2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks

Smartphones for Payments and Withdrawals Utilizing Embedded LED Flashlight for High Speed Data Transmission

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

***Abstract*— In this paper, we experimentally transmit the required information to the automatic teller machine (ATM) or card readers over a visible light communication channel employing mobile smartphones LED flashlight at high data rates. Due to the dependence of users on their personal digital assistants and smartphones to perform almost everyday tasks including payments and banking transactions, it is of great interest to use such phones to replace the magnetic cards. This paper encodes the LED camera flashlight embedded in almost every smartphone with the required information with no additional hardware on the receiver end. However, a small sized non-expensive module is added to ATMs and card readers to detect and decode the received data. The proposed unidirectional optical link offers secure transmission with a speed up to 500 bps with no error detected.**

Keywords—LED; flashlight; magnetic cards; smartphones; OOK; Intensity modulation; visible light

I. INTRODUCTION

The dependence on smartphones has rapidly increased within the past few years to become a vital hybrid personal assistant by executing several of other functions beside phone calls and texting. Consequently, such phones were able to replace a number of electronic devices such as cameras, internet browsers, video games, recorders and music players [1].

On the other hand, credit/debit card technology has rapidly increased and became the main method for payments and withdrawals over the last decade [2]. Such cards save trips to banks, are easier to use and carry and more secure compared to cash. However, those cards are easily lost and malfunction with an unclean or scratched magnetic stripe which decreases the card reliability.

In view of that, there is an emerging trend to replace magnetic cards by personal smartphones for payments and withdrawals. Therefore, the demand for a secured link between smartphones and card readers/automatic teller machines (ATM) has attracted several researchers and giant commercial companies including Google and Samsung [3].

Radio-based transmission such as Wi-Fi or Bluetooth seemed adequate for this application. However, such highly sensitive data transmitted can be easily hacked by other devices using same technologies [3-5]. Google has presented a similar approach which relies on near field communication (NFC) which is a technology based on radio frequency identification (RFID) [3]. This approach requires the user to tap the back of his/her NFC enabled smartphone on compatible hardware on the receiver end for transmitting his/her card information. Meanwhile, this technology is not compatible with all current smartphones and requires expensive hardware on both transmitter and receiver ends. Moreover, hackers have recently managed to copy the card information by hiding an NFC chip at the receiving end or by using certain antennas from a distance up to few meters [3]. Square is another technology recently implemented in the US market that promises a more secure approach, however it requires the user to buy an expensive and bulky additional accessory for their smartphones in order to send the card information to an equally complicated, bulky and expensive hardware at the receiver end [6]. In addition, those technologies are prohibited in certain places, such as hospitals and airplanes due to their interference with other radio frequency (RF) equipment and devices [7].

In this paper, we propose transmitting the required card information over a secure visible light communication link which illuminates the probability of hackers attack. The data is transmitted via the light emitting diode (LED) flashlight of existing mobile smartphones at the user's end with no additional hardware required. However, at the receiver end, a small sized, easily integrated and inexpensive supplementary module is added to the currently installed ATMs and card readers. The experimental setup is introduced in the following section. The results of the executed experiments are presented and analyzed in section III. The final section concludes the findings of the paper

II. EXPERIMENTAL SETUP

The data stored on a magnetic card is found on three different magnetic tracks. Although track 1 which consists of 79 alphanumeric characters carries detailed information about the card holder including the user name, most ATMs and card readers just use the data stored in track 2 which consists of only 40 numeric digits. For that reason, those 40 characters are considered the required information to be transmitted in this paper over the visible light link. On the other hand, track 3 is reserved for future use. The data stored in track 2 consists of the primary account number followed by a single character separator, 3 digit service code and discretionary data and one end sentinel. To mark the start and the end of the track, the first and second last

978-0-7695-5042-8/13 $26.00 © 2013 IEEE
DOI 10.1109/CICSYN.2013.23

character of the track serve as start and end sentinel respectively, while the last stored character is a longitudinal redundancy check used for error correction and calculated from the sum of the previous characters bits [8].

Each of the 40 characters in track 2 is represented using 4 binary digits followed by single parity bit. The bit representation and function of all the characters used on track 2 of an ATM card according to the ISO 7810, 7811 & 7813 standards are shown in Table 1 [8].

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.

A block diagram for the experimental setup is shown in Fig. 1. An HTC Desire smartphone running Android 2.2 is used in this experiment to transmit the card information over a free space channel. The flashlight application provided by this smartphone uses LED as a light source and offers four different light intensity levels.

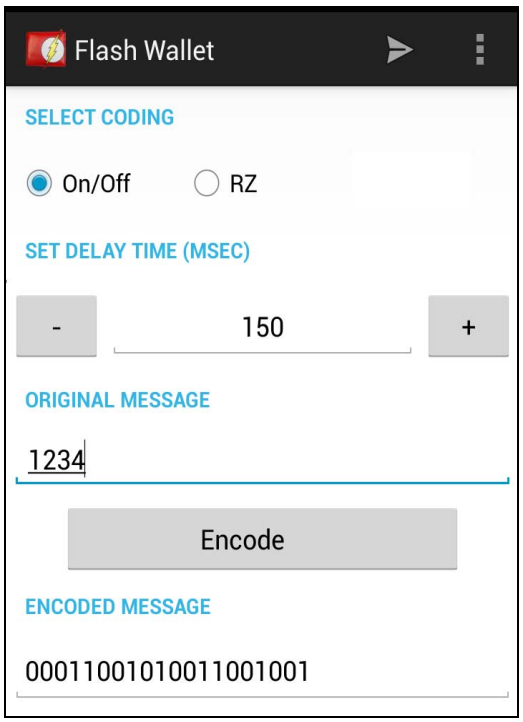

Fig. 2. Snapshot from the user interface of the developed Android application

The required card information represented by the 40 characters modulates the embedded LED flashlight using a

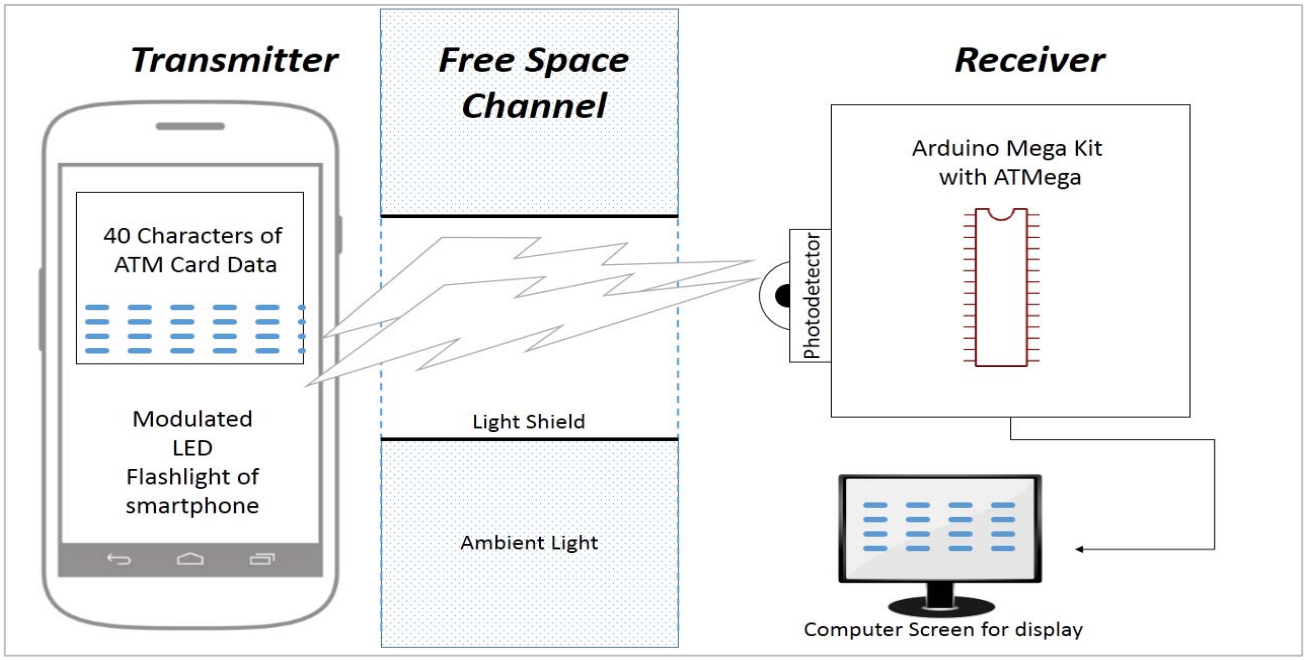

Fig. 1. Block diagram of the experimental setup

proposed software application with no additional hardware required. A snapshot from the user interface of the proposed android application is displayed in Fig. 2 showing the type of coding used, the time delay representing the bit duration (i.e. transmission data rate), the card information and its binary representation.

The modulated light signal propagates along a short free space channel (i.e. the distance between the user and the ATM machine or card reader). In this experiment, the channel is protected by a light shield in order to minimize ambient noise (i.e. external light interference such as sunlight or other lighting sources).

A simple photodetector component is added to the ATM machine or card reader at the receiver end in order to detect the light signal before it is fed to an ATMEGA microcontroller mounted on an Arduino Mega kit.

The microcontroller compares the received intensity level versus a pre-programmed threshold in order to recognize the received bit. The decoded data is then displayed on the computer screen a universal serial port (USB) and.

The performance of the system is measured using Actual data from several expired magnetic cards are used in this paper in order to measure the validity of the proposed technique and to measure the system performance. Since this application only uses highly sensitive and private data, only completely error-free reception is considered successful. All experiments have been executed several times to ensure error-free transmission.

III. RESULTS AND DISCUSSION

The LED flashlight is first modulated using on-off keying (OOK) with non-return-to-zero (NRZ) bit duration t_b. The transmitted signal is detected by a light dependent resistor (LDR) operating in the visible light range centered at $\lambda = 550$ nm [9]. The executed experiment did not achieve an error-free transmission due to the lack of synchronization between both transmitted and received signals shown in Fig. 3. The LDR showed low responsivity to consecutive '1's and '0's due to the absence of transition of states. Accordingly, an accumulation in time delays occurs and results in high bit error rates (BERs) of about 0.4 at any transmission speed.

In order to achieve error-free transmission, a new experiment is executed where the flashlight is modulated using light intensity modulation with return-to-zero (RZ) bits. In this experiment the brightness control feature is employed to represent the '1' and '0' bits by a t_b of high and low intensities respectively, followed by a t_b of an intermediate level. This modulation technique allows the detector to distinguish the transition of states and therefore is able to successfully recognize the transmitted bits regardless of the received bit duration as seen in Fig. 4. The figure illustrates the normalized received signal showing the three different intensity levels.

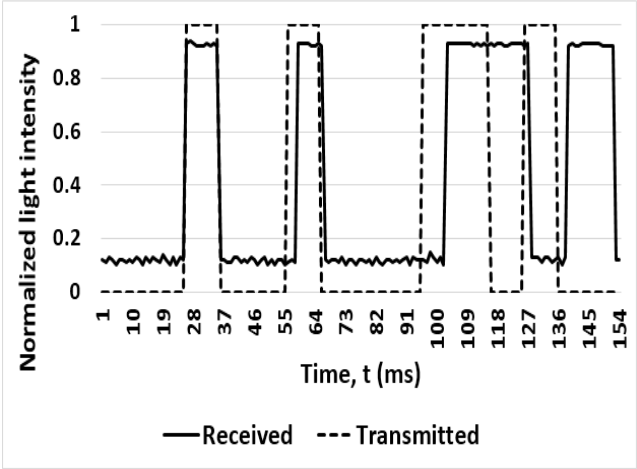

Fig. 3. Normalized light intensity of the transmitted and received signals using OOK modulation and LDR detector

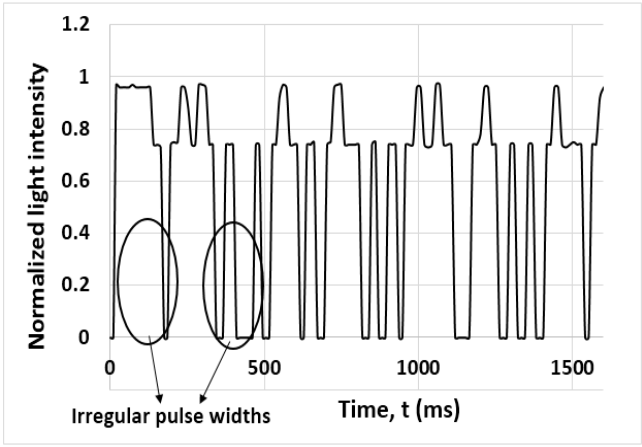

Fig. 4. Normalized light intensity of the received signal using intensity modulation and LDR detector

In order to measure the transmission performance employing the intensity modulation technique, the BER is calculated at different speeds and the corresponding results are presented in Fig. 5. This experiment was able to achieve error-free transmission at high speeds up to 100 bps as shown in Fig. 5. One can also see from Fig. 5 that at all executed speeds, lower BERs are achieved (i.e. < 0.1 at data rates up to 500 bps) compared to the 0.4 value of the previous experiment. In this setup there is no accumulation of error (i.e. the failure to detect a bit does not affect the remaining data), while in the experiment with OOK modulation, the error is accumulated which explains the lower BERs achieved using intensity modulation.

Due to the slow response time of the LDR (with rising and falling times of 18 and 120 ms, respectively [9]), it is replaced by a photodiode (with only 1.5 µs rising and falling times [10]) in the new experimental demonstration which is executed to optimize the transmission speed (i.e. minimize t_b). As expected, the achievement of error-free transmission

is extended to data rates reaching 500 bps (i.e. only 2 ms bit duration) as shown in Fig. 5 which compares the BERs of all executed experiments.

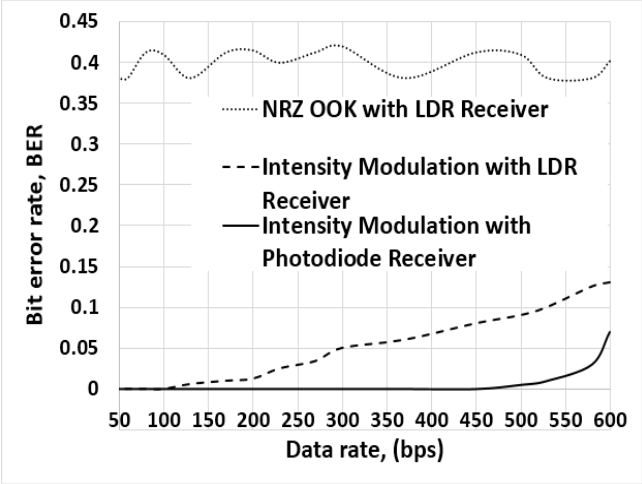

Fig. 5. Bit error rates at different transmission data rates for all executed experiments

IV. CONCLUSION

This paper practically implements a secure visible light replacement of magnetic cards using LED flashlight in smartphones and only a simple circuitry as a receiver. It has been practically proven that an OOK modulation scheme is inefficient for data reception since it is vulnerable to synchronization problems. Using a RZ light intensity modulation instead of OOK resulted in error free transmission of data rates up to 100 bps. The system operates optimally utilizing a photodiode instead of the previously used LDR as a detector, which resulted in error free data rates up to 500 bps.

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] 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

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

[5] 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.

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

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

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

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

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