IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 2, Ver. VIII (Mar - Apr. 2014), PP 06-10
www.iosrjournals.org

Peer-to-Peer Acoustic Near Field Communication

Shreya Kumar, Uma Mounika K., Kavya Kumar
Electronics and Telecommunication
SIES Graduate School of Technology,
Navi Mumbai, Maharashtra, India.

Abstract: *With instant user gratification aspect in mind, and elimination of cumbersome communication channel establishment procedure, NFC concept evolved. An ultra-modern effort,an acoustics based P2P NFC system developed by Microsoft India evolved from the shortcomings of conventional NFC. This paper reviews the advantages of P2P NFC for active tags over established NFC. P2P's ubiquitous characteristics and implementation even on passive tags are projected as being the future of Wireless Communication.*

Keywords: *P2P NFC (Peer to Peer Near Field Communication), PSR (Packet Success Rate), BER (Bit Error Rate), ASDR (Acoustic Software Defined Radio), OFDM (Orthogonal Frequency Division Multiplexing), JamSecure, SIC (Self Interference Cancellation).*

I. Introduction

Near-Field Communication (NFC) enables low data rate, bidirectional communication between devices within close proximity, usually within a few centimetres, in a P2P manner. The key advantage of NFC is that it eliminates the need for cumbersome network configuration efforts required to set up a communication channel using alternatives such as Bluetooth or Wi-Fi. This is due to its inherent property of association by physical proximity [5].

Several NFC-based applications have been proposed or demonstrated, e.g., contact-less payment, access control, social networking, ticketing, museum services, automatically initiate and set up a high data rate communication channel such as Wi-Fi or Bluetooth,etc.. However, the adoption of these applications has been stymied by the low levels of penetration of NFC hardware, estimated to be just 3-5% among mobile phones worldwide and only about 12% even in an advanced market such as the U.S., as of 2008. Even as far out as 2020, the penetration is expected to be fewer than 40%. Correspondingly, the prevalence of NFC-enabled point-of-sale (POS) terminals is also low — under 5% today and expected to rise to only about 39% globally by 2025.[1] Even disregarding the optimism that usually colours such forecasts, it seems likely that the majority of phones andPOS terminals globally will not be NFC-enabled even 6-7 years from now. Thus, the opportunities for using NFC applications such as P2P transfers or contact-less payment will remain rather limited. [2]

Can we enable NFC-like functionality on today's devices? We answer this question in the affirmative by presenting P2P Acoustic NFC [10], a novel, acoustics-based system that uses the existing microphones and speakers on phones to enable NFC, thus, eliminating the need for specialized NFC hardware. As in conventional NFC, where communication through magnetic coupling is confined to a short range, acoustic communication in P2P Acoustic NFC is confined to a short range (few cm) as shown in Fig(1). Thus, similar to conventional NFC, P2P Acoustic NFC enables the "association by proximity" functionality needed for applications such as P2P transfers and contact-less payments. A key advantage of P2P Acoustic NFC over conventional NFC is that it is a purely software-based solution that can run on legacy phones, including feature phones, so long as they have a speaker and a micro- phone. Consequently, much of the installed base of phones today could use P2P Acoustic NFC to perform P2P NFC communication. That said, the use of acoustic communication means that, unlike conventional NFC, P2P Acoustic NFC is not amenable to implementation in passive tags. A second significant advantage of P2P Acoustic NFC over conventional NFC is in terms of information-theoretic, physical-layer security. The security model in P2P Acoustic NFC is that the devices seeking to communicate are trusted and immune to tampering. Conventional NFC does not incorporate any security at the physical or MAC layers since the short range of communication (about 10 cm) is in it presumed to offer a degree of protection.

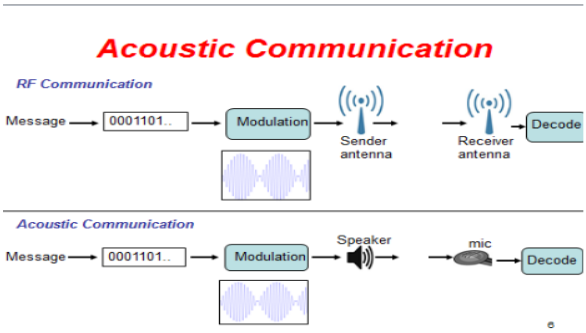

Figure 1. Compares RF communication system and Acoustic communication system

P2P Acoustic NFC provides security at the physical layer using a novel self- jamming technique, JamSecure, whereinthe receiver intentionally jams the signal it is trying to receive, thereby stymieing eaves-droppers,but then usesself-interferencecancellation to successfully decode the incoming message. The security thus obtained is information-theoretic, i.e., P2P Acoustic NFC inherently prevents the leakage of information to an eavesdropper. This is in contrast to cryptographic security, which is based on assumptions about computational hardness. Even if cryptographic security protocols[4] are employed at the higher layers, P2P Acoustic NFC enables key exchange without the need for any shared secret or certificates to be set up a priori. This is a significant advantage, since creating a public key infrastructure (PKI) spanning billions of devices would be challenging. In order to enable P2P Acoustic NFC we implemented an Acoustic Software Defined Radio (ASDR) on the mobile devices that uses speakers and microphones to receive and transmit data.

II. Assumptions

• Both transacting devices (transmitter and receiver) are trusted entities. These devices are assumed to function correctly and execute the P2P protocol faithfully. Any failure is presumed to be only accidental (e.g., due to a power outage).
• The attacker is presumed to be capable of mounting both passive (e.g., eavesdropping) and active attacks (e.g., message insertion). However, we assume that the attacker is unable to directly tamper with the trusted entities or alter their functioning.
• The communication range of the transacting devices is limited to a few centimetres. [7]

III. Components

a. *Acoustic Software Defined Radio and Design:*

P2P provides an Acoustic Software Defined Radio (ASDR) service, which is used to transmit or receive packets. P2P's ASDR implements almost all of the functionality of a standard modern day radio, including OFDM modulation and demodulation, error correction coding, etc. However, a key difference in P2P's ASDR compared to traditional RF radios is that it has no notion of a carrier frequency and a separate baseband. The reason is that the ADC is able to sample at a rate (44 KHz) that is sufficient for the entire acoustic bandwidth supported by the speaker and microphone. A sampling rate of 44 KHz allows operating (at best) in the 0-22 KHz band. Consequently, P2P implements a carrier-less OFDM over the entire 0-22KHz band, simply suppressing (i.e., nulling) sub-carriers that are not suitable for use, either because of the ambient noise or because of the speaker and microphone characteristics.

P2P implements an OFDM-based software defined radio[3] for enabling communication between devices. The choice of OFDM 1 In current day NFC systems based on magnetic induction, such interference is not a serious problem since magnetism decays much faster than acoustic signals. Our OFDM radio allows the choice of various sub-carrier modulation schemes such as BPSK, QPSK, 16QAM, etc., and includes basic error correction coding mechanisms.

b. *Jam Secure:*

JamSecure is a novel self-jamming technique used by the receiver in P2P to cloak the message being transmitted by the transmitter, thereby preventing an attacker from receiving the message [10].

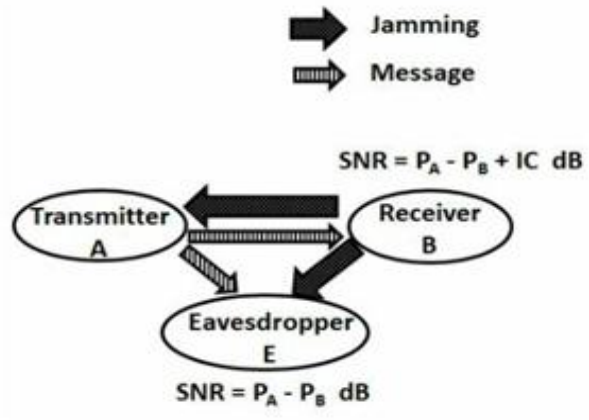

Figure 2 . Depicts the key idea behind JamSecure.

Transmitter A wishes to transmit a message M to receiver B while aneavesdropper E attempts to listen to message M as shown in Fig(2). As A transmits its message with a power PA dBm, simultaneously, B jams A's transmission by Transmitting a Pseudorandom Noise (PN) sequence with power PB dBm. The PN sequence is generated afresh for each secure reception and is known only to B. The eavesdropper E can only overhear the combination of the message M from A and the jamming noise from B. The received Signal to Noise Ratio (SNR) at E will thus be,

SNR=(PA−PB) dB (1)

If PB is high enough, then information-theoretically, E will not be able to extract any useful information about M. While B also receives a combination of its own jamming and the message M, it performs Self Interference Cancellation (SIC), i.e., subtracts the (known) jamming signal from the received signal, in an attempt to retrieve M. Since SIC is not perfect in practice, suppose that B can cancel IC dB of its own signal. Then, the SNR seen by B is,

SNR= (PA − PB + IC) dB (2)

If IC is "high enough", B will be able to retrieve the message M from A. While SIC is conceptually simple, the characteristics of the acoustic hardware and channel make it challenging to directly perform channel estimation for SIC. Instead, we employ a hybrid offline-cum-online approach, which works with a predetermined library of PN sequences, and random combinations thereof.

How much jamming is needed? For each physical-layer modulation technique, the SNR at the receiver imposes a theoretical lower bound on the Bit-Error-Rate (BER), and hence an upper bound on the Packet Success Rate

(PSR) for error-free reception.

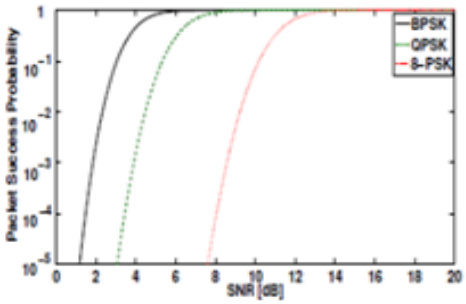

Figure 3.depicts the best possible PSR that can be achieved for a 256-bit packet, as a function of SNR, for BPSK, QPSK, and 8-PSK.

The key observation is that in each case, PSR falls very sharply around a certain SNR threshold; e.g., with QPSK, just a 4dB drop in SNR (from 6dB to 2dB) causes PSR to fall by 5 orders of magnitude. In P2P we need to ensure that the receiver injects enough noise that the SNR at the eavesdropper is to the left of the chosen curve inFig (3) while, at the same time, the SNR at the receiver itself, with the benefit of SIC, is to the right.

c. ***SIC (Self-Interference Cancellation):***

In P2P, a receiver defeats an eaves- dropper by jamming the transmissions from the sender. It then uses Self-Interference Cancellation (SIC) to decode the transmission despite jamming. Consequently, there are two key goals in the design of jamming and SIC in P2P:

- Security: The jamming should be random and powerful enough that an eavesdropper is unable to cancel out the jamming and retrieve the message.
- Effective SIC Cancellation: At the same time, SIC must be good enough for the receiver to decode the message.

d. ***Scrambler-Descrambler:***

P2P uses scrambling prior to encoding and modulation, to amplify the impact of bit errors, thereby rendering the received (scrambled) message unreadable and preventing any information leakage. While a special-purpose scrambler could be designed, we simply re-purpose the widely-available and highly-efficient Advanced Encryption Standard (AES) scheme. Whereas AES is typically used for encryption, with a private key that is kept secret, we use it with a well-known key, since our objective is to achieve the desired error propagation, not secrecy. The block-size in AES equals the key length — 128, 192, or 256 bits — which allows the possibility of sending a short NFC message (with padding) as a separately encrypted block or longer messages as multiple blocks. When the receiver, with the benefit of SIC, retrieves an error-free copy of the scrambled message, it is able to unscramble it with the well-known key. However, an eavesdropper, who typically suffers several bits of error, will be unable to decode the message, even knowing the key.

IV. Working

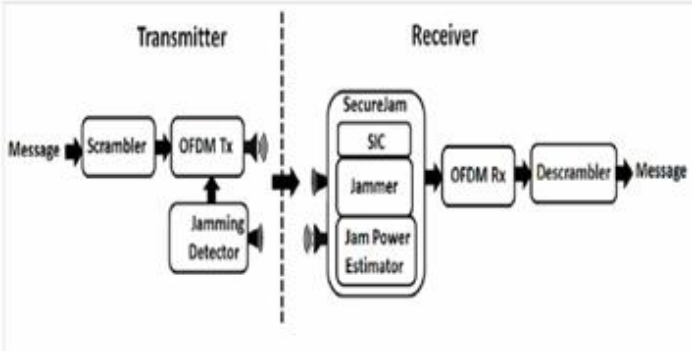

Figure 4. Represents the overall system of P2P.

a. ***Transmitter Overview:***

At the transmitter, the message is first scrambled to ensure that bit errors result in the entire message being corrupted at the receiver as shown in Fig(4). This is important in order to ensure that the eavesdropper cannot benefit from extracting parts of the message that are error free. The OFDM radio then transmits the scrambled message over the air using the speaker. The jamming detector continuously monitors the ambient jamming level to ensure that there is "enough" jamming to prevent any eavesdropper from receiving the message. Upon detecting a drop in jamming levels below a "safe" threshold, it simply directs the OFDM transmitter to abort the transmission mid-way.

b. ***Receiver Overview:***

The received signal first passes through the JamSecure module as shown in Fig (4). The JamSecure module transmits the jamming signal over the speakers, while simultaneously performing SIC on the received signal. An additional function that the JamSecure module performs is to estimate the appropriate jamming power needed to simultaneously ensure that an eavesdropper cannot decode the message; the receiver, with the benefit of SIC, can decode the message and a concurrent transaction at a distance of 1.5m or greater is not interfered with. This requirement just imposes an upper bound on the jamming power; this then leaves the task of balancing the former requirements. The estimation of jamming power for these purposes is performed with the help of the transmitter, as described. The OFDM receiver then decodes the message, after which the descrambler retrieves the original message. Successful reception of a packet is indicated by a 24-bit CRC check.

V. Security Analysis

a. ***Information-Theoretic Security in P2P:***

P2P's approach falls primarily under the purview of Wyner's wiretap model [9], since the channel to the eaves- dropper is noisier than that of the intended receiver due to jamming coupled with self-interference-cancellation. Consequently, the transmitter can use an error correcting mechanism (e.g., error correcting codes) that is sufficient for correcting errors in the less noisy channel, ChAB, but not so for the noisier channel, ChAE, for the eavesdropper as shown in Fig(2). Further, since the jamming sequence is generated pseudo-randomly for each transaction and never reused, it can be viewed as a random string for one-time-pad encryption 4. However, unlike Shannon's OTP [8], P2P does not apply the OTP encryption at the transmitter itself and may be vulnerable to certain attacks such as those based on shielding and directional antennas, which undermine the Wyner wiretap assumption.

b. ***Security Attacks on P2P*:**

P2P seeks to defend against both passive and active attacks on a pair of proximate, communicating nodes, which are assumed to be trustworthy. In this section, we discuss various security attacks on P2P [10].Assuming that node A intends to transmit a message M securely to B, while E is a malicious node.

- *Man-in-the-middle and replay attacks:* When A transmits M to B, a co-located eavesdropper E can receive it and try to transmit a Modified (or unmodified) version to someone else, pretending to be A. However, since E has no way of receiving any meaningful data, given the jamming from B, these attacks will remain ineffective.
- ***DOS attacks:*** A co-located device E could transmit its own jamming signal, to disallow meaningful communication between A and B. While E may succeed in disrupting communication between A and B, there will be no loss of security since E cannot recover the data transmitted by A.
- *Stopping Attacks:* This attack arises because of P2P's reliance on the receiver, B, to jam A's transmission [6]. If B were somehow disabled, then E could receive M in the clear. In fact, as it disables B, E can start emitting its own jamming signal, to keep A in the dark about B's disablement. However, a deliberate attack by E to disable B is not within scope. However, if B were to fail accidentally (e.g., lose power), A would detect that the jamming has ceased and stop transmitting immediately.

VI. Conclusion

In this paper, we have presented P2P, a software-only acoustic NFC system that is accessible to the large base of existing mobile devices. The design of P2P is informed by our characterization of acoustic hardware and environment, and includes several novel elements. Chief among these is the receiver-based, self-jamming technique called JamSecure, which provides information- theoretic, physical-layer security. We inferred that P2P is suitable for secure NFC communication.

Acknowledgement

We would like to thank our Principal, Dr.Alka Mahajan, our HOD, Dr.Atul Kemkar as well as all the faculty members of the EXTC Department and our parents for their precious inputs. We would also like to thank Microsoft India Research team and all the relevant authors for their significant contribution in this field which provided an impetus to our paper.

References

[1] Advanced Encryption Standard (AES), Nov 2001. U.S. FederalInformation Processing Standard Publication 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[2] Near Field Communication Interface and Protocol (NFCIP-1), Dec2004. ECMA-340 Standard (2nd Edition), http://www.ecmainternational.org/publications/standards/Ecma-340.htm.
[3] NFC-SEC Whitepaper, Dec 2008. http://www.ecmainternational.org/activities/Communications/tc47-2008-089.pdf.
[4] NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH ndAES, Jun 2010. ECMA-386 Standard (2nd Edition),http://www.ecma-international.org/publications/standards/Ecma-386.Htm.
[5] http://www.nfcworld.com
[6] At Villanova University, NFC Technology Being Tested, Mar 2012.http://www.todaysfacilitymanager.com/2012/03/at-villanovauniversity-nfc-technology-being-tested.
[7] H. Kortvedt and S. Mjolsnes. Eavesdropping Near Field Communication. In The Norwegian Information Security Conference (NISK), Nov 2009.
[8] C. E. Shannon. Communication Theory of Secrecy Systems. BellSystems Technical Journal, 28, Oct 1949.
[9] A. Wyner. The Wire-Tap Channel. Bell Systems Technical Journal, 54, 1974.
[10] Paper325P2P: Secure P2P Acoustic NFC Rajalakshmi Nandakumar, Krishna Kant Chintalapudi, Venkata N. Padmanabhan, RamarathnamVenkatesan Microsoft Research India.