Modern Applied Science; Vol. 12, No. 4; 2018
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Robot Secured Wireless Authentication Using Look-Up Table Based Coding

Mahmoud Malek Abu-A'ra[1]

[1] Philadelphia University, Amman, Jordan

Correspondence: Mahmoud Malek Abu-A'ra, Philadelphia University, Amman, Jordan. E-mail: mahmoudabuarra90@gmail.com

Received: March 1, 2018 Accepted: March 14, 2018 Online Published: March 30, 2018

doi:10.5539/mas.v12n4p193 URL: https://doi.org/10.5539/mas.v12n4p193

Abstract

Securing restricted areas is a major concern for sensitive institutes, like military or research labs. Most security measures rely on having some of the biometrics that human beings possess to identify the user and grant access permissions. Yet, with the wide spread of robotic systems and avatars, these entities need to be authenticated as well, since they might require access to such facilities, hence, the need to provide security measures that can handle non-biological entities with high levels of security and that is not vulnerable to hacking is becoming essential.

In this research we propose a novel and unique system for encoding the passcode that is known only to the authorized user using a specially designed look-up table. The system's hardware requires reconfiguring doors' security modules to have Near Field Communication (NFC) initialized inside them, and have the Robot initialized with the same hardware, and a wireless controller for the NFC will be given to the operator. The hardware has low-cost, and is easy to use since it is considered as plug and play module. XBEE was adopted as a wireless communication module between the operator and the robot in order to wirelessly connect to an NFC chip that is installed (as plug and play) on any Robotic system.

Keywords: wireless authentication, Near Field Communication (NFC), Triple DES Encyption, Encryption/decryption, XBEE network

1. Introduction

Although robots are increasing equipped with high technology integrated into them these days, they still lack to biometrics that human beings have. For example, a wireless controlled Robot working in a restricted area such as military HQ or an airport, might be required to provide biometric authentication to access areas with restricted access, and by nature; it is really hard and inefficient for the Robot to physically the access door's security module and start typing access password like a human, or provide any other biometric security authentication measure. So even if the Robot's operator (usually a human) has access to that door, the Robot has not.

Altering the security procedures imposes a great risk of being prone to hacking, or have high costs to reconfigure existing hardware or provide new hardware that is able to cope with authenticating a robot.

Robot's authentication issues have been tackled often in research; the term "artimetric" has become widely used to indicate the processes of identification, authentication, and classification of robot entities wherever they are used (Gavrilova and Yampolskiy, 2010).

To the extent of our knowledge, few research and experiments have been conducted in the field of non-biological authentication. Some researchers suggested "adding" biological features to robotic entities to make them verifiable, like the work in (Yanushkevich, 2006).

Yet both of these techniques require major changes to the robot itself and the environment it will be working in. therefore, we believe that using the current cheap, accessible, and easy to use tools and technologies with minor modifications to ensure the security of robots' interaction with secured facilities.

Near Field Communication (NFC) technology is a very efficient and widely used technique for entities communication (Mohanalakshmi and Arun, 2015). It has been used by many applications to replace holding cards for payment (Ghosh et al., 2017), card-less personal data retrieval systems (Sethia, et al., 2014), and secured peer-to-peer data transfer (Neafsey et al., 2016).

In securing robotic systems, NFC was used in a limited range of applications, like being used to secure mobile printing in the work mentioned in (Lee et al., 2015), where NFC protocol was employed to grant proper user and documents privilege that is verified by a recognition robot. Other researchers used NFC to authenticate payments done by the robot (Choi et al., 2014), where NFC protocols were combined with a Universal Subscriber Identity Module (USIM) that would provide technical (hacking attempts) and physical (robbery attempts) to the robot's payment service.

Attempts to secure robot communications were the subject of research by (Nong, 2017), where a Certificate-less signature scheme was developed to secure communication with the robot in a public network that doesn't require securing the channels themselves, only the exchanged messages, with straight forward cryptographic primitives. The authors of (Moh'd et al., 2013) preferred to decrease security computations to preserve energy, by merging security related data into one layer, and hiding the packets' headers and trailers in the system they chose to name Compact Security Protocol, or briefed as "C-Sec".

Several techniques and modules were developed to secure the transmission media and channels of the messages exchanged between robots (or robot and controller), like the research of (Champaty et al., 2016) that used XBEE and Bluetooth communication protocols to secure control of wheelchairs, others combined ATmega and XBee-Based wireless communication (Kioumars et al., 2014) for secured component-based health data gathering from databases and warehouses, and monitoring of changes done on these data.

2. System Overview

Authentication of robots is becoming an urgent issue for several applications, the proposed system in this research suggests reconfiguring doors' security modules to have an NFC adapter plugged into the door opening mechanism, while the robot (that needs to be granted authority) is also equipped with a similar adapter. The human operator, who already has access to the door, will communicate with the robot wirelessly via XBEE module. When the robot is near the authentication site, the remote operator will enter the passcode wirelessly from his/her base, where this passcode is encrypted, and transferred to the robot which will decrypt it, and then broadcast it through the NFC adapter to the nearby door, which will activate the opening mechanism should the passcode was correct.

The system consists of a cheap, specially designed hardware circuits that controls the transmission of data, authentication of robots, and security of the transmission of data itself. These hardware circuits are distributed over three main locations: the hardware at the base sender's location (where the human controller of the robot resides), the hardware that will be equipped on the robot, and the door authentication and opening mechanism.

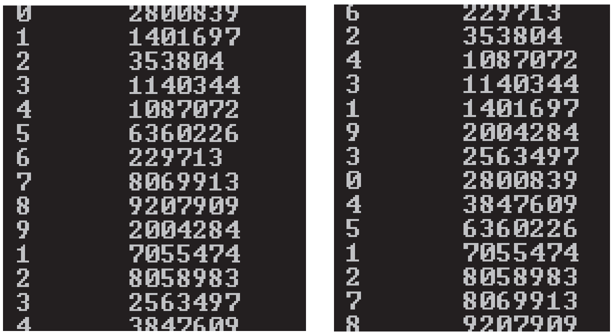
2.1 Base Sender

This part consists of an Atmel Atmega 328p controller, a 3x4 Matrix keypad, an alphanumeric 16x2 LCD screen and a wireless transmitter from type XBEE HP900 (with 28 Mile range). All of these parts cost under $20 as the suggested prices in table 1 show.

Table 1. Suggested prices for base sender's equipments

Part	Cost ($)
ATMEGA328	1.2
XBEE module	13
LCD 16x2	1.5
Potentiometer 10K	0.1
8MHz Crystal	0.1
2x 22pF capacitors	0.002
Push button	0.01
10K resistor	0.001
Keypad	0.4
2x LED	0.004
Total	16.317

A list of 32 bits' random numbers is generated (which means that the list contains hundreds of millions of records), now each of these records is given an index number of size 1 byte (index 0 to 9) to work as the original look-up table (as in figure 1-A). Then these records are sorted according to the random numbers, and the indices are moved according to their new corresponding position (as shown in figure 1-B). The original unsorted look-up table stays on the base station, while the sorted table is flashed (uploaded) to the door authentication unit, and only the column with the random and sorted 32 bit numbers is flashed to the Robot unit.



```
0    2800839
1    1401697
2    353804
3    1140344
4    1087072
5    6360226
6    229713
7    8069913
8    9207909
9    2004284
1    7055474
2    8058983
3    2563497
4    3842609
```

A

```
6    229713
2    353804
4    1087072
3    1140344
1    1401697
9    2004284
3    2563497
0    2800839
4    3847609
5    6360226
1    7055474
2    8058983
7    8069913
8    9207909
```

B

Figure 1. Randomly generate Numbers look-up tables (A: orinigal, B: Sorted)

When the authorized user (who seeks access through the secured door via the Robot) chooses a passcode, the code's digits are looked-up individually from the look-up table that is already installed on the base station. The user chooses a code combination 123 for example, the system picks a 32-bit value that corresponds to each of the chosen code's digits (in the example 1 corresponds to 1401679, 2 corresponds to 8058983, and 3 corresponds to1140344). Once a passcode is chosen, the digits (the random values from the lookup table) are inverted (from left to right) and then deleted from the table to prevent re-using them again, in case a silent attacker sniffed this passcode and tried using it on a different session.

The chosen and inverted password is encrypted using triple DES; the first digit of the code is encrypted with the first 64-bit DES key, and then this encrypted code is decrypted but using the second 64 bits' key, and a final encryption of the whole message is encrypted with the third 64-bit key, to make a total key length of 192-bit. Even with a meet-in-the-middle attack is performed, the attacker won't be able to know what the ciphered text is (because it's been manipulated before it was encrypted, and the time required for that is not enough since the keys will be deleted from the base station and the authentication site by the time the attacker decrypts the code). An overview of the process is illustrated in figure 2.

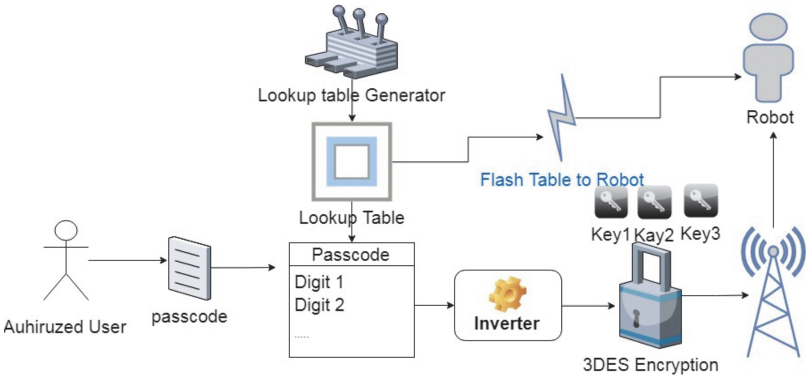


Figure 2. System Components

This encrypted password is sent wirelessly through a specified network to the Robot Receiver XBEE module (via serial number). XBEE has been chosen because of its high security through special networks and wide range of operation (28-mile model was used)

Atmel Atmega328p microcontroller has been chosen in this design because of its 32kb wide memory, and sufficient RAM and IO pins number, and its availability in small SMD size which is compatible with small designs, and of course, this microcontroller can run on an internal crystal oscillator of 8MHz on low power consumption mode which makes it even easier to deal with. Figure 3 shows hardware connection of the base sender unit.

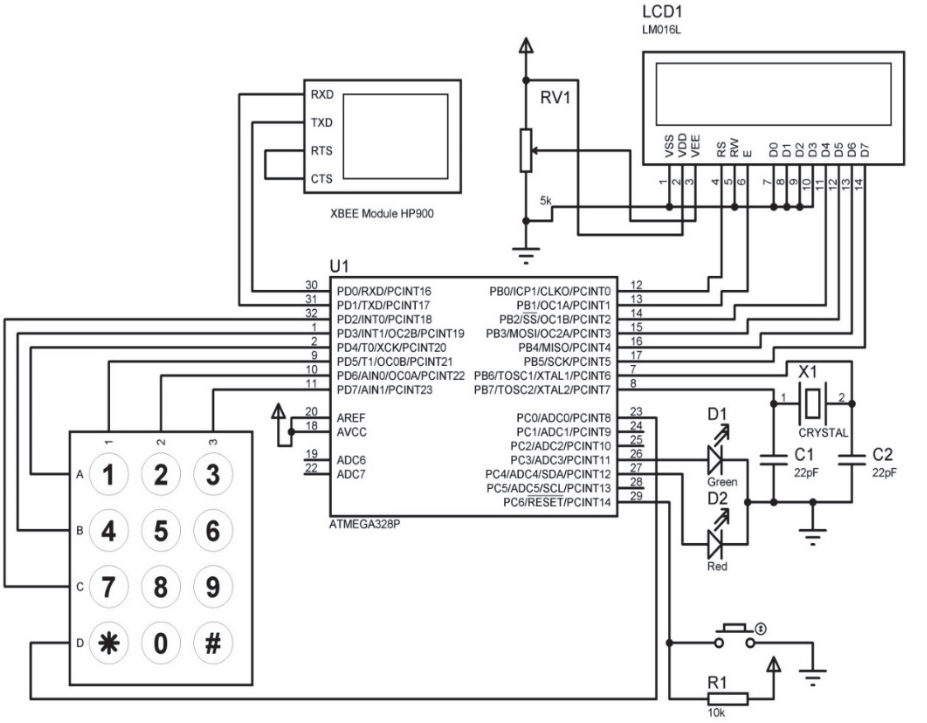


Figure 3. Base sender unit hardware design

Green LED will (shown in figure 4) turns on when the base station's unit is ready to receive a new password, while Red LED will turn on when unit is busy processing something, such as encrypting or sending operations. Figure 4 shows a prototype hardware circuit that will be installed at the sender's station.

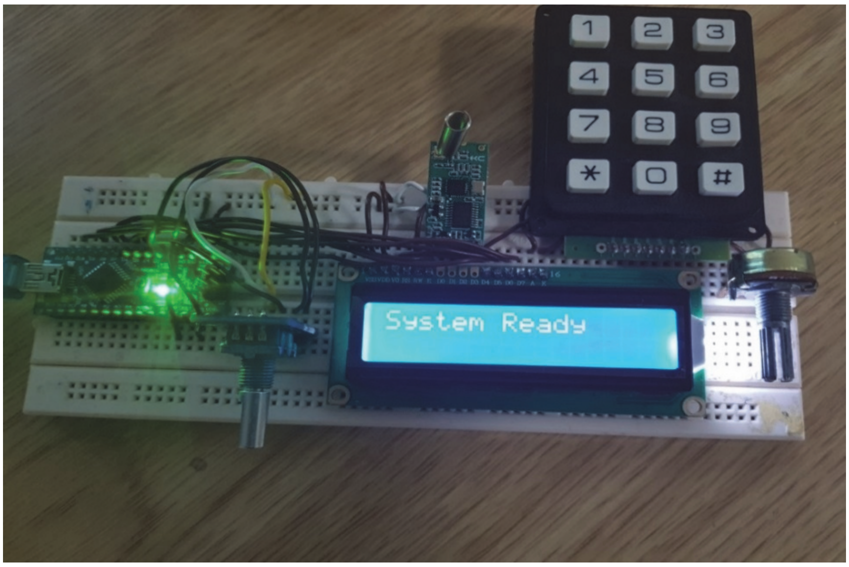


Figure 4. Base sender unit prototype

2.2 Robot Receiver

The receiving device on Robot will only work as a redirector; its main function is receiving XBEE commands from base station and redirect them as they are to authenticator. This limits taking extra security procedure to the base station and authentication site, and of course the wireless connection itself.

This part consists of Atmel ATTINY85 microcontroller unit, XBEE receiver HP900 (with 28 miles range) and an NRF module (which is an ultra-low power (ULP) circuit that has a 2Mbps Radio Frequency Transceiver Integrated Circuit) with a 1.5 meters' transmission range. Talking about cost; all of these parts would also cost less than $20 as the list of suggested prices in table 2 show, which indicates that this system is very cost efficient.

Table 2. Suggested prices for robot's equipments

Part	Cost ($)
ATTINY85	1
Push button	0.01
10K resistor	0.001
NFC	4
XBEE module	13
Total	18.011

Atmel ATTINY85 has been chosen because of its small size, yet enough IO pin count for the required type of processing of the proposed system. All of these parts are integrated with internal crystal and 8kb of memory, that facilitates the decryption process of received commands. NRF module has a range of 1.5 meters where this limited range makes sure that only the door in front of the authorized Robot will receive the signal. This provides a new security layer by not allowing hackers or wrong doors (those that do not need authorization for this robot) to catch the signal. While, high range XBEE has been chosen to add an extra secure control range between the Robot and its operator.

The unit on the robot receives the encrypted passcode from the controller at the base station, then it decrypts the received packet with the pre-loaded decryption keys, and use the loaded look-up table to search for the received code. If all received values are found in the table, the unit encrypts the data again and forwards the packets to the authentication site and immediately deletes the received numbers from the table, if not all values are found (the code has been used before), the robot does nothing and ignores the transmission.

Figure 5 shows the circuit's design, while figure 6 shows the actual hardware connection that will be equipped on the robot.

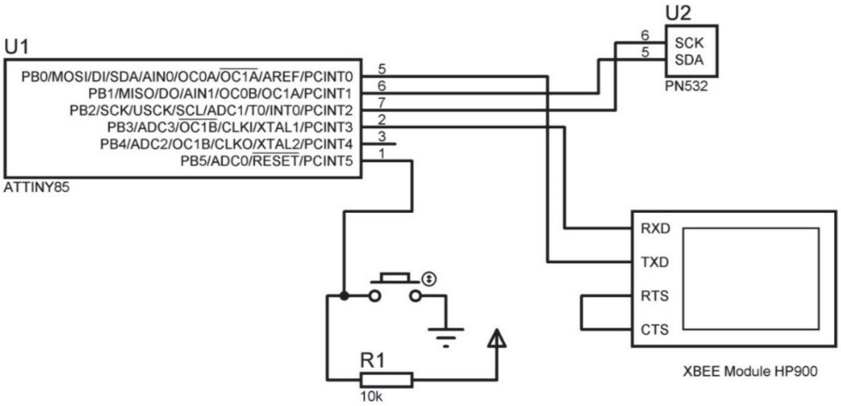

U1
PB0/MOSI/DI/SDA/AIN0/OC0A/$\overline{OC1A}$/AREF/PCINT0
PB1/MISO/DO/AIN1/OC0B/OC1A/PCINT1
PB2/SCK/USCK/SCL/ADC1/T0/INT0/PCINT2
PB3/ADC3/$\overline{OC1B}$/CLKI/XTAL1/PCINT3
PB4/ADC2/OC1B/CLKO/XTAL2/PCINT4
PB5/ADC0/$\overline{RESET}$/PCINT5
5
6
7
2
3
1
ATTINY85
U2
6
5
SCK
SDA
PN532
RXD
TXD
RTS
CTS
XBEE Module HP900
R1
10k

Figure 5. Robot receiver unit hardware connection

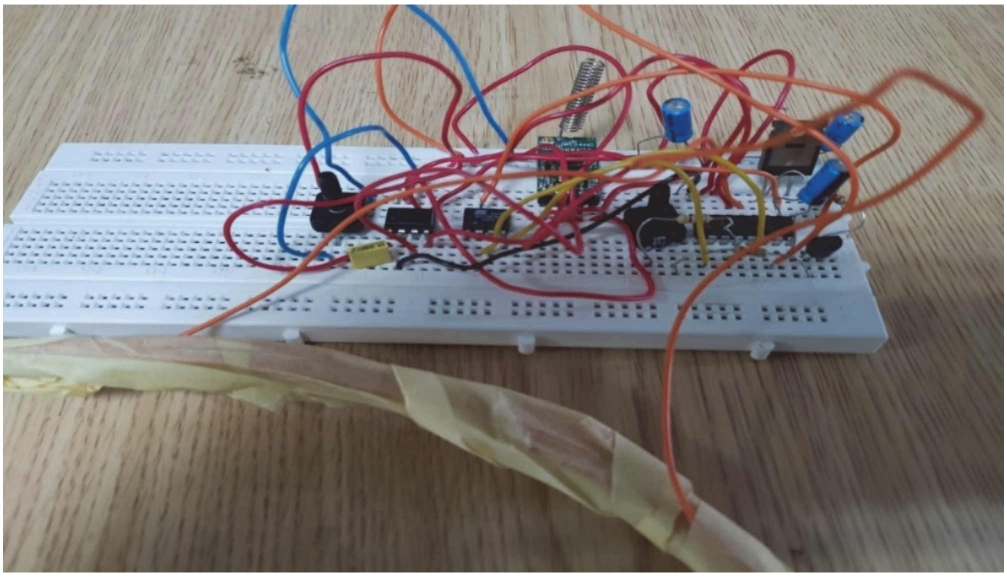


Figure 6. Robot receiver unit prototype

2.3 Door Authenticator

This unit consists of a microcontroller of type ATMEL ATMEGA328P, 16 solenoids of type "Adafruit small push/pull solenoid" and a 3x4 keypad, along with the NFC receiver among other needed transistors. All of these required hardware parts also cost less than $20 (check out table 3 for suggested market prices), yet they compose a very efficient and reliable authentication system.

Table 3. Suggested prices for authentication site's (door) equipments

Part	**Cost ($)**
ATMEGA328	1.2
8MHz Crystal	0.1
2x 22pF capacitors	0.002
Push button	0.01
8x 10K resistor	0.008
Keypad	0.4
NFC	4
8x 2n2222a transistors	0.08
12x solenoid	12
Total	**17.8**

The receiver at the authentication door decrypts the receive code, and check the match the values with those in the pre-loaded look-up table to get the correct code sequence. These entries from the table are immediately deleted for extra security, and the received code is reverted back to its correct order. The resulting code is forwarded to actuators to press them physically on the keypad. The next steps are illustrated in the flowchart in figure 7.

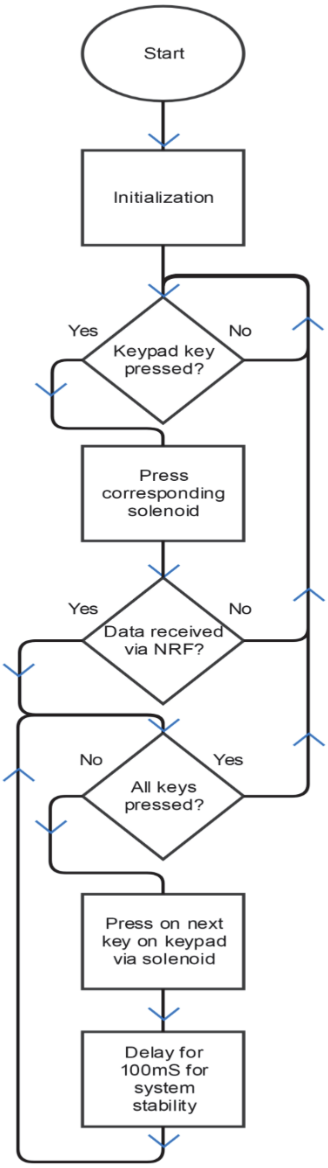

Start
Initialization
Yes
No
Keypad key pressed?
Press corresponding solenoid
Yes
No
Data received via NRF?
No
Yes
All keys pressed?
Press on next key on keypad via solenoid
Delay for 100mS for system stability

Figure 7. Door authenticator unit flowchart after decrypting passcode

To save IO pins on microcontroller and assure reliability, solenoids are connected as a matrix, as shown in the circuit design in figure 8. Because only one solenoid will be active at a time, the microcontroller can map needed solenoid using seven pins only (for example, if row 1 and column 2 are activated, then solenoid 2 (refer to figure 8) will be activated).

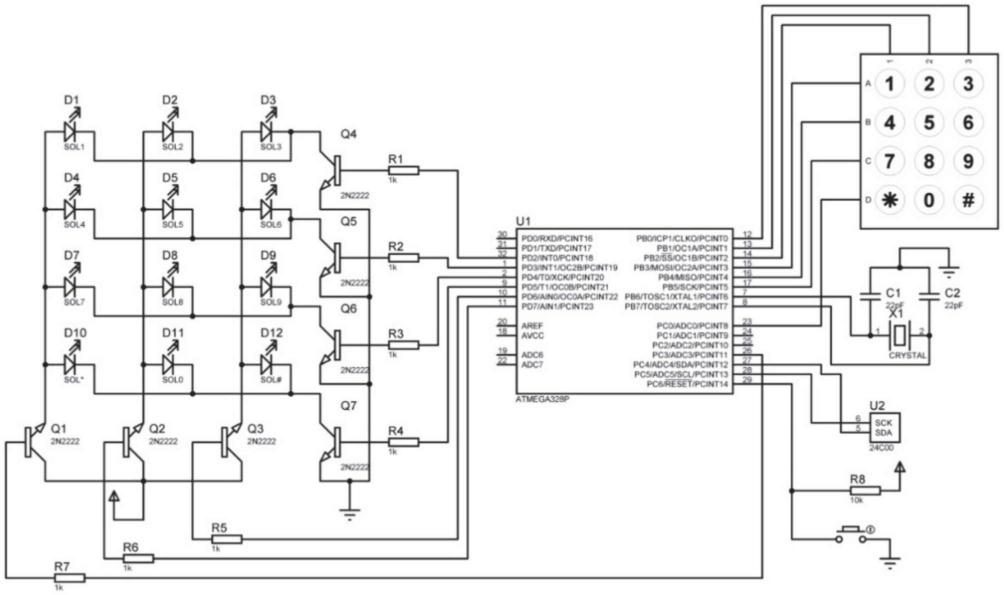


Figure 8. Door authenticator unit hardware

The microcontroller is also connected to a keypad for manual access (when a human user personally wants to get access), so when an authorized user presses on microcontroller's keypad, the corresponding solenoid under the system will be activated, simulating an actual press on the selected button. Yet, if a Robot is authorized (has the passcode sent to it) it transmits the decrypted passcode via NFC, and the microcontroller simulates a key press of corresponding buttons by activating solenoids. The system can be used by either a robot or a human user, where the parts are integrated to facilitate both options, and makes it an easy to adapt plug-and-play authorization system. Figure 9 shows the prototype design of the hardware unit at the door site.

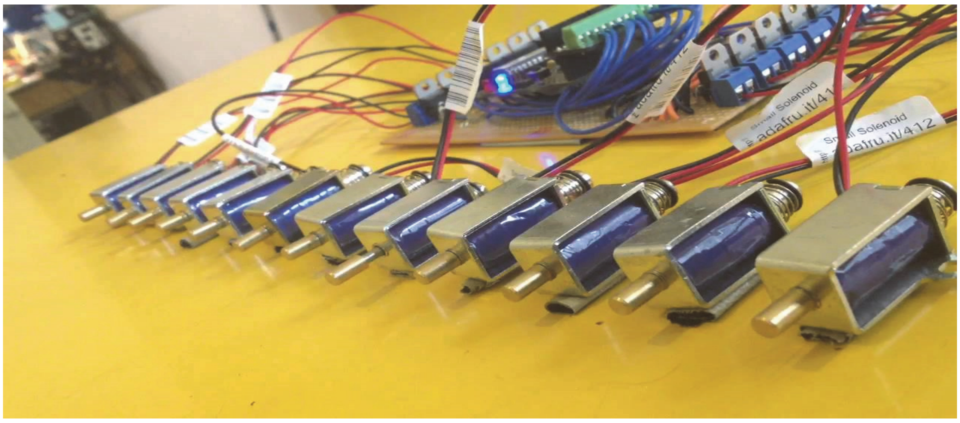


Figure 9. Door authenticator prototype

3. System Performance Testing Results

The proposed system was coded via Atmel studio and connected to actual Chinese made door access system. The system provided stable and reliable response over a wide range of 320 meters within an indoor environment.

Delivery ratio of transmitted packets was very high, with an average 98% successful packets delivery, over a transmission period of 60 minutes. Compared to other systems, like the one developed in (Moh'd et al., 2013), where the success ratio scored around 95% over the same period of time. The system developed in (Moh'd et al., 2013) was based on merging security related data of consecutive packets to minimize power consumption in WSN. This technique has a low security level, and not yet very efficient in packet success ratio. The chart in figure 10 shows the difference in packet delivery performance for the proposed system against the C-Sec system proposed in (Moh'd et al., 2013).

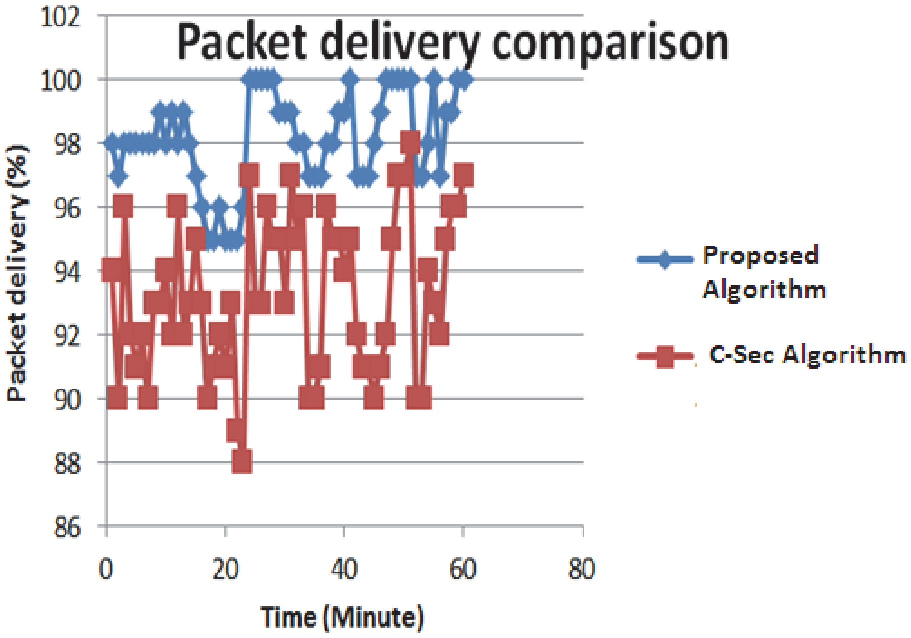


Figure 10. packet delivery performance for proposed system and C-Sec system (Moh'd et al., 2013)

One of the closest systems that we were able to find that has similarities in concepts and applications to the one proposed in this research was the one studied in (Cho et al., 2011). Their proposed system depended on having Radio Frequency IDentification (RFID) initiate a hash-based mutual authentication protocol that has a similar manipulation technique to the one proposed in this research.

Yet; comparing the technique used in (Cho et al., 2011) with the one proposed in this research using a small segment of encrypted data. Both algorithms were tested against a brute force attack that was built under Linux OS in attempt to decode the sent data packet. Brute force attacks have been activated on IMAN Jordanian supercomputer system (Note 1) (using 18000 processors). The technique in (Cho et al., 2011) took about three times the amount of time taken to decode the same data packet against that for the proposed algorithm. The chart in figure 11 plots success attempts of decoding a packet against time.

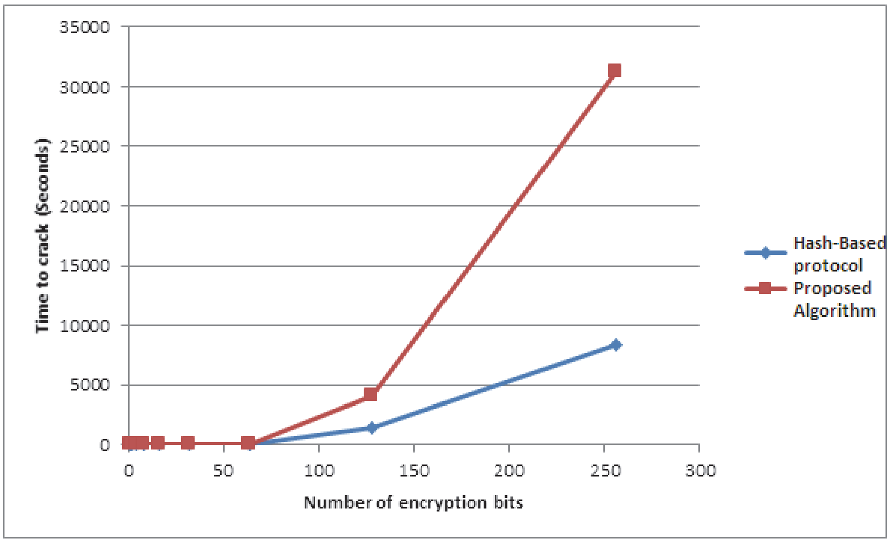


Figure 11. Brute force decoding performance for proposed system against Hash-Based Security System (Cho et al., 2011)

When the encrypted message was coded with a 512bit encryption, the attack was a total failure for both techniques, yet; based on the values and the exponential relationship depicted by the test results, we believe that the proposed algorithm would be even harder to break than the hash-based protocol proposed in (Cho et al., 2011). As the number of bits used in encrypting the passcode increases, the time required to decrypt it increases exponentially, testing the technique for a 1024bit encrypted data on an 18000 multi-processor super computer took 21 days (note that such a computer is not used by a hacker; hence; decrypting the passcode with the best computer hackers possess would take much more time). A comparison in number between the proposed algorithm and the one proposed in (Cho et al., 2011) is shown in table 4.

Table 4. Comparing time required to decrypt data between proposed algorithm and the hash-based

	Time to crack the code (in seconds)	
Number of encryption bits	Hash-based protocol (Cho et al., 2011)	Proposed algorithm
1	0	0
2	0	0
4	0	0
8	0	0
16	0	0
32	1	1
64	2	2
128	15	16
256	894	1807
512	3815	9107
1024	12405	28711

The test results prove that this simple plug-and-play system is highly secured and can be used in authentication of robots to access doors under the supervision of their operators, as well as the human user him/herself. The security of the data that is being transmitted is guaranteed through the strong encryption technique that was encapsulated within the system.

4. Conclusion and Future Work

This research presented a secured system that allows remotely controlled robots to open doors that are secured with a passcode. Simple plug-and-play alteration to the door's hardware along with simple adapters on the robot were implemented to allow the controller of the robot give permission to the robot to access such doors.

A unique and novel encryption technique was presented that prove the very high level of security this technique has with low computational requirements. Carrying out hacking attempts using brute force attacks, along with attacks on the transmitted passcode and robot commands showed that the time required is too long for a hacker, and even if time was not an issue for the hacker, the fact that this system changes the passcode with every transmission makes a successful hacking useless, even when working on a supercomputer.

The cost of this system is considered very low, and would be even lower if mass produced. The prices suggested by parts vendors did not exceed $100 for all three modules (the base-station, the robot, and the authentication site's door), which makes this system feasible, in addition to being highly secured and reliable.

References

Champaty, B., Nayak, S. K., Thakur, G., Mohapatra, B., Tibarewala, D. N., & Pal, K. (2016). Development of Bluetooth, Xbee, and Wi-Fi-Based Wireless Control Systems for Controlling Electric-Powered Robotic Vehicle Wheelchair Prototype. In Classification and Clustering in Biomedical Signal Processing (pp. 356-387). IGI Global. https://doi.org/10.4018/978-1-5225-0140-4.ch015

Cho, J. S., Yeo, S. S., & Kim, S. K. (2011). Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. *Computer communications, 34*(3), 391-7. https://doi.org/10.1016/j.comcom.2010.02.029

Choi, O., Choi, T., Kim, J., & Moon, S. (2014). NFC Payment Authentication Protocol for Payment Agency of Service Robot. In Future Information Technology (pp. 65-70). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-55038-6_10

Gavrilova, M. L., & Yampolskiy, R. V. (2010). State-of-the-Art in Robot Authentication [From the Guest

Editors]. *IEEE Robotics & Automation Magazine, 17*(4), 23-24. https://doi.org/10.1109/MRA.2010.938838

Ghosh, S., Majumder, A., Goswami, J., Kumar, A., Mohanty, S. P., & Bhattacharyya, B. K. (2017). Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment. *IEEE Consumer Electronics Magazine, 6*(1), 82-93. https://doi.org/10.1109/MCE.2016.2614522

Kioumars, A. H., & Tang, L. (2014). Wireless component-based health data acquisition and monitoring system. In Industrial Electronics and Applications (ICIEA), 2014 IEEE 9th Conference on (pp. 1567-1572). IEEE. https://doi.org/10.1109/ICIEA.2014.6931418

Lee, E., Yeh, H., Yang, H. S., Moon, S., & Choi, O. (2015). A secure NFC-based mobile printing service using recognition robot. *International Journal of Distributed Sensor Networks, 11*(9), 564506. https://doi.org/10.1155/2015/564506

Moh'd, A., Aslam, N., Phillips, W., & Robertson, W. (2013). A dual-mode energy efficient encryption protocol for wireless sensor networks. *Ad Hoc Networks, 11*(8), 2588-604. https://doi.org/10.1016/j.adhoc.2013.07.006

Mohanalakshmi, K., & Arun, B. (2015). NFC Signals Based on an Effective Mobile Robot Localization. *Elysium J, 2,* 1-5.

Neafsey, J. S., Malone, M. W., & Abouhashem, H. (2016). System and method for NFC peer-to-peer authentication and secure data transfer. U.S. Patent No. 9,307,403. Washington, DC: U.S. Patent and Trademark Office.

Nong, Q. (2017). Practical Secure Certificateless Cryptographic Protocol with Batch Verification for Intelligent Robot Authentication. In International Conference on Mechatronics and Intelligent Robotics (pp. 483-488). Springer, Cham. https://doi.org/10.1007/978-3-319-65978-7_73

Sethia, D., Gupta, D., Mittal, T., Arora, U., & Saran, H. (2014). NFC based secure mobile healthcare system. In Communication Systems and Networks (COMSNETS), 2014 Sixth International Conference on (pp. 1-6). IEEE. https://doi.org/10.1109/COMSNETS.2014.6734919

Yanushkevich, S. N. (2006). Synthetic biometrics: a survey. In Neural Networks, 2006. IJCNN'06. International Joint Conference on (pp. 676-683). IEEE. https://doi.org/10.1109/IJCNN.2006.246749

Note

Note 1. Technical information are available online through: http://www.iman1.jo/iman1/

Copyrights