Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.431 – 444

Survey- Secured Data Transmission from WBAN to Sink

A.Subbarayadu[1], G.R.Radhika[2], R.Vedhavathi[3]

Assistant Professor, Dept. of IT, Prathyusha Engineering College, India

Student, Dept. of IT, Prathyusha Engineering College, India

Student, Dept. of IT, Prathyusha Engineering College, India

ABSTRACT: ***Wireless body area network (WBAN's) consisting of small sensing and computing devices can help to improve medical care and well-being of humans. Obviously, the data recorded in WBANs such as vital parameters are personal and should be private. To protect this privacy, such data are usually encrypted when transmitting it over a wireless link. In the past, many cryptographic algorithms and methods for the encryption and decryption of data have been proposed and most of them have become obsolete. In this paper, we are protecting a wireless body area network (WBAN) by implementing OTP whereas mathematically proven to be secure and impossible to crack. But, for most purposes OTP's are complicated to handle, because if applied correctly, for each bit of plain text data, another bit of OTP must be available. Thus, numerous OTP's can be pre-installed on WBAN devices and ensure a long lasting and secure data transmission. It gives more secure privacy on WBAN data's using windows 10 IOT core and Rapberry PI sensor kit.***

Keywords-- Wireless body area networks(WBANs), encryption, One-time pad(OTP), privacy, security, wireless sensor networks(WSNs), healthcare, protocols, wearable sensor node, online monitoring, medical sensors.

I. INTRODUCTION

In most wireless sensor network (WSN) scenario, data are gathered by wireless sensor nodes and transmitted wirelessly to a sink or stored within the network. In wildlife monitoring or similar scenario, it may be uncritical to transfer data unencrypted and in plain text-as normally any third parties are not interested in such data, but in many other scenario, there is a demand for

© 2016, IJCSMC All Rights Reserved

reliable and secure data transmission. Health insurance may be interested in your heart rate, thieves may be interested in your outdoor activity data or potential sexual partners may be interested in your fertility. Here, the data is stored on a micro SD card and processed after the recording, the data is continuously transmitted via a wireless link to a processing personal computer (PC) and analyzed in real time.DTN protocols are designed to handle such harsh circumstances and to provide a reliable and secure communication where conventional protocol would fail. This is achieved by a dependable multi-hop communication (i.e) wireless networks use two or more wireless hops to convey information from a source to a destination.

In the past, many cryptographic algorithms and methods for the encryption and decryption of data have been proposed and most of them have become obsolete. History shows that nearly every algorithm proposed for cryptography get cracked overtime. Thus, any of these encryption is only secure for a certain time.

In fact, most of the previously proposed once secure and insuperable cryptographic methods have either been hacked because of a fault-prone design, or can be successfully attacked with just enough computation power, nowadays. If not by now, then surely in the near future with brute force. The generally practiced way to handle this fact is to continuously enlarge the key length of implemented. Ciphers or to "exchange" cryptography algorithms. But in WBAN's , this not always easily possible.

We present a best secure pad exchange approaches after the OTP's have been created by an adequate random number generator. The recorded raw data is discrete encrypted and transmitted to a sink. All available memory can be pre-filled with OTP's and the used OTP's can be freed. If the encrypted data cannot be transmitted immediately, it can be stored on the node. Online encryption of the recorded sensor data is performed. Therefore, the encrypted data can be stored in place. All the nodes available storage capacity could be equipped with OTP's in advance. With growing data, the number of available and usable OTP decreases and its place is taken by the encrypted raw data. The unencrypted data must stay available for processing.

We implement our project in the current newest windows 10 IOT Technology. We are going to explore our project as a windows universal application in more efficient way and outstanding performance with raspberry pi kit.

II. METHODALOGY

2.1 DISRUPTION TOLERANT NETWORK PROTOCOL

It provides seamless handover between online and offline monitoring of activity data or vital parameters. These can be implemented in medical sensors and application .It can be implemented in wireless sensor nodes. It is a bundle protocol implementation for WSNs(Wireless Sensor Node). Implementing DTN protocol for WSNs called µDTN. The capability of a DTN protocol depends on the generated data rate of the used sensors and on

© 2016, IJCSMC All Rights Reserved

the achievable payload data rate of the wireless communication channel. Implementation is done in Linux operation system .It performs the online fall detection and loss of data is avoided by DTN protocol.

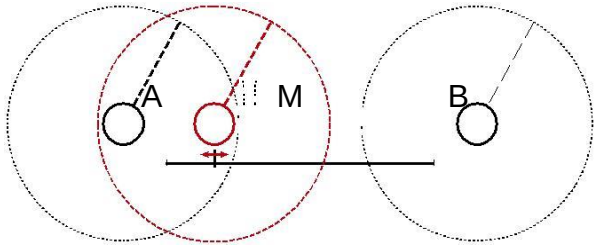


Figure 1. Node M moves between the communication radii of nodes A and B. In a DTN node M stores, carries and forwards the data.

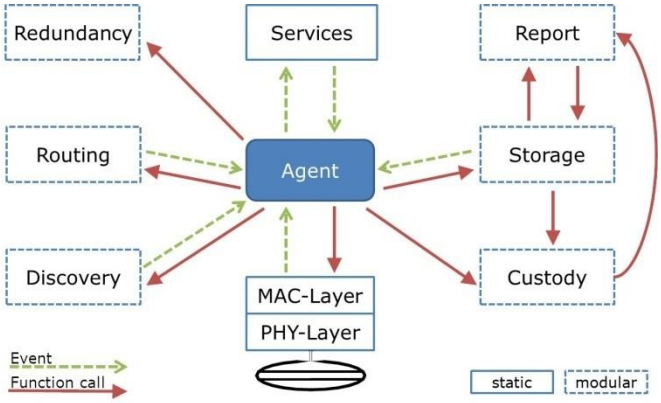


Figure 2. Block diagram of DTNs architecture

These causes the bottleneck of the error-prone serial communication between receiving node and base station.

2.2 AES IMPLEMENTATIONS

Encryption is essential in many WSN applications. Several encryption frameworks exist which are mostly based on software algorithms. However, nearly every up-to-date radio transceiver chip is equipped with an integrated hardware encryption engine. It shows utilizing an integrated hardware encryption engine in comparison to pure software-based solutions One of the major challenges for encryption in WSNs is the limited computational power of common wireless sensor nodes.AES was the opportunity to run it even on weak processors, therefore, it is surely possible to implement AES on such microcontrollers. Most of the current available radio transmitters have an integrated hardware AES unit. These units can usually be addressed by

© 2016, IJCSMC All Rights Reserved

special registers via SPI bus. When using an operating system like Contiki or TinyOS, the corresponding hardware drivers have to be implemented.

2.3 MESH ROUTING

Mesh routing protocol is based on AODV. System develops must adopt their application and systems to accommodates a wide range of underlying protocols and mechanisms. Each node keeps a list of destination node addresses together with the address of the next hop node. To setup a routing path through a network, the protocol floods the network with route request packet, it sets up a background path to the sender of the route request ,and rebroadcasts the route request towards other neighbours If a node receives a route request for its own address, the node sends or route reply packet back to the sender of the route request. Data packets are sent using multi-hop unicast.

The Rime implementation of the mesh routing protocol uses the network flooding primitive(nf) to send route request to the entire network and the best effort multi-hop forwarding primitive(mh) to send multi-hop unicasts.

Zig-bee specifies how applications can be constructed by requiring a pre-defined application profiles along with associated commands, called clusters, for all nodes in the network. Zigbee supports mesh routing protocol based on AODV.

In this case, there are high chances of redundancy in many of the network connections and overall cost of this network is way too high as compared to other network topologies. Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

2.4 CHAMELEON ARCHITECTURE

The chameleon architecture is an adaptive communication architecture for sensor networks. The purpose of architecture is threefold. First, the architecture is designed to simplify the implementation of sensor network communication protocols. This is done through the use of the Rime protocol stack. Second, the architecture allows for sensor network protocols that are implemented on top of the architecture to take advantage of the features of underlying MAC and link layer protocols. This is done by using packet attributes instead of packet headers. Third , the architecture allows for the packet headers of outgoing packets to be formed independently of the protocols or application running within the architecture.

This architecture is a communication architecture for sensor network. This architecture is expressive enough to accommodate typical sensor network protocols. Measurements show that the increase in execution time over a non-adaptive architecture is small.

It overcomes the problem of memory footprint and decreases the execution time. Thus an adaptive communication architecture such as chameleon can be efficiently used for wireless sensor network.

© 2016, IJCSMC All Rights Reserved

III. EXPLANATION

3.1 OTP STORAGE IN NODE:

OTP was considered to be an optimal solution for secure data transmission between webserver to web client the fill level of OTPs decreases over time. When the node is not worn-the OTP storage can be filled up again.

After the OTPs have been created by an adequate random number generator. One copy has to be stored on the base station and another copy has to be transferred to the node.

The recorded data is directly encrypted and transmitted to a sink all available memory can be prefilled with OTPs and the used OTPs can either be marked as used or be deleted and the memory can be freed.

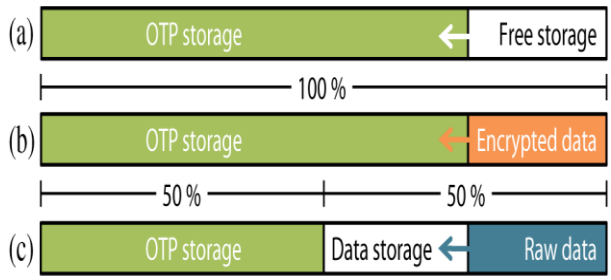


Figure. 3. (a) Storage utilization of the node at immediate transmission. (b) Direct encryption. (c) Deferred encryption in the worst case.

3.2 DATA RATES IN APPLICATION SCENARIO

It can be stated that OTs are secure for all time and due to the enormous capacity of memory and the comparatively low data rates in WBANs, OTPs can be utilized to guarantee a secure transmission of confident data.

MINIMUM, MAXIMUM, AND TYPICAL DATA RATES OF EXEMPLARY SENSORS IN WBANS

Sensor	D_{min}	D_{max}	D_{typ}
Accelerometer	3 bit/s	124 800 bit/s	1500 bit/s
Gyroscope	4800 bit/s	38 400 bit/s	9600 bit/s
Pressure and temperature	35 bit/s	4392 bit/s	70 bit/s
Heart rate	8 bit/s	32 bit/s	16 bit/s
ECG	800 bit/s	96 000 bit/s	8400 bit/s

3.3 CREATE OWN WEB SERVER

Develop an Http web server for a web service. A Web server is a system that delivers content or services to end users over the Internet. A Web server consists of a physical server, server operating system (OS) and software used to facilitate HTTP communication. A Web server is also known as an Internet server.

© 2016, IJCSMC All Rights Reserved

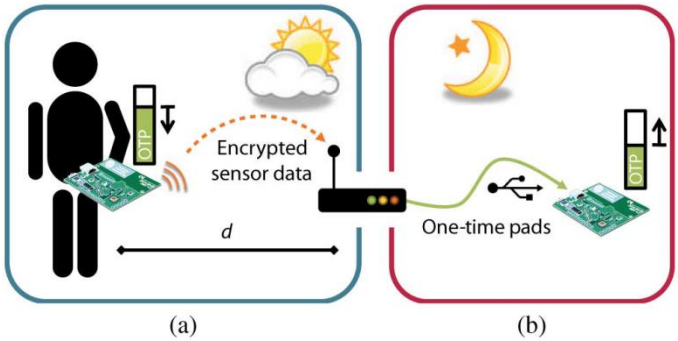
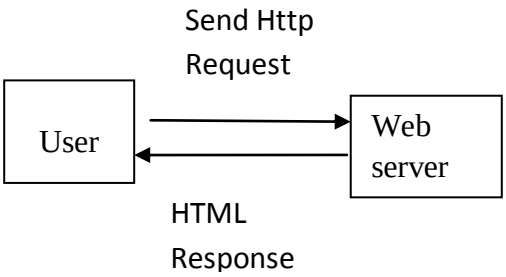


Figure. 4. System design for securing data transmission in WBANs (a) and charging new OTPs (b) on the wireless node.

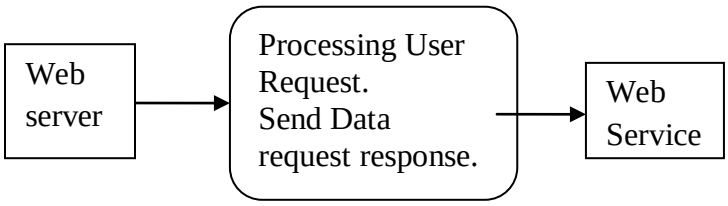
Level 0:



3.4 CREATE OWN WEB SERVICES

A Web service is a method of communication between two electronic devices over a network. In WSN we are used web service for OTP secure data transmission. All the methods and logics are done here. Finally the web methods of web services are run in web server, it was already developed. User sent a request from web browser to web server and web server will call the corresponding web methods. The web methods execute result with sensor network.

Level 1:



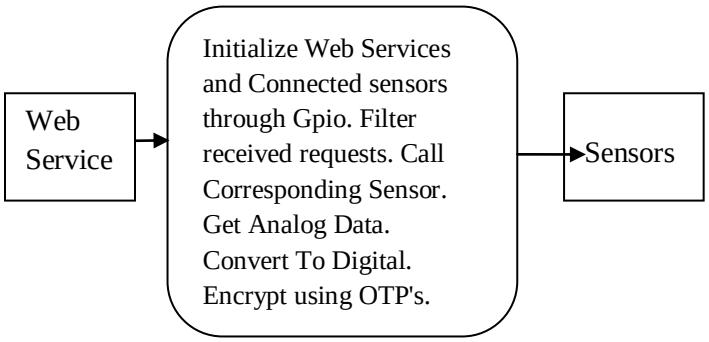
3.5 OTP AND SECURE DATA TRANSMISSION ON IoT

The system design for the usage of OTPs for securing WBAN data transmission is illustrated in system Architecture. In contrast to the above-mentioned for all time preinstalled OTPs, here we also provide the possibility to recharge a nodes' OTPs. A node of a WBAN records data, encrypts the raw sensor data with according OTPs Therefore, the node has to be

© 2016, IJCSMC All Rights Reserved

physically connected to the sink e.g., via a universal serial bus (USB) cable—which can do both, charge energy and charge OTPs.

Level 2:



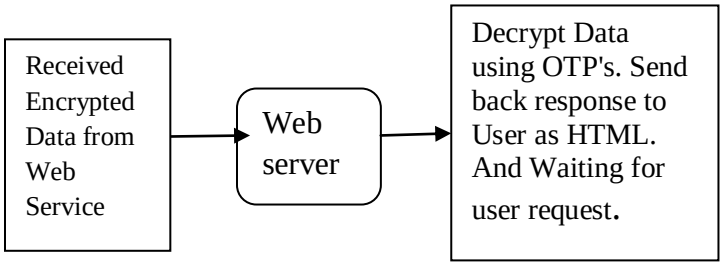
In the past, many successful attacks to cryptography systems could be performed because of an insufficiently implemented random number generator. In this case, the random number generator did not deliver real random numbers, but only a small subset of known numbers this decreased the solution space significantly. Having really random numbers it is essential for our proposed system.

After the OTPs have been created by an adequate random number generator, one copy has to be stored on the base station and another copy has to be transferred to the node. Thus, to be able to (re)charge OTPs to a node, a secure channel has to be used. Securing the transmission of new OTPs with existing OTPs would not make much sense, as both will have the same length and nothing is gained. Thus, shielded wired connections are the means of choice. Whenever a node is connected to the base station, new OTPs can be transferred. A USB connection, therefore, could be used to simultaneously charge the battery and the OTPs. We have to consider three different scenarios for the memory usage of OTP encryption on wireless nodes. The recorded raw data is directly encrypted and transmitted to a sink. All available memory can be profiled with OTPs and the used OTPs can either be marked as used or be deleted and the memory can be freed. If the encrypted data cannot be transmitted immediately, it can be stored on the node. Online encryption of the recorded sensor data is performed.

When anyway using an external storage, nearly no overhead in RAM and ROM usage is evoked. Additionally, the achievable payload of the transport protocol is not influenced. Thus, a reliable, disruption tolerant, transparent, resource efficient, and secure data transmission can be achieved by using OTPs.

© 2016, IJCSMC All Rights Reserved

Level 3:



IV. CONCLUSION

With OTPs, we can protect the wireless transmission of personal data and guarantee its security. The proposed implemented and evaluated system is able to recharge OTPs of WBAN nodes and therefore allows for a secure and persistent monitoring of confidential data. The capacity of memories available now is sufficient to store an enormous amount of pre-generated OTPs and by this to secure data transmission for a long time. Surely depending on the generated data rate. The DTN transmission leads to a stable data transmission with no packet loss.

When anyway using an external storage, nearly no overhead in RAM and ROM usage is evoked. Thus, a reliable, disruption tolerant, transparent, resource-efficient and secure data transmission can be achieved. Numerous OTPs can be pre-installed on WBAN devices and ensure a long lasting and secure data transmission.

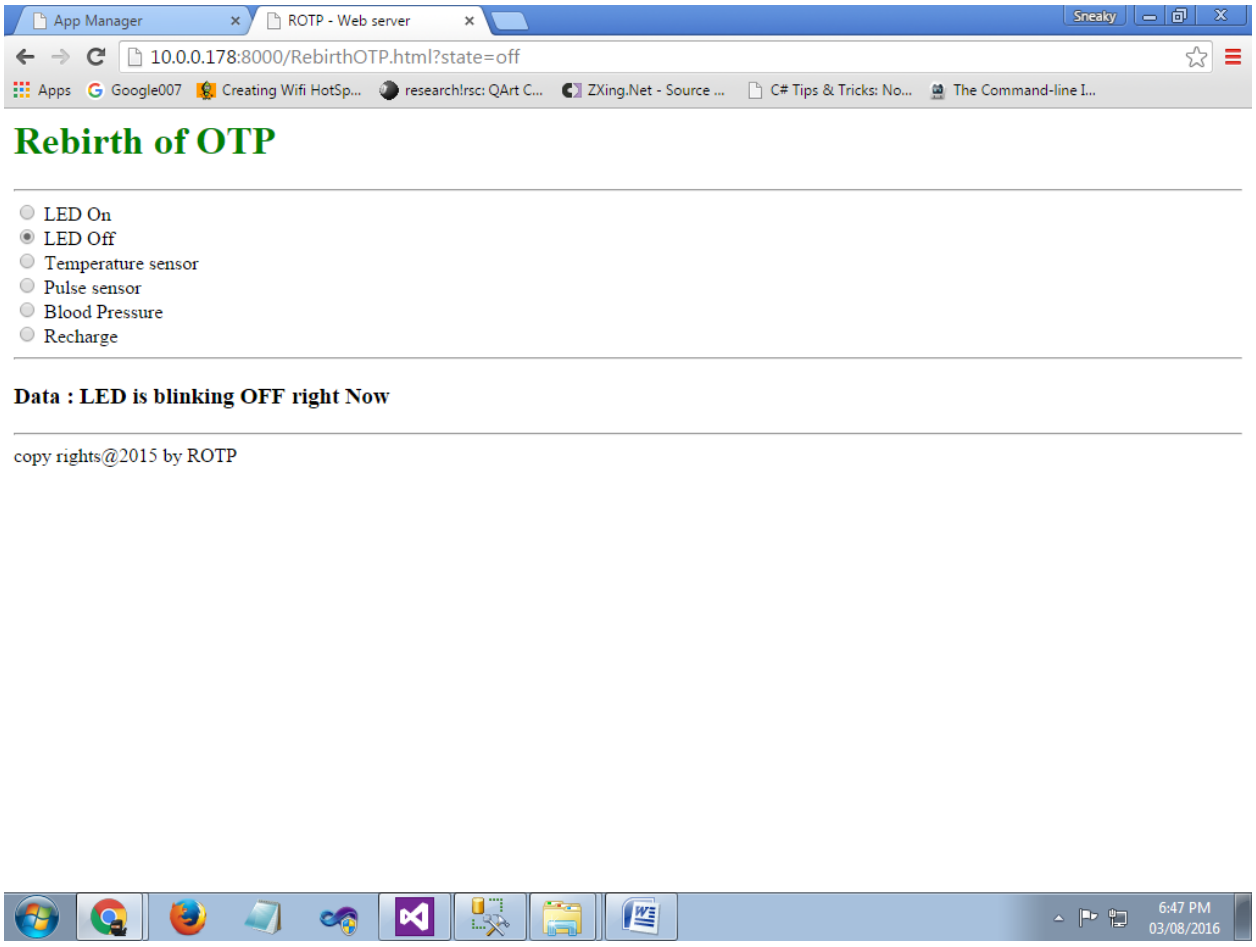
It gives more secure on WBAN datas using windows 10 IOT core and raspberry PI sensor kit

© 2016, IJCSMC All Rights Reserved

APPENDICES:

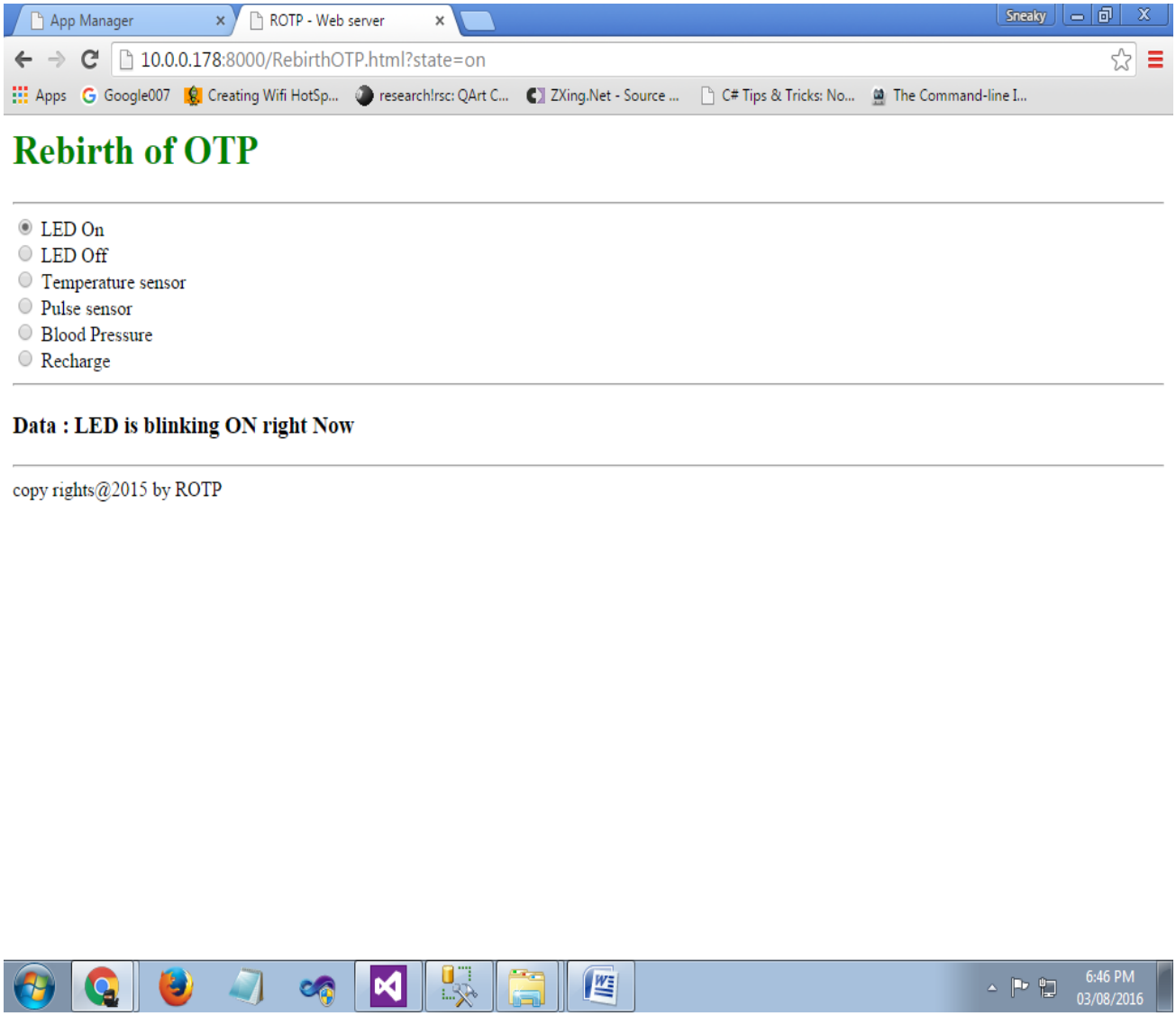
SCREENSHOTS:

LED OFF



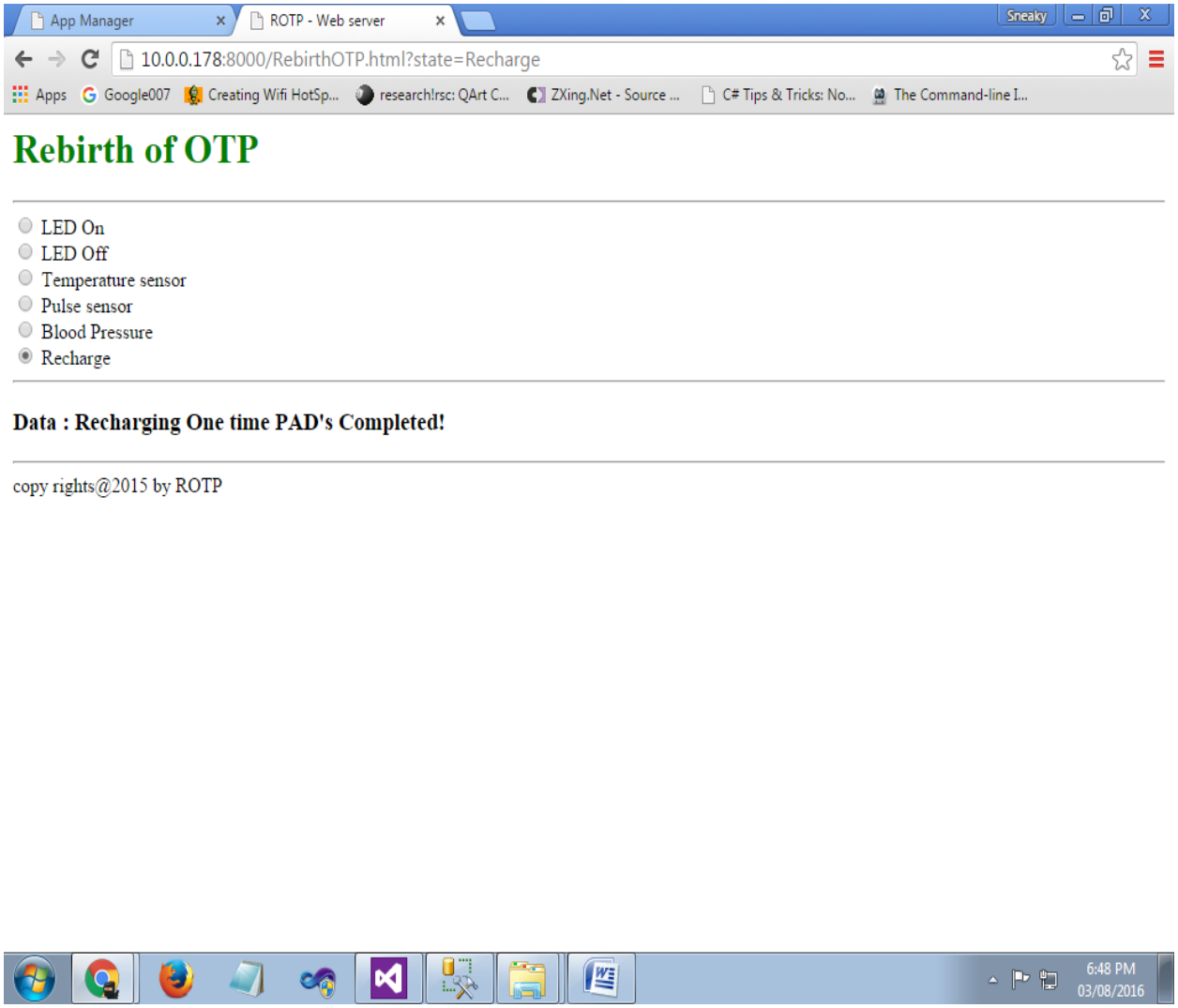
© 2016, IJCSMC All Rights Reserved

LED ON:



© 2016, IJCSMC All Rights Reserved

RECHARGE:



© 2016, IJCSMC All Rights Reserved

TEMPER SENSOR:

© 2016, IJCSMC All Rights Reserved

PULSE SENSOR:

REFERENCES

[1] F. Büsching, M. Bottazzi, W.-B. Pöttner, and L. Wolf, "DT-WBAN:Disruption tolerant wireless body area networks in healthcare applications," in *Proc. Int. Workshop e-Health Pervasive Wireless Appl. Serv. (eHPWAS'13)*, Lyon, France, Oct. 2013, pp. 196–203.

[2] F. Büsching, A. Figur, D. Schürmann, and L. Wolf, "Poster: Utilizing hardware AES encryption for WSNs," in *Proc. 10th Eur. Conf. Wireless Sensor Netw.*, Feb. 2013, pp. 33–36 [Online]. Available: http://www.ibr. cs.tu-bs.de/papers/buesching-ewsn2013.pdf

[3] A. Dunkels, F. Österlind, and Z. He, "An adaptive communication architecture for wireless sensor networks," in *Proc. 5th Int. Conf. Embedded Netw. Sensor Syst.*, 2007, pp. 335–349 [Online]. Available: http://doi.acm. org/10.1145/1322263.1322295

© 2016, IJCSMC All Rights Reserved

[4] L. Casado and P. Tsigas, "ContikiSec: A secure network layer for wireless sensor networks under the Contiki Operating System," in *Proc. 14th Nordic Conf. Secure IT Syst. Identity Privacy Internet Age*, Berlin, Germany, 2009, pp. 133–147.

[5] V. Gupta *et al.*, "Sizzle: A standards-based end-to-end security architecture for the embedded Internet," in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun.*, 2005, pp. 247–256.

[6] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst.*, 2004, pp. 162–175.

© 2016, IJCSMC All Rights Reserved