Simple & Secure Wi-Fi Configuration for Internet of Things

Jia Xu

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2013-89
http://www.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-89.html

May 17, 2013

Simple & Secure Wi-Fi Configuration for Internet of Things

By Jia Xu

A Thesis

Required For the Degree of Master of Engineer

In Electrical and Electronics Engineering

Of University of California, Berkeley

Spring 2013

ABSTRACT

This paper introduces a secure and simple way to set up initial Wi-Fi configuration for “Internet of Things” based on Wi-Fi Protected Setup (WPS) protocol. The “Internet of Things”(IoT) refers to any electronics appliances that can be connected to the local Internet with an embedded Wi-Fi chip. To accomplish this configuration, the basic concept is to transfer PIN number, which is a unique number for each device, to smartphones by using out-of-band signal and extract it based on computer vision technology with a developed Android App. After that, the PIN number will be sent from smartphone to the Access Point (AP) to finish the process of adding the IoT device to the local network. The benefits of the project is that the physical signal transmission improves the security level as well as saves people’s effort to enter any PIN number or passwords to set up a new Wi-Fi enabled device.

To implement Wi-Fi configuration based on WPS, a crucial step is to accomplish credential transfer. In this project, uplink credential transfer is applied due to its high system efficiency and cost-effective installation. Besides, some encode methods for out-of-band signal are applied to improve the reliability of signal transmission, which is an initial part of the credential transfer. According to the testing result, PIN number can be recovered successfully under a dim environment, which indicates the practicality of the communication protocol. Finally the factors that influence the decode quality is

discussed and several solutions are proposed.

Key Words: Internet of Things, Wi-Fi configuration, WPS, uplink

1. INTRODUCTION

As an integrated part of the future Internet, the Internet of Things (IoT) has gained more and more public attention. The term of Internet of Things means any electronic appliance that can be identified and inventoried over the Internet. Due to the technology of Internet of Things, physical objects can be integrated into the Internet and become participants in the network. These days, many products connect IoT devices to the local Internet by using Wi-Fi. However, it is essential to enter passwords to set up initial Wi-Fi connections for IoT. The goal of this project is to accomplish this process without requiring users to type in any password. This goal presents reliability and security issues that must be taken into account when designing both the hardware and software components of the system.

A crucial issue taken into consideration in the paper is security. Due to the development of Internet of Things (IoT), each physical object might have a unique virtual representation on the Internet in the future. This would make it possible to have an electronic map on a smartphone that shows the position and status of every appliance in a house. Thus, it is extremely important to improve the security of the Internet of Things in case users' private information is let

out.

Additional, reliable signal transmission and processing during the process of setting up initial Wi-Fi configuration is key to a good customer experience. In the proposed design, users hold smartphones to record a video of the LED lights that are attached to the IoT devices in order to decode the PIN number. Decoding the PIN number might fail due to environmental changes or hand shaking, etc. In that case, users need to hold the smartphones for a longer time or start over to accomplish the Wi-Fi configuration. If the influence of external variables to the decoding process can be eliminated to the minimum, it is more likely to get the PIN number in an accurate and efficient way that can enormously reduce the wasting time due to decoding error. Thus, improving the reliability of signal transmission and processing can significantly increase the practicality of the proposed technology by promoting users' experience.

In the thesis, methods, which are applied in this project to improve the system's security as well as reliability, are mainly discussed. To improve wireless network security, the Wi-Fi configuration is based on the method of WPS, which has a safer wireless protocol. Besides, to ensure the robustness of signal processing, "flag" signal and check sum signal are introduced. The testing result of the decoding with an App on smartphone is presented. According to the result, main factors that impact the decoding quality significantly will be analyzed and then potential solutions to improve the decoding quality will be proposed for the further studies.

3. LITERATURE REVIEW

I. ABSTRACT

In this paper, the technologies used in setting up initial Wi-Fi configuration for Internet of Things (IoT) are mainly discussed.

Our group focuses on the techniques of out band signal processing and Wi-Fi connection based on the theories of computer vision and Wi-Fi Protected Setup (WPS). This paper mainly focuses on the technology of WPS. The biggest advantage of our method is that the process of adding new electric appliance to the local Internet requires users to have little knowledge about Wi-Fi configuration.

Keywords: Internet of Things (IoT), Wi-Fi configuration, WPS

II. INTRODUCTION

Kevin Ashton first put the concept of “Internet of Things” forward in 1999. The main idea is that people have limited time, attention and accuracy of collecting data in the real world. If we can make Internet know everything that they are supposed to know about physical objects without any help from us, we could definitely reduce waste, loss and cost [1].

These days, the notion of Internet of Things has become so popular that many people believe that its happening is just around the corner. The reason is that you can imagine a world where any object that carries a Wi-Fi enabled chip

can communicate with nearby access point. If any change happens, Internet will collect the information of the “things” more accurately and timely without using any human labor.

Due to the technology of Internet of Things, objects are expected to be able to take part in business, information and social activities as soon as we can set up the communication between themselves as well as between the objects and the physical environment. They can collect data from the environment and exchange information through Internet to let us know their physical status. Furthermore, additional function can be added to Internet of Things such as remote control and monitoring. Their appearance will definitely affect the real world events in a more physical way with or without direct human intervention.

III. TECHNOLOGY OF IoT

A. RFID vs Wi-Fi

At early age of the appearance of IoT, it is related to the technology of RFID (radio frequency identification devices). RFID is a kind of wireless non-contact system that can transfer information from a tag embedded in an object.

One big problem of RFID is that it usually carries low-level location [2] information in terms of tags and antennas. To get higher-level events, a tool that can make users directly identify and manage the metadata on the tags and antennas is required. The application of such tools might give rise to a privacy issue for the metadata stored on the tags must be personalized. Another big

issue relating to the RFID is how to deal with the tags if people don't want to use it anymore. The most common way is to destroy the abandoned tags, which will result in a waste of resource. Due to the problems mentioned above, the application of RFID is limited.

These days, the hottest applications of IoT are related with Wi-Fi technology.

Wi-Fi has been used universally in our daily life. Many personal computer, video-game console, smartphone, tablet, or digital audio player can connect to a network resource via a wireless Wi-Fi access point. The IoT devices based on the Wi-Fi technology are attracting and easy to be carried out for the widespread use of Wi-Fi network. On the other hand, setting up Wi-Fi configuration for IoT devices doesn't require a tag to save users' personal information. Users can manage the information of the "Things" in a safer way.

These days, we already see a lot of products that can associate electric appliance with Wi-Fi network. Many big electrical vendors like Qualcomm and Ti have entered this field. The Trend of combining more and more IoT devices with Wi-Fi is inevitable.

B. WEP vs WPS

The Wired Equivalent Privacy (WEP) is a security algorithm invented to provide data confidentiality for wireless network in 1999. Because of the fact that WEP reduces network speed due to its long key and suffers from several security flaws, it has lost favor among most telecommunication companies.

WPS, a new standard Wi-Fi security introduced in 2007, has two major merits compared with WEP. One is its high degree of usability. WPS provides an easy solution for customers to set up secure network in small office and home office (SOHO) environment. Another advantage is that WPS improves the Wi-Fi security with the application of WPA protocol, which will be discussed in details in the next part.

C. WEP vs WPA

Wi-Fi Protected Access (WPA) is a new security standard adopted by the Wi-Fi Alliance to provide stronger data protection and network access control. Before the application of WPA, the Wired Equivalent Privacy (WEP) was widely used as the standard protocol to give users the similar level of security as on a wired network. However, as it turns out that WEP is not as safe as it is supposed to be, WAP is introduced to improve the wireless network security.

The main weakness of WEP is that it uses static encryption keys [3]. Every time a packet is transmitted over the wireless local network, the key will be used to encrypt it. Compromising this WEP-protected network might only take few minutes by intercepting and analyzing enough amounts of data [3](fewer than100, 000 packets). This makes WLAN based on WEP protocol quite vulnerable.

Compared with WEP, WPA provides stronger wireless encryption by applying user authentication and temporal key integrity protocol (TKIP). The extensible authentication protocol (EAP) is based on a more secure encryption

system to prevent unauthorized users to access the network. And TKIP enables every packet to be sent with a unique encryption key. Those factors make WAP protocol the mainstream technology in the field of wireless network.

D. Existing Product of IoT Devices

There are some realized IoT devices based on Wi-Fi connection such as the Electric Imp, which was displayed at Maker Faire Bay Area 2012.

The Electric Imp [5] is a module containing an ARM Cortex M3 System on Chip (SoC) with embedded Wi-Fi [5]. After inserting the module into a board or electric appliance, it can connect the appliance to the Access point via Wi-Fi.

To set up Wi-Fi configuration for IoT devices, a critical step is to construct credential transfer between IoT devices and smartphones. There are two types of communication links for this process, which are uplink and downlink. Downlink credential transfer requires smartphones to send out credential information, which is received by IoT devices. Uplink credential transfer is the other way around. For the Electric Imp, downlink credential transfer is used, which requires smartphones to work as a physical interface to allow users typing in SSID and password. Then, by pulsing the smartphone's screen on and off, the credential information can be beamed to the Electric Imp's light sensor.

In the process of out-of-band credential exchange, the reliability and accuracy are mainly determined by the technology of data collection and analysis. As the downlink credential transfer requires the IoT devices to receive and process the signal, it is costly to further improve the quality of signal

transmission since every IoT device needs to be updated in this case. On the contrary, uplink credential transfer only requires the updating of smartphones, which is much easier to be achieved.

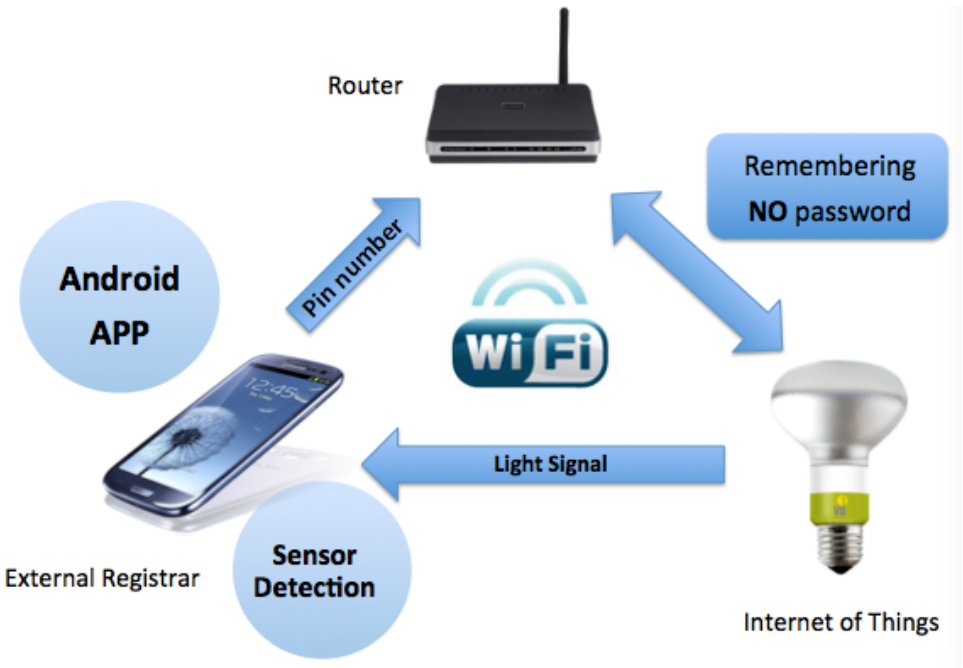
In this project, uplink is applied based on the comparison of these two links, which is discussed in the next section.

IV. METHODOLOGY

In this project, IoT devices are connected with Wireless Local Area Network via Wi-Fi based on the theory of WPS and uplink credential transfer.

This section discusses the methods to improve the reliability and efficiency of credential transfer.

The process of initial Wi-Fi configuration is shown as follows:



1st step: The IoT device sends PIN number to smartphone by controlling the LED bulb on it. The LED light control is implemented on an Arduino board in our

prototype.

2nd step: Smartphone decode the PIN number and sends it to router.

3rd step: Router recognizes the IoT device and adds it to the local Wi-Fi network.

The first and second step consist the process of uplink credential transfer.

A. Uplink vs Downlink

The evaluation of the communication quality based on uplink and downlink shows that they are so difference due to their asymmetric system structures [4].

The variance in SIR due to traffic distribution is bigger in downlink than that in uplink. The larger variance in downlink communication results in lower system efficiency. Besides, a shadowing variation [4] will affect the communication quality in downlink. In order to build a more efficient system, uplink is applied in this project.

From the view of product upgrade, uplink is also preferable. The reason is that in uplink communication, it has little requirements on the quality of out-of-band signal senders. Thus, every time there is a demand of improving the accuracy of signal transmission, the solution is to promote the smartphone instead of upgrading the sensor and processor in every IoT devices.

B. Use "Flag" and Check Sum in Signal Transmission

To improve the accuracy of signal transmission in the process of credential transfer, "Flag" signal and check sum signal are put together with the 8-bit Pin number to form an integrated data. These additional signals provide essential

information to solve the problem of clock synchronization and to check the correctness of received signal.

V. SECURITY ISSUE

Even through IoT will bring people with a lot of convenience, it will also raise some security issues such as privacy, regulations and security. If everything around us can exchange information with each other, people will feel they are lack of privacy and freedom. Even worse, if those intelligent “things” are out of control, it will result in a disaster that might significantly influence human beings’ regular and normal life.

In fact, the Internet and its users are under continual attack. In December 2011, a severe security problem [5] was reported relating to WPS-enabled Wi-Fi networks. A brute-force attack on WPS makes it possible for unauthorized users to get access to the network. Thus, seeking for a resolution to the security problem is of great urgency.

A further method to increase security and privacy is Peer-to-Peer (P2P) system, which generally shows good scalability and performance in the applications.

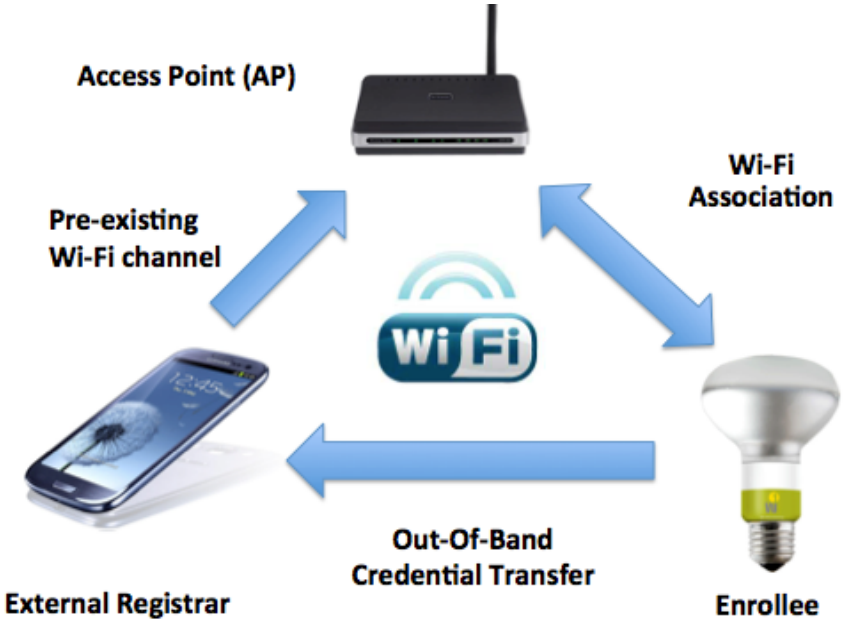
VI. CONCLUSION

In our project, improvement has been made to make it safer and simpler for people to set up initial Wi-Fi configuration for Internet of things based on Wi-Fi Protected Setup. Further study should focus on the security and robustness

issues of the Internet of Things.

4. METHDOLOGY

I. PIN BASED WI-FI CONFIGURATION [6]



The process of PIN based Wi-Fi configuration is shown as following:

A. User activates PIN based configuration and obtains PIN from Enrollee.

B. External Registrar notifies the AP when it becomes active by setting the Selected Registrar attribute to TRUE using SetSelected Registrar UPnP action.

C. After an AP receives a SetSelected Registrar UPnP action with Selected Registrar TRUE, AP incorporates Selected Registrar flag set to TRUE in its Beacons and Probe Response.

D. Enrollee starts PIN based registration protocol and scans for an AP in active PIN mode

E. Enrollee associate with target AP in active PIN mode and send M1 message. M1 message enables External Registrar(s) registered to receive UPnP events.

In the project, out-of-band credential transfer was implemented by controlling LED light, which represented the IoT device. And the smartphone Samsung Galaxy3 worked as an external registrar that also was responsible for decoding the PIN number.

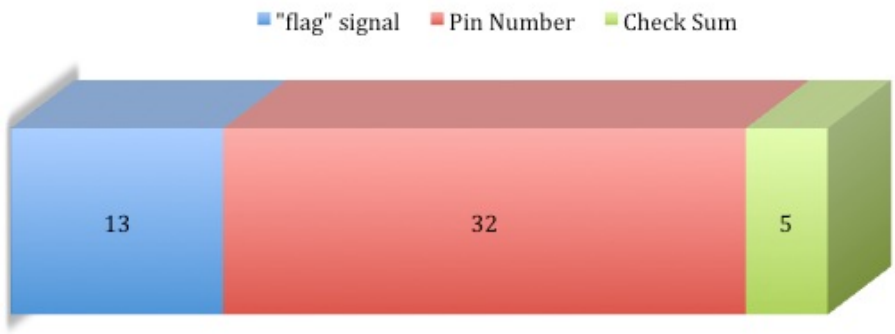
II. UPLINK CREDENTIAL TRANSFER

Uplink credential transfer applied in this project requires IoT devices to send PIN to smartphones. This process consists of two parts. The first step is to send light signal from IoT devices to smartphones. I accomplished the signal sending by using Arduino board, which is a single-board microcontroller designed to make the process of using electronics more accessible. The second step is to recover the PIN number from the light signal received by the smartphones. Anne and Grace worked on the graphic processing based on the computer vision.

III. LED LIGHT CONTROL WITH ARDUINO BOARD

In order to set up Wi-Fi configuration for electronic devices, Arduino board was applied in the project to control the blinking of LED light. And a smartphone worked as an external registrar to receive and process the light signal. The camera on the smartphone would record a video of the blinking and the

developed Android App on the smartphone could decode the light signal into 50-bits binary numbers, which contains the “Flag” signal (13-bits), PIN number (32-bits) and check sum (5-bits). Then, the Pin Number would be sent to the router to finish connecting the electronic device with the local Wi-Fi network. In this part, methodology of sending Pin Number is mainly discussed.



In our methodology, the digital modulation scheme is amplitude-shift keying (2 ASK), which is referred as on-off keying (OOK) in optical system. OOK is a modulation where a binary “1” was represented by turning on the LED light for a certain time interval and a binary “0” was represented the other way around. To make the LED light working at the supposed mode, a code consists of three parts was loaded to the Arduino board. In the first part, a “flag” signal was defined and sent in order to tell the signal receiver the beginning of the actual data and the data frequency. In the second part, the real data, which was an 8-bits Pin Number, was stored in an array with a width of 8 and was sent after the finish of sending “flag” signal. Because decimal numbers were used to represent the 8-bits Pin Number, a 4-bits binary number was required to represent each Pin Number. In the process of sending one bit Pin Number (4-

bits binary number), the Most Significant Bit (MSB) was read and sent in each cycle of the loop. Before starting next cycle, the 4-bits binary number was shifted to left so the second MSB can be accessed in the next cycle as the MSB. To help receiver check the correctness of the signal sending, a check sum variable was also declared in the second part. Every time when a signal “1” was sent, the value of check sum would be increased by one. In the end, after sending the 8-bits Pin Number, the check sum signal was sent with a value of the total number of “1” in the real data. The “flag” signal, 8-bits Pin Number and the check sum composed the integrated data package that the external registrar would accept.

The reason why the methodology mentioned above was applied in our project was to solve the problem of time synchronization as well as to improve the reliability of signal transmission. Clock synchronization for wireless signal transfer was a big issue since any mismatch in clock synchronization could result in a catastrophe that prevented the receiver to get the valid data. Because the camera, which was used in our project as a sensor on the smartphone to collect the light signal, might have a clock rate that was different from the sending frequency, it was hard to tell accurately when the actual data would begin. Also the mismatch in sampling frequency and sending frequency could result in errors in the decoding process. Our solution was to set a “flag” signal before the actual data to help the Android App to process the actual data properly. The “flag” signal was a 13-bits binary number with a value of “0000001111110”. The

receiver was told that the “flag” signal contained only 6 bits “1” in continuity. Thus, by measuring the total duration of the “1”, the receiver could calculate the duration for one bit signal and then determine how many frames were required in sampling one bit signal. From the “flag” signal, the receiver could get enough information to determine the start time of the real data as well as the start time of each bit signal. Another benefit of using “flag” signal was to improve the flexibility of the Android App for it could process the light signals with different frequencies.

Before the methodology mentioned above was applied in our project, another method was used which suffered from two big problems. In the previous methodology, Manchester code was used to define “1” and “0”. Since Manchester code required that the encoding of each data bit had at least one transition and occupied the same time, it took more time to send one bit signal compared to the code used in the final methodology. Another problem was the mismatch in time synchronization, which was eliminated by adding a “flag” signal as we discussed in our final method.

5. DISCUSSION

I. RESULT

In this project, the deliverable result is that the PIN number can be successfully recovered in the process of credential transfer.

In the practical test, Samsung Galaxy3, which was used as the external

registrar, was placed 10 cm away from the LED light while recording the blinking. The test was conducted in an indoor environment under normal room light. The probability of decoding the PIN number correctly is 100%.

II. Comments on Testing Result

The testing result verified the feasibility of setting up initial Wi-Fi configuration by using out-of-band signal in the process of credential transfer. However, the performance needs to be improved related to the testing distance, record time and robustness under different light environments.

A. Hardware Factors

The paramount hardware factors that affect the performance of credential transfer are camera's frame rate while recording and LED light's luminous features.

The biggest frame rate of camera on smartphones is about 30 frames per second, which is not available in many smartphones. In the project, the frame rate is 10 frames per second and 3 frames are required to determine 1-bit binary signal. Thus, it requires users to record the LED light for at least 15 seconds in order to get the integrated data.

Besides, two characteristics of LED lights should be taken into consideration to promote the quality of graphic processing. One characteristic is the luminous intensity, which is a measure of wavelength-weighted power emitted by LED lights in a particular direction per unit solid angle. A LED light with bigger luminous intensity is brighter so that it enables smartphones to

determine its status in a larger distance.

Another important feature of LED is its spatial radiation pattern (viewing angle). Because the developed app detects the switch of the LED light based on the amount of red pixels (red LED light is used in the project) accounted in a frame of the video, it is better to have a large viewing angle to produce more red pixels when the light is on.

B. Software Factors

From the perspective of software, the main factor that influences the decode accuracy is the algorithm applied while determining the switch of the LED light. The algorithm applied cannot eliminate the noise caused by environment changes and is unable to process the image of remote LED light. An improved algorithm is needed to fix these problems.

III. METHODS TO IMPROVE PERFORMANCE

A. Improve Encoding Method

The method to improve encode efficiency is to transfer multi-bits information during one clock cycle of LED control. Two alternative methods to accomplish this are using LED matrix and controlling LED light brightness at different levels.

In this project, one cycle light signal represents 1-bit binary number (i.e. ‘0’ or ‘1’). If quaternary code were used in encoding, transmission time would be significantly reduced.

B. Improve Modulation Method

To improve the testing distance, Orthogonal Frequency Division Multiplexing (OFDM) [7], an advanced modulation formats, can be applied. OFDM. Besides, Return-to-Zero coding could be applied to improve the system sensitivity [8].

6. CONCLUSION

From this capstone project, I gained a lot of knowledge about Internet of Things from technology aspect. First of all, our group studied the initial Wi-Fi configuration for IoT device based on WPS and focused on the process of credential transfer, which is an important step to allow only authorized users to set up the Wi-Fi connection. Besides, I learned how to control LED light with Arduino, which is an open-source electronics prototyping platform. During the implement process of credential transfer, I also get an insight into the method of encoding and decoding while considering how to improve the reliability of signal processing.

The testing result shows that the Wi-Fi configuration based on uplink communication is practical. The further study should focus on improving the reliability of signal transmission by using a better processing algorithm and hardware components with higher performance. Besides, the encoding efficiency should be improved to reduce the record time. Last but not least, a big issue that might endanger the application of Internet of Things might be the

security of wireless network. Even though WPS is safer than WEP, it is reported that security problems still exist. An extra encryption related to the IoT device should be developed to make up for the WPS's security flaws.

7. REFERENCE

[1] Kevin Ashton, (2009) "That 'Internet of Things' Thing", *RFID Journal,* June 22.

[2] Evan Welbourne, Leilani Battle, Garret Cole, Kayla Gould, Kyle Rector, Samuel Raymer, Magdalena Balazinska, and Gaetano Borriello, (2009) "Building the Internet of Things Using RFID", *IEEE Computer Society*, May/June.

[3] Vangle Beal, (2007) "The Differences Between WEP and WPA", *WEBOPEDIA*, June 15.

[4] Takeo, Shinichi Sato, and Akira Ogawa, (1999) "Uplink and Downlink Communication Qualities in CDMA Cellular Systems Effects of Traffic Distribution", *IEICE TRANS.*, vol. E82-A, no. 12.December.

[5] Stefan Viehböck, (2011) "Brute forcing Wi-Fi Protected Setup", December 26.

[6] Wi-Fi Alliance, (2009) "Wi-Fi Simple Configuration Specification", January 5.

[7] Sridhara K, (2012) "FREE SPACE OPTICAL COMMUNICATION", *International Journal of Latest Research in Science and Technology*, vol. 1, issue 3, September-October, pp 202-205.

[8] Hennes Henniger, Otakar Wilfert, (2010) "An Introduction to Free-space Optical Communications", *Radioengineering,* vol. 19, no. 2, June.

[9] SheQiang Peng, HongBing Shen, (2012) "Security Technology Analysis of IOT", *Communications in Computer and Information Science,* vol 312, pp 401-408.

[10] Weber, Rolf H. Weber, Romana, (2010) *Internet of Things: Legal Perspectives*, Springer Publishing Company.

[11] Wi-Fi Alliance, (2007)"Wi-Fi CERTIFIEDTM for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi® Networks"

[12] Rodrigo Roman, Pablo Najera, and Javier Lopez, (2011) "Securing the Internet of Things", *IEEE Computer*, vol. 44, no. 9, September,pp. 51-58.