Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-11

A review of Bluetooth and NFC for financial applications

Z. Mngomezulu, S. Rimer, K. Ouahada, A.R. Ndjiongue

***Abstract*--Bluetooth and near field communications (NFC) are two of the most recently emerging wireless technologies** [1] [2]**, largely because of the integral role they play in the Internet of everything (IoE). In this paper, the security aspect is evaluated for these two wireless technologies for potential applications in financial systems. Their frame size is also analyzed. This is done by reviewing their characteristics based on the state of the art and on the standards governing their deployment. It is found that Bluetooth has good security mechanisms when compared to NFC, which requires developers to implement their own security features at application level; however, NFC's short range and its requirement for intentional communication between devices makes it inherently secure. It is also found that NFC has a larger message size, however, the classic Bluetooth message size is not that far below that of NFC data exchange format (NDEF) short records (SR) message size.**

***Keywords*– NFC; Bluetooth; Security; Message size; Internet of Everything**

I. Introduction

Bluetooth and near field communications (NFC) are two short range technologies of communication that can be used in many applications to transmit data, information or media between devices. These two technologies share many characteristics that are related to their transmission range and the different communication characteristics they use. These characteristics are given in detail in the IEEE 802.15.1 (Bluetooth) and ECMA- 340 (NFC) standards.

Bluetooth exploits the 2.4 GHz industrial scientific and medical (ISM) radio frequency (RF) spectrum (unlicensed), to transmit data with a bandwidth of 83 MHz [3]. It has evolved from a standard that defines basic processes for discovering and connecting to other Bluetooth devices to a standard that has low energy (LE) consumption capabilities, higher data rates, intermediate ranges and security features such as simple secure pairing (SSP) and encryption [4]. Bluetooth allows a temporary ad-hoc network to be created between at least two nodes (master and slave(s)) and up to eight active devices (piconet) can be accepted [4]. If the master and the slave belong to different piconets, then, the network is called scatternet. The Bluetooth radio transmission hops over 79 channels. It also accepts adaptive frequency hopping (AFH), which is meant to combat interference from other wireless technologies such as wireless fidelity (Wi-Fi). In a piconet, Bluetooth devices make use of packets to transmit information. These packets consist of an address code of the piconet, a header (contains the device identity (I.D.) and control), as well as the payload of the data. In order to increase the efficiency of the channel transmission, multislot (each slot is 625 μs and a packet can fit 1, 3 or 5 slots) packets are used. Packets can be transmitted in either direction (between master and slave).

NFC uses the 13.56 MHz frequency band to transmit information [5]. It uses the principle of electromagnetic induction to send information between two devices. These devices can be classified as either active ((initiator) device generates its own RF field by making use of its embedded power source (NFC enabled smart phone and NFC reader (external and internal))) or passive ((target) device does not have its own power source (NFC tag) and makes use of the power from the RF field generated by the other NFC device). The type of communication mode can also be classified in three ways. The first being an active communication where both devices generate their own RF field (peer-to-peer mode), the second being when the first device generates the field (reader/writer mode) (passive communication) and the last is when the second device generates the RF field (card emulation mode) (passive communication) [6]. An NFC tag is a simple RF identification (RFID) tag. Because only a small amount of data can be stored in an NFC tag, the applications of NFC in reader/writer mode are those that require small data capabilities such as smart posters. An NFC reader is an active device that has a bidirectional information transfer capability [5].

The success of internet of everything (IoE) largely depends on the type of communication technologies used. Because IoE requires the connectivity of devices through wired and wireless networks, in a wide variety of environments (houses, businesses, vehicles, farms, to mention only a few) and at any given time [7], a good understanding of how these technologies behave under various conditions is needed in order to enable effective and suitable implementation. Bluetooth (more specifically Bluetooth-LE) and NFC are among recent emerging wireless technologies [1] [2], whose growth has been widely accepted. There are quite a number of implementations in smartphones (iPhone operating system, android and windows) [8]. Already this gives and adds advantages to IoE systems that are centered on smartphones because there are a large number of the users that have access to this technology. With this in mind, we present in this paper a review of recent works that have been done on the evaluation of these two technologies according to their security and frame size for financial applications. We explore for both Bluetooth and NFC, the message frame and the security techniques available and draw a conclusion for financial applications.

The rest of the paper is organized as follows, Section 2 presents related work for this topic, and Section 3 provides a review for security evaluations in financial applications. Section 4 covers analysis of each technology's data frame size and Section 5 contains a comparison of both

Z. Mngomezulu, S. Rimer, K. Ouahada, A.R. Ndjongue
University of Johannesburg
South Africa

Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-11

technologies. Lastly, all the conclusions drawn from the reviews are given in Section 6.

II. State of the art

There has been quite a fair amount of research that has been done on both Bluetooth and NFC technologies with varying application interests. They all propose solutions to enhance the technologies and solve their weaknesses. Gomez et al [1] provides an overview of Bluetooth LE (BLE) by providing an evaluation of its protocol stack and its performance (energy consumption, latency, maximum piconet size and throughput), as well as by providing a comparison with other wireless technologies (ZigBee, 6LoWPAN, Z-wave and classic Bluetooth). Kurawar et al [9] evaluated Bluetooth and Bluetooth Ad hoc networks (MANETs). The structures of the communication or network are explained. The advantages of Bluetooth are given.

Ghosh et al [2] focuses on reviewing the current NFC technology in terms of operating theory, modes of operation, the security measures put in place against three of the most likely security risks and identifying some of the problems inherent to NFC as a whole (technology and market) and a proposed solution is given.

Smith [10] presents the characteristics of both Bluetooth and NFC. In addition to that, he states that the latency values of these technologies are approximately 2.5 ms for BLE and manufacturer specific for NFC.

Coskun et al [5] identifies some of the financial applications that are already employing NFC-based systems and some applications that can potentially gain from using NFC-based systems as a payment technology, e-money and e-wallet, ticketing, coupons and loyalty. In order for Bluetooth or NFC-based financial applications systems to be accepted and trusted by the end-users, Ali et al. [12] presents the following acceptance factors for these applications: Ease of use, usefulness, trust, mobility, cost, security, technical feasibility, universality, expressiveness, anonymity and scalability. However, the only acceptance factors that will be considered by this review are security, technical feasibility, anonymity as well as trust.

There are also investigations that seek to make use of each technologies' strengths. In fact, in one of the studies done in literature by Monteiro et al [11], a system that combined both these wireless technologies' strengths (short setup time of NFC and relatively higher data rate of Bluetooth) was proposed and implemented.

III. Security

Financial applications require strong security and privacy mechanisms because they deal with people's personal, and hence private information.

Bluetooth has built in security mechanisms (four modes) that are inherent with the technology [13]. All the data in the transmission is encrypted. Despite these security features, threats such as surveillance, sniffing, denial of service (dos) amongst others can still be experienced. For authentication, older versions of Bluetooth (such as v2.0 + EDR) make use of a 4 digit or fixed PIN passive eavesdropping protection, while newer versions use a 16 digit alphanumeric PIN. A strong link key and encryption can be used to protect against passive eavesdropping. Bluetooth v4.0 uses the secure simple pairing technique, which protects against recording and eavesdropping, which is a very important feature that will prevent any third parties from getting one's card details and banking PINs especially when one is using Bluetooth to connect to a POS device or performing a credit transfer using smartphones. The added elliptic curve diffie Hellman encryption will protect one's information during the transaction. Bluetooth numeric comparison, just works and passkey entry association models would be suitable for financial applications such as POS, credit transfers, businesses' promotional and specials communications to customers using mobile banking services amongst other things. Threat mitigation techniques such as manufacturers adopting procedures that test Bluetooth products' vulnerability to security attacks with the relevant security bridging tools can be applied [14].

NFC components that can be compromised include the host controller, the NFC controller as well as the secure element (SE) [15]. With the use of an adversary model adapted from Avoine [16], security threats such as an attack on NFC transponders through the use of the fixed IDs on smart cards, relay attacks, dos, phishing as well as the cloning of tags are identified. The type of attack depends on the use case, which in-turn determines the type of communication and the mode of operation. When an NFC-based system is deployed at POS locations, an active-to-passive (AtP) communication will be used. An external reader can access the devices SE (chip used to protect secret information such as credit card, bank details, and PINs etc.). In the case of loyalty and coupon applications, an AtP communication will take place. Malicious information could be stored on the tag. In the case of credit transfers among smartphones, active-to-active (AtA) communication will take place, the authenticity, integrity and confidentiality of the data cannot be guaranteed because the transaction would not have encryption or authentication unless this is added on the application level. Lastly, there are also cases where applications stored on the smartphone can read and alter information stored on the SE. Some of the possible (already) implemented solutions include the use of signatures on tags and transponders in order to validate information stored on tags. The use of a random number for anti-collisions instead of a fixed ID, using hardware for ID spoofing purposes, adding a security layer to NFC devices that can employ certificate-based authentication or a Diffie-Hellman encryption [15] are all possible solutions for countering the mentioned security threats/attacks.

IV. Frame analysis

In NFC technology, a small binary message enclosure format namely, NFC data exchange format (NDEF) is used to transmit information between devices [17]. An NDEF message is made up of records, which can have formats called record type definitions (RTD), which are text, uniform

Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-11

source identifier (URI), smart poster (SP), generic control (GC) as well as a connection handover (CH). Fig. 1 depicts the layout of an NDEF message. The NDEF message is shown to contain a three records (it can contain up to n records) [5]. These records are used to encapsulate payloads and can be chained together to enable the transmission of larger payloads. The header contains information about the data's type and size [18], while the value of the type name format (TNF) corresponds to the type of information that is in the payload [20]. Fig. 2 shows the structure of an NDEF record. The first record is shown to be labelled message begin (MB) while the second is labelled message end (ME). Payload length specifies the amount of bytes that a payload contains, while the type specifies the type of payload that the record is carrying and the ID field is an identifier that enables user applications to identify the type of payload that is carried in the message. The size of the payload (in one record) can range up to 2^{32} -1 bytes [5] while short records (SR) can fit payloads ranging from 0 to 255 bytes [21].

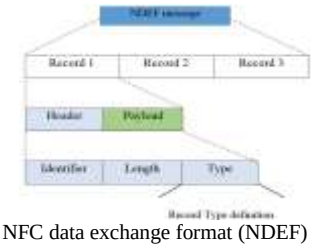
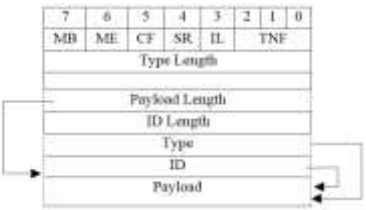


Figure 1. NFC data exchange format (NDEF) Message [18]

Classic Bluetooth has a maximum frame size of 358 bytes while BLE has frame sizes that range from 8 to 47 bytes [1]. Bluetooth has two types of packet formats that it transmits; these are asynchronous-connectionless (data) and synchronous connection-oriented (voice) [3]. Tables I and II are taken from the Bluetooth IEEE standard, and provide a brief summary of the characteristics of the packets while Fig. 3 depicts their format. It is indicated that the user payload field excludes forward error correction (FEC), cyclic redundancy check (CRC) as well as the payload header [3].



*Message Begin (MB), Message End (ME), Chunk Flag (CF), Short Record Flag (SR), ID Length (IL) Present Flag, Type Name Format (TNF) [19]

Figure 2. NFC data exchange format (NDEF) Record [19]

TABLE I. ACL PACKETS CHARACTERISTICS [3]

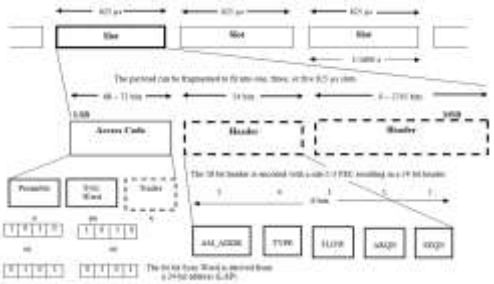
Type	Payload header (bytes)	User payload (bytes)	FEC	CRC	Symmetric max. rate (kb/s)	Asymmetric max. rate (kb/s)	
						Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	Yes	172.8	172.8	172.8
DM3	2	0-121	2/3	Yes	258.1	258.1	54.4
DH3	2	0-183	no	Yes	390.4	390.4	86.4
DM5	2	0-224	2/3	Yes	286.7	286.7	36.3
DH5	2	0-339	no	Yes	433.9	433.9	57.6
AUX1	1	0-29	no	No	185.6	185.6	185.6

* Data Medium (DM) rate, Data High (DH) rate, Auxiliary (AUX) [3]

TABLE II. SCO packets characteristics [3]

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)
HV1	na	10	1/3	no	64.0
HV2	na	20	2/3	no	64.0
HV3	na	30	no	no	64.0
DV*	1D	10+(0-9)D	2/3 D	yes D	64.0+57.6 D

* High-quality Voice (HV), Data Voice (DV) [3]



* Active Member Address (AM_ADDR), Automatic Repeat Request Negative (ARQN), Sequential Numbering Scheme (SEQN), Header Error Check (HEC) [3]

Figure 1. Bluetooth packet format [3]

V. Comparison

Table III, provides a brief summary of the main characteristics of Bluetooth and NFC.

When comparing the two technologies in terms of their security, it can be seen that because Bluetooth has a longer range compared to NFC, it is more susceptible to eavesdropping and Man-In-The-Middle attacks [13]. However, it carries an advantage over NFC in the sense that it comes with standard security protocols (which are handled at the beginning of the communication, after which, the communication between the two devices will be secured), so there is no extra work of adding security protocols on the user at the application level. However, it should be noted also that the short range of NFC and application controlled devices interaction make it considerably secure as well. From the information obtained in the frame analysis section, NFC (232 – 1 bytes max and 255 bytes for SR) seems to have a larger frame size than classic Bluetooth (358 bytes max), while BLE has the lowest size of 47 bytes. Evaluating these values for financial applications, which mostly require the exchange of information in data form (not voice), Bluetooth ACL packets would be suitable. It should be noted however, that the frame size of classic Bluetooth is not smaller than that of NFC NDEF SRs (255 bytes), so Bluetooth-based systems would not be inefficient.

VI. Conclusion

An evaluation of Bluetooth and NFC was done for financial applications. Through a review of literature and standards, the suitability of the application in financial systems was evaluated. Because the nature of this application field is one of dealing with sensitive and private information, the security, confidentiality as well as the integrity of the user's data and information transferred between the devices is of outmost importance. It was found that Bluetooth has more security mechanisms compared to NFC, which does not offer authentication and encryption unless developers add the feature in the application level, however, NFC has an inherent security level due to its short range (4 cm) and the fact that communication between devices has to be intentional. Going back to the acceptance factors stated in the introduction, having a wireless technology that has a large frame size would have a positive impact on the efficiency of the system (if the system can transmit large sizes of payloads at a time, then the transmission of data

Proc. of The Sixth Intl. Conf. On Advances In Computing, Control And Networking - ACCN 2017

ISBN: 978-1-63248-117-7 doi: 10.15224/ 978-1-63248-117-7-11

TABLE III. SUMMARY OF BLUETOOTH AND NFC CHARACTERISTICS [2], [3], [5], [6], [7]

	Bluetooth	Near Field Communication
Frequency band	2.4 GHz	13.56 MHz
Data rate	Ver. 1.2 – ≤ 721 kbps Ver. 2 + EDR – ≤ 3 Mbps Ver. 3 + HS – ≤ 24 Mbps Ver. 4 + LE – ≤ 1 Mbps	106 kbps 212 kbps 424 kbps
Range	10 – 100 m	4 – 10 cm
Modulation scheme	Gaussian Frequency Shift Keying (GFSK) π/4 Differential Quadrature Phase Shift Keying (π/4 DQPSK) 8 Differential Phase Shift Keying (8DPSK)	Amplitude Shift Keying (ASK) Load Modulation (LM)
Hopping technique	FHSS	NFC ID
Type of communication	Two way Active - Active	Two way Active – Active Active – Passive
Networks	Piconets (point-to-point) (point-to-multipoint) Scatternets (multi-Masters)	Point-to-Point
Security	Authentication Encryption Confidentiality	Authentication Encryption (Advanced Encryption Standard) confidentiality
Output power	Classic Bluetooth Class 1 – 100 mW Class 2 – 2.5 mW Class 3 – 1 mW BLE 0.01 mW to 10 mW	≤ 15 mA
Modes of operation	Sniff Hold Poll	Passive Active
Error correction	Classic Bluetooth 8-bit CRC (header), 16-bit CRC and 2/3 FEC (payload), Acknowledgements BLE 24-bit CRC acknowledgements	16-bit CRC

between devices will be faster), which would result in a better customer user experience, because they would not have to spend long periods of time when making use of the system. When comparing the communication technologies' data frame size also, it was found that NFC (2^{32}–1 bytes max and 255 bytes for SR) offered a larger frame size than Bluetooth (358 bytes and 47 bytes for BLE), however, the values are not too far apart in the case of classic Bluetooth and NFC NDEF SRs (358 bytes and 255 bytes respectively). It would be beneficial however, to consider financial systems that are designed to take advantage of the strengths of both technologies (such as the short set up time and effortless use of NFC and the data rate, security, and range of Bluetooth). In fact, studies are done where systems that combine both these wireless technologies' strengths (short setup time of NFC and relatively higher data rate of Bluetooth) [11] are proposed and implemented.

Acknowledgment

I would like to thank all the authors (S. Rimer, K. Ouahada and A.R. Ndjongue) of this paper for all their continued support and guidance, as well as for going beyond the call of duty to assist me. I would also like to thank O. Jantjies, for always standing by me.

References

[1] C. Gomez, J. Oller and J. Pradells, "Overview and Evaluation of Blueooth Low Energy: An Emerging Low-Power Wireless Technology," *Sensors*, vol. 12, pp. 11734-11753, 2012.

[2] S. Ghosh, J. Goswami, A. Kumar and A. Majumder, "Issues in NFC as a Form of Contactless Communication: A Comprehensive Survey," in *International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, Chennai, T.N., 2015, May.

[3] *IEEE Standards 802.15.1: Part15.1-Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)*, New York: The Institute of Electrical and Electronics Engineers, Inc., 2002, June 14.

[4] L. Harte, Introduction to Bluetooth: Technology, Market, Operation, Profiles, and services, Fuquay-Varina: Althos, 2010.

[5] V. Coskun, K. Ok and B. Ozdenizci, Near Field Communication: From Theory to Practice, Chichester: Wiley and Sons Ltd, 2012.

[6] V. Coskun, B. Ozdenizci and K. Ok, "The Survey on Near Field Communication," Sensors, vol. 15, pp. 13348-13405, 2015, June.

[7] O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, Aalborg: River Publishers, 2013.

[8] S. Silva, S. Soares, T. Fernandes, A. Valente and A. Moreira, "Coexistence and Interference Tests on a Bluetooth Low End Front-End," in Science and Information Conference (SAI), (pp. 1014 - 1018), IEEE, London, 2014.

[9] A. Kurawar, A. Koul and V. Patil, "Survey of Bluetooth and Applications," International Journal of Advanced research in Computer Engineering and Technology (IJARCET), vol. 3, no. 8, pp. 2832-2837, 2014.

[10] P. Smith, "Comparisons between Low Power Wireless Technologies". US Patent CS-213199-AN, 2011.

[11] D. Monteiro, J. Rodrigues and J. Lloret, "A secure NFC Application for Credit Transfer Among Mobile Phones," in International Conference on Computer, Information and Telecommunication Systems (CITS), (pp. 1 -5), IEEE, New York, 2012, May.

[12] A. Ali, R. Abouhogail, I. Tarrad and M. Youssef, "Assessment and Comparison of Commonly used Wireless echnologies from Mobile payment Systems Perspective," Internal Journal of Software Engineering and its Applications, vol. 9, no. 2, pp. 255-266, 2014.

[13] S. Sandhya and D. Sumithra, "Analysis of Bluetooth Threats and v4.0 Security Features," in International Conference on Computing, Communication and Applications (pp. 1-4), IEEE, 2012, February.

[14] J. Dunning, "Taming the Blue Beast: A Survey of Bluetooth based threats," IEEE Security and Privacy, vol. 8, no. 2, pp. 20-27, 2010, March-April.

[15] G. Madlmayr, J. Scharinger and C. Kantner, "NFC Devices: Security and Privacy," in The Third International Conference on Availability, Reliability and Security, ARES 08, (pp. 642-647), IEEE, 2008, March.

[16] G. Avoine, "RFID: Advesary Model and Attacks on Existing Protocols," Swiss Federal Institute of technology: School of Computer and Communication Sciences, Lausanne, 2005, September.

[17] S. Hameed, U. Jamali and A. Samad, "Integrity Protection of NDEF Message with Flexible and Enhanced NFC Signature Records," in IEEE Trustcom/BigDataSE/ISPA, 2015.

[18] G. Zhang, C. Fan and J. Zou, "A Research on the Transcoding Mechanism for NFC Message Format," in 10th international Conference on Wireless Communication, Networking and Mobile Computing (WiCOM 2014), (pp. 593-597), IET, 2014, September.

[19] M. Roland, J. Langer and J. Scharinger, "Security Vulnerabilities of the NDEF Signature Record Type," in Third International Workshop on Near Field Communication (NFC), (pp. 65-70), IEEE, 2011, February.

[20] M. Roland and J. Langer, "Digital Signature Records for the NFC Data Exchange Format," in Second International Workshop on Near Field communication (NFC), (pp.71-76), IEEE, 2010, April.

[21] P. Stiparo, "A Fuzzing Framework for the Security Evaluation of NDEF Message Format," in 2013 Fifth Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), (pp. 165-170), IEEE, 2013, June.

[22] IEEE Standards 802.15.1: Part 15.1 - Wireless Medium Access Control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs), New York: The Institute of Electrical and Electronics Engineers, Inc., 2005.

[23] Standard ECMA - 340: Near Field Communication Interface and Protocol (NFCIP-1), Geneva: Ecma International, 2004.

"The success of internet of everything (IoE) largely depends on the type of communication technologies used"