many underwater wireless communication systems. For short-range communications, most existing works utilized on-off keying modulation techniques, achieving hundreds of bits/s at short distances of less than a few tens of centimeters. In terms of the software acoustic modem, in 2001 Lopes and Aguiar [7] presented an aerial acoustic communication system using a software modem. Mostafa [8] released a software modem called minimodem that supports many traditional modem protocols, e.g., Bell 103 on Linux OS. Michel [9] implemented a software modem for Android systems supporting ASK modulation, and it can modulate data in musical tones. Houmansadr et al. [10] realized a software modem supporting QAM modulation, and they used it to build IP over VoIP to achieve communication unobservability against traffic analysis and standard censorship techniques. Acoustic modems are also used in ubiquitous computing and navigation systems [11]. However, the existing literature does not investigate the use of acoustic signals for securing NFC running on legacy devices.

**Design Challenges for Acoustics-Based NFC**

Compared to barcode-based NFC, the transmission of an acoustic signal does not require line-of-sight, which offers much higher usability than the barcode-based communication. In addition, unlike conventional NFC technologies that require specialized NFC chips, the acoustics-based NFC only requires a speaker and a microphone being equipped in all smartphones. However, the major challenges in building an...
The first acoustics-based NFC system, called Dhwani, enables NFC-like functionality over smartphones, and was proposed by Rajalakshmi et al. [12] in 2013. Dhwani is a software-based solution that requires only a speaker and a microphone compatible with legacy devices currently. The main components of Dhwani include an ingress filter, an OFDM-based software module, and a self-jamming module. The ingress filter is used to attenuate “bad” frequencies in the acoustic band and annul the effects of ambient noise. The reason for using OFDM radio is to combat high frequency selectivity and at the same time increase the data transmission rate. To achieve data confidentiality, Dhwani utilizes a self-jamming technique to intentionally generate signal interference [13], defeating an eavesdropper by jamming signals from the sender. At the receiver end, efficient self-interference cancellation is conducted while making cancellation extremely difficult for eavesdroppers. Based on the assumption that the channel between the sender and the eavesdropper is more noisy (caused by jamming signals) than the channel between the sender and the receiver, the eavesdropper cannot recover the message by error-correcting codes. Recently, Tippenhauer et al. [14] investigated the limitations of friendly jamming and showed its potential security weakness for confidentiality. Thus, from a practical perspective the security of acoustics-based NFC systems needs to be carefully examined.

As a parallel and independent work, another acoustics-based NFC system called PriWhisper was proposed in [15]. Different from Dhwani, which focuses on more implementation aspects, the authors aim to provide rigorous security of acoustics-based NFC systems. Correspondingly, other security enhanced schemes or practical countermeasures may need to be designed to improve the system security.

**Future Research Issues**

The practical use of acoustics-based NFC systems relies on the throughput performance and the security strength provided by the self-jamming technique. Further work needs to be done in the following areas.

**Performance Enhancement** — For performance enhancement design, it has been observed that the data rate of the acoustics-based NFC system is also closely related to the modulation and error-correcting coding methods. To further improve the system performance and dependability, it is possible to explore advanced error correction codes (e.g. LT code, Online code, Reed Solomon code, etc.), higher modulation schemes (e.g. QAM), and frequency selectivity-resilient physical layer radio techniques (e.g. OFDM) for achieving higher data-rate transmission. On top of this, a systematic study of the SNR, the multipath effect, the effects of signal bandwidth, and modulation methods is necessary to evaluate the security of the acoustics-based NFC system. Correspondingly, other security enhanced schemes or practical countermeasures may need to be designed to improve the system security.

![Figure 3. Data signal recovery.](imageURL)
There is still much room for researchers to improve the practicality of NFC systems in terms of data rate, security strength, and so on. We believe that NFC will soon be pervasive in our daily life after some technical hurdles are successfully overcome.

Security Evaluations under Strong Threat Models — The security of a friendly jamming/self-jamming scheme relies on the assumption that it is hard for the attacker to extract the original message from the mixture of the jamming signal and the signal carrying the confidential message. The existing literature on self-jamming only focuses on weak threat models where the attacker has limited capabilities in terms of the number or directionality of receiving antennas. As a future research direction, it is important and necessary to investigate the effectiveness of self-jamming in the NFC systems in terms of data rate, security strength, and so on. We believe that NFC will soon be pervasive in our daily life after some technical hurdles are successfully overcome.

Non-Invasive Design for Acoustics-Based Communication — The carrier frequency of the smart device hardware usually has a wider range than the human voice band. For example, smartphone hardware usually lies in the audible spectrum between 20 ~ 20000 Hz while the voice frequency (VF) or voice band is only within part of the audio range, approximately from 300 Hz to 3400 Hz. While the signals transmitted over the human voice band can be heard or noticed by surrounding people, signal transmissions over 20 ~ 300 Hz and 3400 ~ 20000 Hz are hard to detect and can be considered as “hidden” transmission. Motivated by this observation, it is possible to have a non-invasive design of NFC systems using the non-voice frequency band, achieving even higher security guarantee. To this end, new and novel mechanisms need to be designed for jamming signal generation/cancellation and robust and secure signal transmission. Since channel gains on higher frequencies are lower and transmissions on lower frequencies are subject to ambient noise, other advanced signal processing and fading-resilient physical layer techniques may be utilized to mitigate and eliminate the effects of noise and fading. Compared to the acoustic signal transmission over voice band, the non-invasive designs are more prone to jamming signals, which are also hard to detect on the same non-voice band. Thus, to defend against active adversaries, the use of smartphone sound localization techniques may help automatically detect the distance of the incoming acoustic signal source and reject unintended signals.

Discussions and Comparisons

Different from the existing NFC-enabled applications that operate at high frequency and require additional hardware, the use of barcodes and acoustic signals for NFC can provide a purely software-based solution and enable NFC applications on the off-the-shelf smart devices. To achieve secure NFC, the barcode-based NFC system depends on secure visual communication, while the audio-based NFC system relies on the secure transmission of acoustic signals. In the barcode-based NFC system, based on the analysis of the geometric screen model, we can see that the direction and distance of the screen-camera link can be controlled to enhance the communication privacy and security. However, different from the barcode-based NFC, the audio-based NFC system utilizes the friendly jamming technique, which exploits the physical layer properties of the acoustic communication to provide strong security guarantee at the physical layer. For both systems, successful defense against eavesdropping vastly depends on careful analysis of the attack scenarios and adopting suitable protection mechanisms based on the analysis. As pointed out in the future research directions, it still requires researchers to establish much more stronger attack models and evaluate the system security comprehensively.

Concluding Remarks

NFC is expected to revolutionize a range of mobile applications and must overcome many technical hurdles for wide acceptance by the legacy smart devices. In this article we presented two alternative NFC technologies, barcode-based NFC and acoustics-based NFC, which provide NFC-like functionalities and enable much stronger security guarantees but require less strict hardware support. However, as we point out in the above discussions, there is still much room for researchers to improve the practicality of NFC systems in terms of data rate, security strength, and so on. We believe that NFC will soon be pervasive in our daily life after some technical hurdles are successfully overcome.

Acknowledgment

K. Ren’s research is supported in part by the U.S. National Science Foundation under grants CNS-1262275, CNS-1318948, and CNS-1421903.

Q. Wang’s research is supported in part by the National Natural Science Foundation of China (Grant No. 61373167) and the Natural Science Foundation of Hubei Province (Grant No. 2013CFB297). D. Ma’s research is partially supported by the NSF grant DGE-1419280. X. Jia’s research is supported in part by the Research Grants Council of Hong Kong with Project No. CityU 114713.

References


KUI REN is an associate professor of computer science at the State University of New York at Buffalo. He received his Ph.D. degree from Worcester Polytechnic Institute and both BE and ME degrees from Zhejiang University. Kui’s research interests include cloud security, wireless security, and smartphone-enabled crowdsourcing systems. His research has been supported by NSF, DoE, AFRL, MSR, and Amazon. He is a recipient of an NSF CAREER Award in 2011 and a Sigma Xi Research Excellence Award in 2012. He has published 135 peer review papers. He is broadly interested in the general area of security, privacy, and applied cryptography. He is currently a professor with the School of Computer Science, Wuhan University. His research interests include wireless network security and privacy, cloud computing security, and applied cryptography. Kui is a senior member of the Internet Privacy Task Force, State of Illinois.

QIAN WANG received a B.S. degree from Wuhan University, China, in 2003, the M.S. degree from the Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, China, in 2006, and the Ph.D. degree from the Illinois Institute of Technology, USA, in 2012, all in electrical engineering. He is currently a professor with the School of Computer Science, Wuhan University. His research interests include wireless network security and privacy, cloud computing security, and applied cryptography. Qian is an expert under the “1000 Young Talents Program” of China. He is a co-recipient of the Best Paper Award at IEEE ICNP 2011. He is a member of the IEEE and a member of the ACM.

Di Ma is an assistant professor in the Computer and Information Science Department at the University of Michigan-Dearborn, where she leads the Security and Forensics Research Lab (SAFE). She is broadly interested in the general area of security, privacy, and applied cryptography. Her research spans a wide range of topics, including smartphone and mobile device security, RFID and sensor security, vehicular network and vehicle security, computation over authenticated/encrypted data, fine-grained access control, secure storage systems, and so on. Her research is supported by NSF, AFOSR, Intel, and Research in Motion. She received the Ph.D. degree from the University of California, Irvine, in 2009. She was with the IBM Almaden Research Center in 2008 and the Institute for Infocomm Research, Singapore, in 2000-2005. She won the Tan Kah Kee Young Inventor Award in 2004. She is a member of the IEEE.

XIAOJIA JIA received his BSc (1984) and MEng (1987) from the University of Science and Technology of China, and the DSc (1991) in information science from the University of Tokyo. He is currently chair professor with the Dept. of Computer Science at City University of Hong Kong. His research interests include cloud computing and distributed systems, computer networks, and mobile computing. Prof. Jia is an editor of IEEE Internet of Things, Transactions on Parallel and Distributed Systems (2006-2009), Wireless Networks, the Journal of World Wide Web, the Journal of Combinatorial Optimization, etc. He was the general chair of ACM MobiHoc 2008, TPC co-chair of IEEE GlobeCom 2010 – Ad Hoc and Sensor Networking Symp, area-chair of IEEE INFOCOM 2010 and 2015, and local co-chair of ACM SIGCOMM 2013. He is Fellow of IEEE.