High Speed Data Transmission over a Visible Light Link Employing Smartphones Xenon Flashlight as a Replacement of Magnetic Cards

Mariam M. Galal, Ahmed Abd El Aziz, Heba A. Fayed and Moustafa H. Aly
Photonics Research Lab (PRL)
Arab Academy for Science and Technology (AAST)
Alexandria, Egypt
prlsupervision@gmail.com

Abstract— This paper uses built-in Xenon flashlight in today's smartphones to experimentally replace the magnetic card. Due to the high dependence of the users nowadays on their smartphones and their wide availability and use in nearly all everyday tasks, the idea of integrating smartphones in financial transactions such as payments and withdrawals has attracted the interest of many researchers. Therefore, in this paper, we experimentally modulate the embedded Xenon flashlight in a smartphone with the required information of a traditional magnetic card and transmit the light over a secure high speed optical link at 15 bps with no additional hardware at the user end to a small, inexpensive supplementary circuit module, easily attached to a contemporary card reader or Automatic teller machines (ATM).

Keywords—Visible light communication; Xenon flashlight; ATM machines; smartphones; smart payments

I. INTRODUCTION

Nowadays, smartphones are more integrated in our lives and play a vital role in the daily tasks. Not only are they used for phone calls and texting, but their functions are extended to replace many electronic devices such as cameras, media players, gaming consoles and personal digital assistants [1, 2]. The dependence and reliability of smartphone has increased dramatically over the last decade thanks to the advances in technology resulting in an increase of the battery life, decrease of the hardware and circuitry size as well as the built-in memory and thereby an obvious improvement of hardware and software performance. For that reason, researchers have tried to further integrate smartphones in more sensitive and critical daily tasks, such as for payments [3].

Furthermore, financial transactions and banking has taken many advanced and smarter forms in the past decade. Regular trips to the bank have been decreased dramatically thanks to advances in technology and secure communication. Today's user can depend on internet banking, phone banking and of course credit and debit cards along with ATM machines for performing all financial tasks such as transfers, withdrawals and payments [2].

In order to accommodate these technological advances in the financial sector, smartphone giants have been working hard on integrating smartphones in payments and withdrawals. Different technologies have been proposed in order to transmit the required information to automatic teller machines (ATMs) or card readers. For instance, Google and Samsung developed the so called Near Field Communication (NFC), which requires the user to tap the back of his NFC enabled smartphone on the surface of an also NFC enabled card reader to transmit the required credit card information [4]. On the other hand, Square, another company working in the field of technology in payments, has created a bulky cubic accessory to be attached to the smartphone, which is used to transmit the credit card information over Wi-Fi to the vendor for payment [5]. However, due to the incompatibility, complexity, expensive hardware or the lack of security, an alternative technique is still required [6-9].

In this paper, we experimentally transmit the card data at high speed rates over a secure visible light link by modulating the embedded flashlight existing in almost all contemporary smartphones to a small sized, easily integrated and inexpensive supplementary module added at the receiver end. In the next section, previous research dealing with information transmission over flashlight is introduced. In section 3, the experimental setup and circuitry of the proposed system is described, followed by the measured results in section 4. Section 5 concludes the experimental work.

II. PREVIOUS RELATED WORK

Many researchers have shown interest in studying the possibility of using the built-in flashlight of the smartphone for other communication-related functions. T. Hesslemann el at studied in their paper the use of the built-in LED flashlight for transmitting data between smartphones and interactive tabletops. In their study, they claimed that visible light communication between smartphones and tabletops are more advantageous than the commonly used Bluetooth and wireless radio frequency (RF) technologies since it's more secure and prevents eavesdropping. -For the uplink, the authors modulated the built-in flashlight of a Nexus S smartphone using Non-return-to-zero (NRZ) On-Off-Keying (OOK) modulation scheme and transmitted it over a zero-length secure channel to the tabletop by placing the smartphone

978-1-4799-2569-8/13/$31.00 ©2013 IEEE

scree-side up on the tabletop. The tabletop then detects the transmitted light on its surface and decodes the transmitted message. Data rates of up to 25 bps have been achieved using this setup [7].

In another research conducted by A. S. Shirazy et al, the possibility of interaction with large public displays using smartphones has been studies. In this case, the built-in flashlight is used in its raw form without modulation. The user holds his/her smartphone with the flashlight on and directed towards the display screen. A webcam located under the screen captures the movement of the user's hand by video processing and accordingly maps the hand movement and gesture to the movement of a cursor on the display screen. Moving the smartphone closer or farther from the screen results in zooming in or out respectively, while turning the flashlight off and back on quickly results in a selection of the item on which the cursor is placed, similar to a computer mouse click action[10].

In this paper, the Xenon flashlight of a smartphone is modulated with the required magnetic card information and transmitted over a short length free space shielded channel to a photodetector circuit on the receiver side.

III. EXPERIMENTAL SETUP

An ATM card consists mainly of 3 magnetic tracks. Although track 1, which consists of 79 alphanumeric characters, contains detailed information about the bank account and the card owner including his/her name, it is very rarely used. On the other hand, track 2, which contains only 40 numeric characters and carries information about the bank account number, expiry date, CVC number and some security information, is very widely used. Lastly, track 3 is reserved for future use. Each character of the stored information on track 2 is represented by 4 binary bits followed by one parity bit, resulting in a total of 200 binary bits. Table 1 shows the binary code used to represent each of the numeric characters possibly found on track 2 [11].

Data bits				Parity	Character	Value	Function
b1	*b2*	*b3*	*b4*	*b5*		*(Hex)*	
0	0	0	0	1	0	00	Data
1	0	0	0	0	1	01	Data
0	1	0	0	0	2	02	Data
1	1	0	0	1	3	03	Data
0	0	1	0	0	4	04	Data
1	0	1	0	1	5	05	Data
0	1	1	0	1	6	06	Data
1	1	1	0	0	7	07	Data
0	0	0	1	0	8	08	Data
1	0	0	1	1	9	09	Data
0	1	0	1	1	:	0A	Control
1	1	0	1	0	;	0B	Start Sentinel
0	0	1	1	1	<	0C	Control
1	0	1	1	0	=	0D	Field Separator
0	1	1	1	0	>	0E	Control
1	1	1	1	1	?	0F	End Sentinel

Table 1. Bit representation and functions for characters on track 2 of an ATM card.

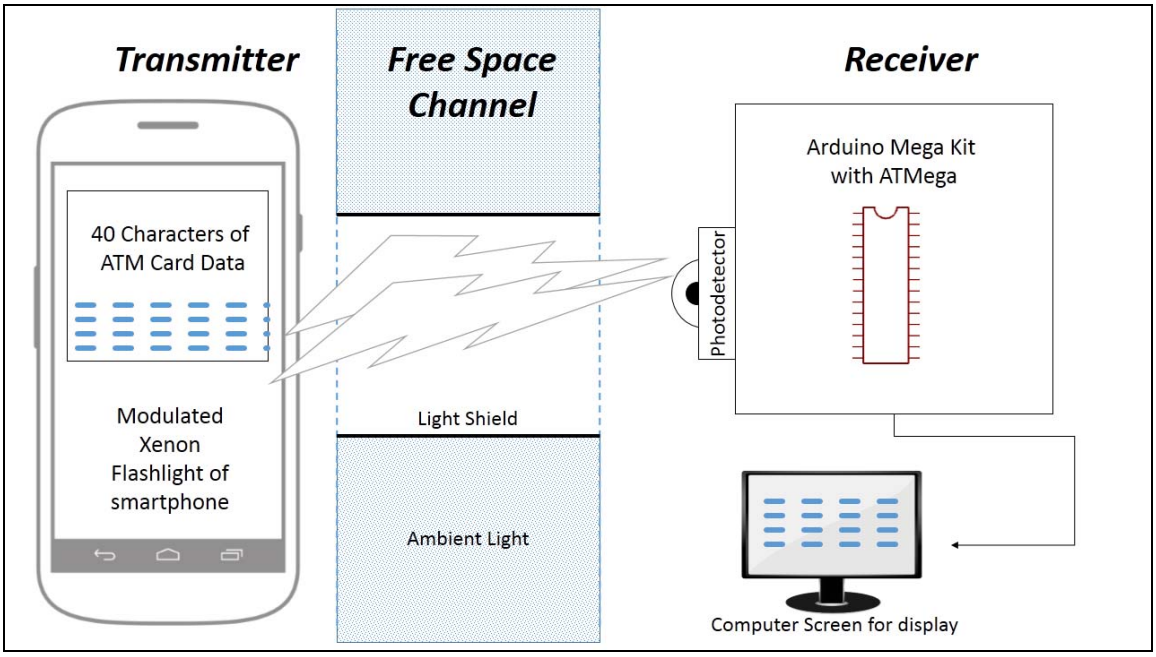

Fig. 1 Block Diagram of the implemented system

As shown in the block diagram of the implemented system in Fig. 1, these 200 binary bits are used to modulate the Xenon built-in camera flashlight of a Samsung smartphone running Android 4.2.2 operating system, aka. Jellybeans. A specially designed Android application has been developed to provide the user interface and to allow the tester to experiment with different pulse widths as well as modulation schemes as seen in Fig. 2. The information carrying flashlight propagates along a free space, shielded, short length channel to the receiver end as shown in the block diagram. A photodetector is used to receive the signal and sends an equivalent electronic signal to an Arduino Mega kit equipped with an ATMEGA microcontroller for data processing. The decoded information is then transmitted to the computer and displayed on the screen.

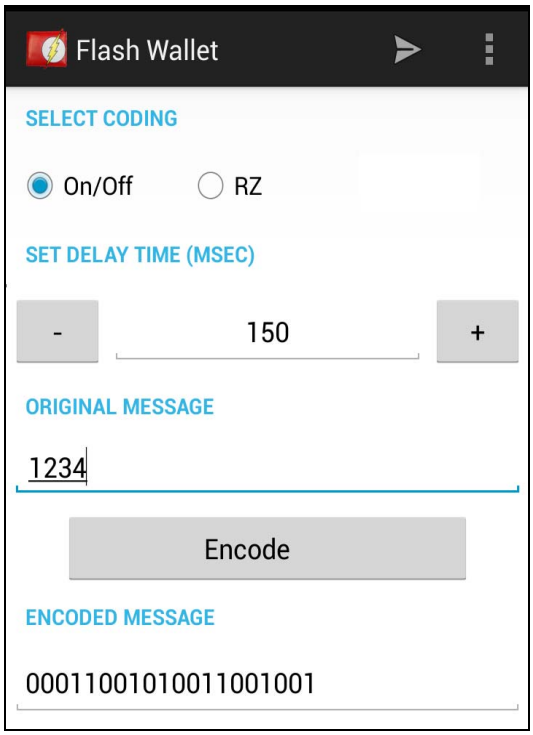

Fig. 2 User interface of the developed Android application

IV. Results and Discussion

The flashlight is first modulated using on-off keying (OOK) with non-return-to-zero (NRZ) bit duration t_b of 50 ms while the data is detected via light dependent resistor (LDR). The normalized light intensity of both transmitted and received data are displayed in Fig. 3. Although the LDR was able to detect the transmitted data, it showed lower sensitivity to bit sequences with consecutive '1's and '0's due to the absence of transition of states, i.e. the system failed to detect the number of consecutive bits. The delay accumulated vastly with increasing number of transmitted bits resulting in no error-free transmission of the required information at any data rate.

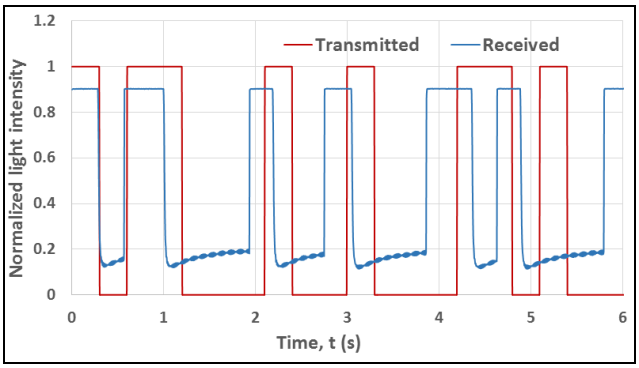

Fig. 3 The normalized light intensity of the transmitted and received signals with OOK modulation

In order to overcome this synchronization problem, pulse width modulation (PWM) is used to encode the Xenon flashlight. This modulation technique uses return-to-zero (RZ) bits to ensure a transition of state after each bit. The '0' and '1' bits are transmitted over t_b and $3t_b$ of high intensity respectively, followed by t_b of zero intensity. As a result, high synchronization between both transmitted and received signals is achieved using the PWM technique as shown in Fig 4 despite time delays or inconsistency of pulses width. This experimental setup results in error-free transmission of the data for data rates up to 4.2 bps (i.e. t_b = 230ms, assuming equal probability of ones and zeros). The bit error rate (BER) rises rapidly for higher speeds and oscillates about a value of 0.4 as shown in Fig. 5.

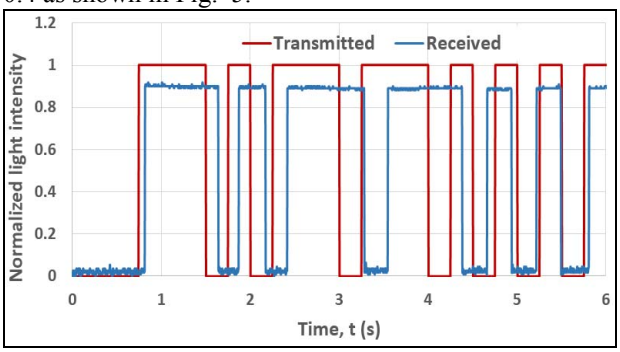

Fig. 4 The normalized light intensity of the transmitted and received signals with PWM modulation

It is important to further carry out the practical investigation in order to maximize the speed of transmission. Accordingly, a photodiode, which has a higher sensitivity with much lower response time compared to LDR [12,13], is used to detect the transmitted signal. While the LDR has a rise and fall time of 18 and 120 ms respectively [12], a photodiode has a rise and fall time of only 1.5 µs, only a small fraction of that of the LDR [13]. Consequently, error-free transmission is achieved at higher rates reaching 15 bps (i.e. t_b = 22 ms assuming equal probabilities for '0's and '1's) as shown in Fig. 5. The figure compares the BER of the three experimental configurations at different data rates and shows that error-free transmission is successfully achieved with experiments using PWM while OOK on the other hand failed at all data rates. Significant

improvement of more than 350% in the transmission speed was obtained by using a photodiode instead of LDR. One can also observe from Fig. 5 that for all experiments, at data rates with no error-free transmission, the BER tends to oscillate close to 0.4. Altering the distance between the transmitter smartphone device and the receiver causes no change of the system performance since the intensity of the Xenon flashlight is high enough to be differentiated from the complete darkness provided by the light shield over long distances. We have experimented with shielded channels of different lengths ranging from 2 to 35 cm without any significant change of the achieved results.

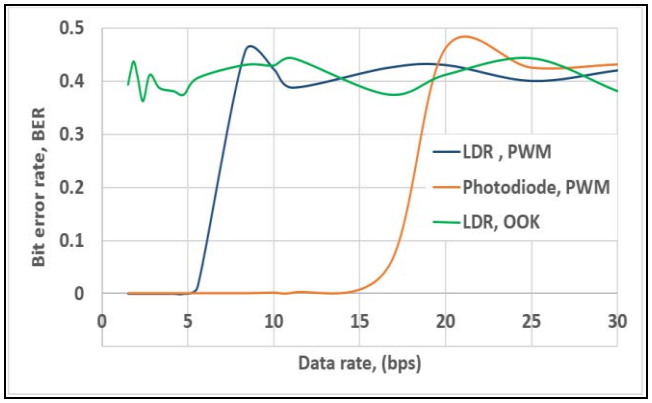

Fig. 5 Bit error rate with rising data rate with different experimental setups

V. CONCULSION

This paper practically implements a simple, high speed and secure visible light link using existing smartphones to replace the magnetic cards. While the OOK modulation scheme resulted in a failure to correctly receive the transmitted signal, the system achieves error-free transmission of the required card information at high speeds up to 4.2 and 15 bps using LDR and photodiode detectors respectively when the Xenon flashlight is modulated with PWM. Since the visible light link requires direct line of sight between transmitter and detector, the system prevents eavesdropping while providing high security for the sensitive credit card data transmitted.

REFERENCES

[1] Amy K. Karlson, Brian R. Meyers, Andy Jacobs, Paul Johns, and Shaun K. Kane, “Working Overtime: Patterns of Smartphone and PC Usage in the Day of an Information Worker”, Proceedings of Pervasive Computing, May 2009, pp 398-405.

[2] Diniz, Eduardo Henrique, João Porto de Albuquerque, and Adrian Kemmer Cernev, "Mobile Money and Payment: a literature review based on academic and practitioner-oriented publications (2001-2011).

[3] Blöchlinger, Michael. "Mobile Payment Systems." Internet Economics VI (2012): 41.

[4] G. Inc., "Google Wallet," 2012-2013. [Online]. Available: http://www.google.com/wallet/.[Accessed 30 June 2013].

[5] S. Inc., "Square," 2009-2013. [Online]. Available: https://squareup.com/. [Accessed 30 June 2013].

[6] M. Roland, J. Langer, and J. Scharinger: Applying Relay Attacks to Google Wallet. In: Proceedings of the 5th International Workshop on Near Field Communication (NFC 2013), Zurich, Switzerland, Feb. 2013, pp. 1-6

[7] T. Hesselmann, N. Henze, and S. Boll, "FlashLight: optical communication between mobile phones and interactive tabletops", in Proc. ITS, 2010, pp.135-138.

[8] Browning, D., & Kessler, G.C. (2009, May). Bluetooth Hacking: A Case Study. In G. Dardick (Ed.), Proceedings of the Conference on Digital Forensics, Security and Law, May 20-22, 2009, Burlington, VT, pp 57-71.

[9] "Aeronautics and Space.", 14 CFR 91.21. 2010

[10] A. . S. Shirazi, C. Winkler and A. Schmidt, "Flashlight Interaction: A Study on Mobile Phone Interaction Techniques with Large Displays," in *ACM 978-1-60558-281-8.*, Bonn, Germany, 2009.

[11] Information technology -- Identification cards -- Financial transaction cards, ISO/IEC 7813:2006

[12] RS, “Light dependent resistors,” NORP12 datasheet, Mar. 1997.

[13] OSRAM, “Silicon photodiode for the visible spectral range,” BPW21 datasheet, Apr. 2007.