PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Mustafa Saad Abdulwahhab Kamoona

Entitled

Internet Of Things Security Using Proactive WPA/WPA2

For the degree of Master of Science in Electrical and Computer Engineering

Is approved by the final examining committee:

EL-SHARKAWY, MOHAMED A.
Chair

KING, BRIAN S.

RIZKALLA, MAHER E.

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): EL-SHARKAWY, MOHAMED A.

Approved by: KING, BRIAN S. 4/13/2016

Head of the Departmental Graduate Program Date

INTERNET OF THINGS SECURITY USING PROACTIVE WPA/WPA2

A Thesis

Submitted to the Faculty

of

Purdue University

by

Mustafa Kamoona

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science in Electrical and Computer Engineering

May 2016

Purdue University

Indianapolis, Indiana

I would like to dedicate my thesis work to my parents Saad Kamoona and Ikhlas Al-Taie who give me their unconditional love and support in every step of my life. I also dedicate this thesis to my brother Abdulla and my sisters Farah and Yousra and thank them for believing in me and being by my side. I would also like to thank my best friends and brothers Faris Rassam and Hasan AlSadik and all my friends who have helped me in my career and education in any ways they could. Without you all, the work done would not be possible.

ACKNOWLEDGMENTS

I would like to acknowledge and thank Dr. Mohamed El-Sharkawy and Indiana University, Purdue University- Indianapolis ECE department for the support and for giving me the time and the equipment needed for the work in this thesis.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

ABSTRACT

Kamoona, Mustafa. MSECE, Purdue University, May 2016. Internet Of Things Security Using Proactive WPA/WPA2. Major Professor: Mohamed El-Sharkawy.

The Internet of Things (IoT) is a natural evolution of the Internet and is becoming more and more ubiquitous in our everyday home, enterprise, healthcare, education, and many other aspects. The data gathered and processed by IoT networks might be sensitive and that calls for feasible and adequate security measures. The work in this thesis describes the use of the Wi-Fi technology in the IoT connectivity, then proposes a new approach, the Proactive Wireless Protected Access (PWPA), to protect the access networks. Then a new end to end (e2e) IoT security model is suggested to include the PWPA scheme. To evaluate the solutions security and performance, firstly, the cybersecurity triad: confidentiality, integrity, and availability aspects were discussed, secondly, the solutions performance was compared to a counterpart e2e security solution, the Secure Socket Layer security. A small e2e IoT network was set up to simulate a real environment that uses HTTP protocol. Packets were then collected and analyzed. Data analysis showed a bandwidth efficiency increase by 2% (Internet links) and 12% (access network), and by 344% (Internet links) and 373% (access network) when using persistent and non-persistent HTTP respectively. On the other hand, the analysis showed a reduction in the average request-response delay of 25% and 53% when using persistent and non-persistent HTTP respectively. This scheme is possibly a simple and feasible solution that improves the IoT network security performance by reducing the redundancy in the TCP/IP layers security implementation.

1. INTRODUCTION

1.1 Introduction to the Internet of Things

Characterized by its rapid paced technology development, todays world was not so a couple of decades ago. A substantial technology leap happened when the Internet became public in the 1980s allowing people to surf the web, send emails, and share files. It is always exciting to look back and see how much the world has advanced and how the Internet helped in this process. The Internet was and is still providing a fertile landmark that enables people to communicate in a simple, fast, and convenient way. It is a fact that the Internet continues to evolve shaping our everyday life in the process.

Although the Internet of Things networks are now ubiquitous in networking environments, in literature, the term Internet of Things (IoT) or Internet of Everything (IoE) is still ambiguous. There is no single unified definition of what the IoT really is, however, we can define the IoT by elaborating what the IoT can provide. The Internet of Things is thought to be the next evolution of the Internet [1] as it is going to provide a networking infrastructure allowing trillions of devices to collect data and communicate with each other and with other devices to make processed smart decisions. The devices can be any object or anything (thus the name Internet of Things) embedded with the needed hardware and software that are required for processing and networking capabilities. In other words, IoT will be a network of the currently existing rather powerful Internet devices like smart phones, personal computers, and servers with addition of new less complex devices like heart or brain activity monitoring sensors, automobile motion or brake sensors, or any environmental sensors.

From the before mentioned examples, it can be seen that an IoT device does not have to be as complex as the current Internet enabled devices. Thus there is a

wider range of devices that can be connected to the IoT networks than that of the Internet. It is predicted that with IoT there will be billions of devices connected and communicating with each other. A typical IoT home environment is shown in Fig. 1.1

Fig. 1.1. Typical IoT Enabled Home [2]

Whether it is home, business, health, or educational IoT environment, a reason why the IoT environments are getting much attention around the world is due to the fact that a larger scale of integration is possible between the physical objects and the computing systems and thus more intelligent decisions can be made. This everyday life impact of the Internet of Things is possible due to its ability gather a huge amount of data from devices surroundings around the globe then analyzing and processing this collected data to be able to make a sophisticated decision.

Therefore, the IoT will allow a new era of data exchange and decision making. That is why in 2008, the U.S. National Intelligence Council (NIC) reported that By 2025 Internet nodes may reside in everyday things, food packages, furniture, paper documents, and more. Todays developments point to future opportunities and risks

that will arise when people can remotely control, locate, and monitor even the most mundane devices and articles. Popular demand combined with technology advances could drive widespread diffusion of an Internet of Things that could, like the present Internet, contribute invaluably to economic development and military capability [3]. Fig. 1.2 shows some of the many possible application uses of the IoT devices.

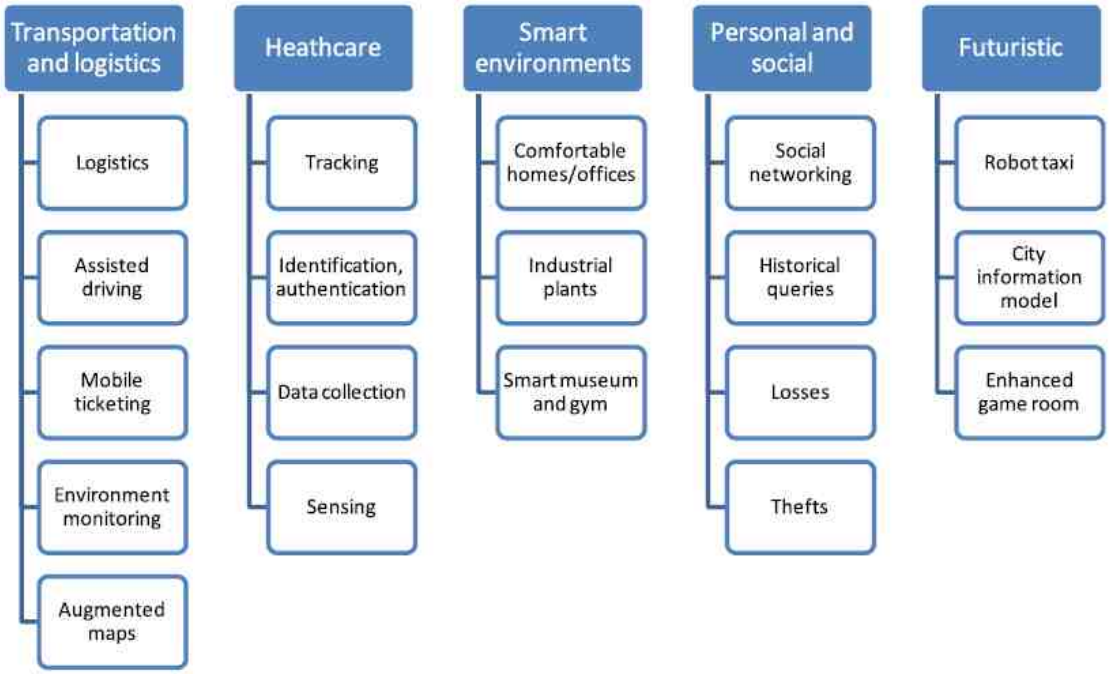

Fig. 1.2. Possible Current and Future IoT Uses [4]

1.2 Brief History

The Internet of Things might be thought of as the point in time where more things or object are connected to Internet than people. An explosive growth of tablets and smart devices happened to increase the number of connected devices from around 500 million connected devices in 2003 while the human population was around 6.3 Billion to 25 Billion connected devices when the population was 7.2 in 2015. According

to [1], the point in time when the number of connected devices surpassed the human population was in 2010. Fig 1.3 shows the timeline of the connected devices versus human population increase.

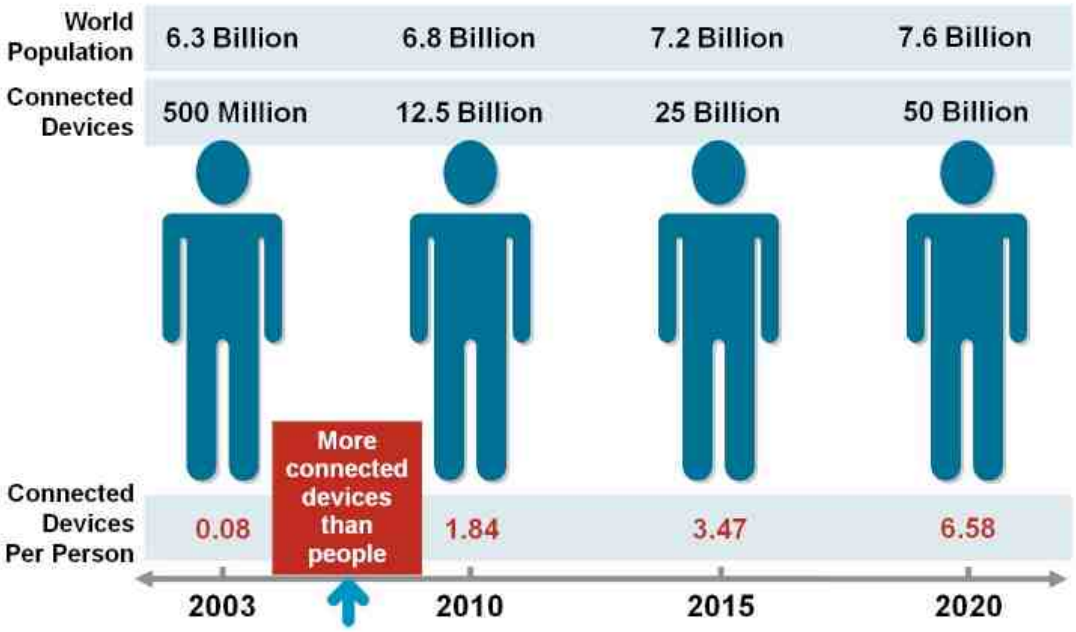

Fig. 1.3. Connected Deices Versus Human Population Timeline [1]

Although the Internet of Things roots can be tracked back to Massachusetts Institute of Technology (MIT) laboratories back in 1999 with the radio frequency identification (RFID) sensing technology [1], whereas the idea of low power communication sensor networks goes back way further in time. The emergence of the distributed low power sensor networks goes back to as early as the year 1967 [4]. Then a series of intermittent events led to the idea of wireless sensor networks (WSN) which in turn led to the concept of smart dust networks. Standards started to emerge for such networks in 2003/2004, when firstly the 802.15.4 standard and secondly the ZigBee standard were released. The emergence of those standards facilitated the development of the idea of the Internet of Things.

Table 1.1 shows a timeline of the events that helped in the process of the Internet of Things development. From the majority of those events, we can notice that there are three basic requirements for Internet of Things Networks:

- Low energy communication. As there is little possibility that the IoT devices will be connected to the mains power, their battery life will have to be long for the Internet of Things applications to be practical, as charging or changing the batteries for a huge number of devices would not be a simple process [4].

- Reliable Internetworking enabled communication stack. The IoT devices should be able to communicate with each other and with other devices on other networks that are connected to the Internet. This connection should be highly reliable and bi-directional as data will be traveling both from and into those devices [4].

- Light Secure End to End environment. Those networks might communicate sensitive information, so a light secure end to end communication is a necessity for those networks in order to preserve the confidentiality of the data those networks are conveying.

Table 1.1
Events Helped in IoT Idea Development [4]

Year	**Event**
1967	REMBASS Remotely Monitored Battlefield Sensor System
1978	Dist. Sensor Networks for Aircraft Detection Lincoln Labs - Lacoss
1992	RAND Workshop - Future Technology Driven Revolutions Military Conflict. Concepts behind Smart Dust emerge.
1993-1994	DARPA ISAT studies - many WSN ideas and applications discussed. Deborah Estrin leads one of the studies.
1994	LWIM - Low Power Wireless Integrated Microsensors
1997	Smart Dust proposal written, Kris Pister (Berkeley)
1998	Seth Hollar makes wireless mouse collars
1999	Endeavour project proposed by Randy Katz, David Culler (Berkeley) PicoRadio project started by Jan Rabaey (Berkeley)
2000	Crossbow begins selling Berkeley motes
2001	Multiple demos proving viability
2002	Dust, Ember, Millennial, Sensicast founded
2003	IEEE802.15.4-2003 standard Moteiv (now Sentilla) founded
2004	ZigBee 1.0 standard ratified TSMP 1.1 shipping
2005	Arch Rock founded
2006	ZigBee 2006 standard ratified IEEE802.15.4-2006 standard
2007	WirelessHART standard ratified IETF 6LoWPANs RFC4944 published WirelessHART shown to achieve 99.999% reliability
2008-2009	IETF workgroup Routing Over Low-power Lossy links (ROLL) created. IEEE802.15.4e work group created
2010-2011	IEEE802.15.4es MAC protocol ratified IEFT 6LoWPANs RFC4944 updated IETF ROLLs RPL routing protocol ratified

1.3 The Future of Internet of Things

The importance of the Internet of Things and the data the IoT devices communicate is growing exponentially. The procedure of processing the data is shown in Fig 1.4, it all starts with the gathering of huge amount of data.

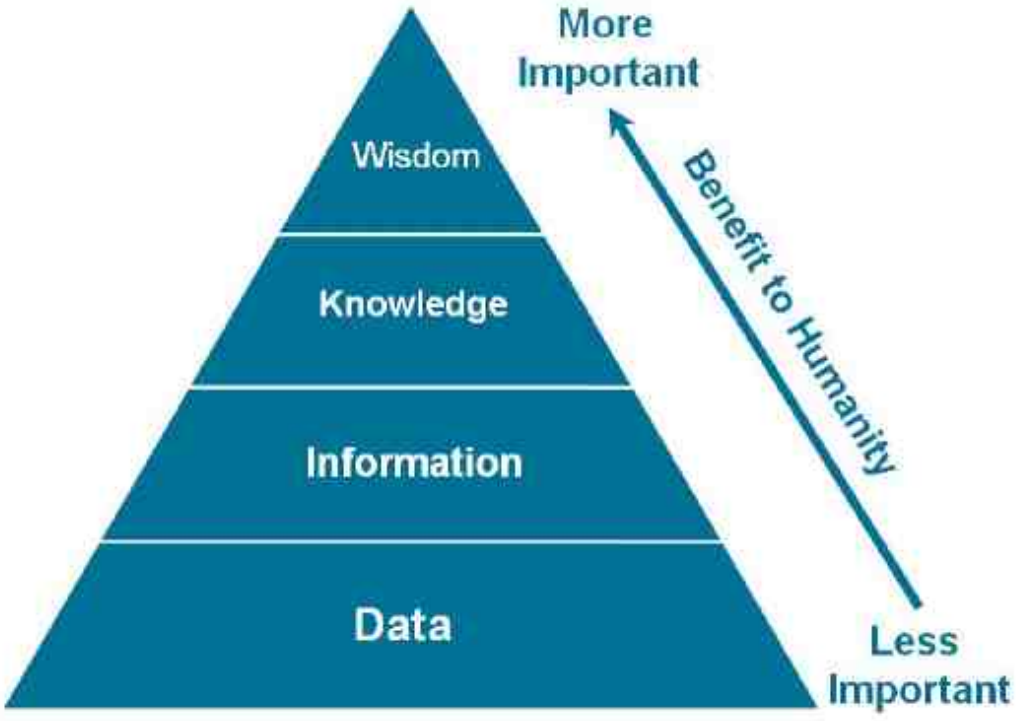

Fig. 1.4. Human Processing of Data [1]

From the bottom up we can see how the data is being processed and becoming more and more important. data is the raw material that is processed into information. Individual data by itself is not very useful, but volumes of it can identify trends and patterns. This and other sources of information come together to form knowledge. In the simplest sense, knowledge is information of which someone is aware. Wisdom is then born from knowledge plus experience. While knowledge changes over time, wisdom is timeless, and it all begins with the acquisition of data [1].

So the Internet of Things is not limited to the currently existing machine to machine (M2M) architecture that is used for remote control and monitoring, but The IoT creates an intelligent, invisible network fabric that can be sensed, controlled and programmed. IoT-enabled products employ embedded technology that allows them to communicate, directly or indirectly, with each other or the Internet [2].

1.4 Connectivity Options

As some might think that the Internet of Things connectivity is a single standard, the reality is, there will be a broad range of connectivity (wired and wireless) solutions for the IoT networks. As more and more Internet of Things networks need to be connected on daily basis, a need for flexibility and adaptive configuration arises depending on the complexity, physical environment, available power, and security requirements. In the majority of the cases, the wireless solution is more suitable for the Internet of Things networks than the wired one as it is easier to set up in tricky physical situations and cheaper to install and maintain. However, a care should be taken when choosing the right wireless technology that is adequate for the present circumstances.

1.4.1 Internet of Things Wireless Connectivity

The wide collection of wireless connectivity solutions ranges from the IPv6 Low Power Wireless Personal Area Networks (6LoWPAN) to the Bluetooth Low Energy (BLE) and Bluetooth technology to the ZigBee technology then to the dominant Wi-Fi technology and more. Fig 1.5 shows the unlicensed frequency bands regions around the world.

Each of the wireless connectivity solutions has its own advantages and disadvantages depending on the range required, circumstances, and environment conditions. Fig 1.6 shows the different wireless area networks and their respective scopes.

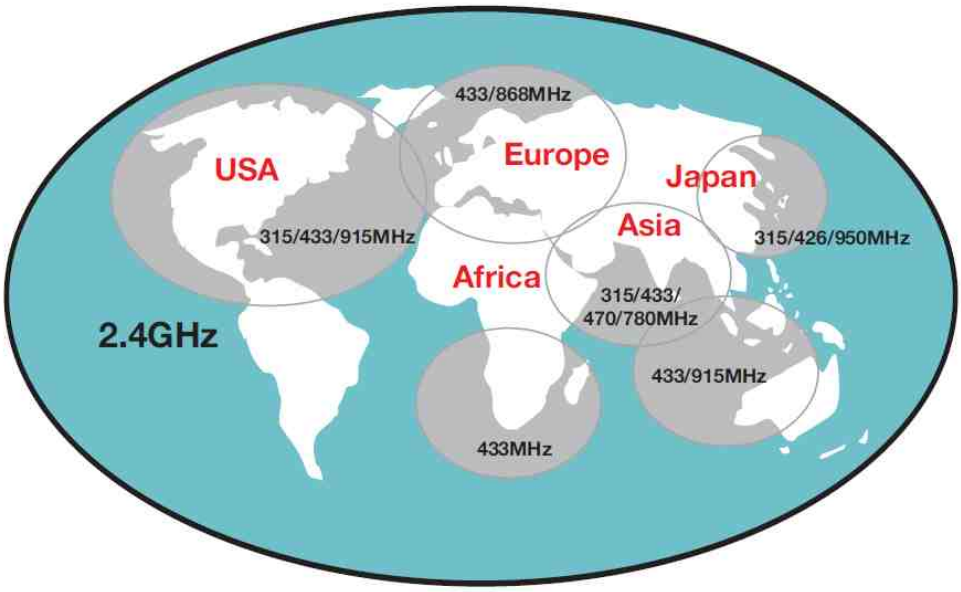

Fig. 1.5. Unlicensed Wireless Frequency Bands [5]

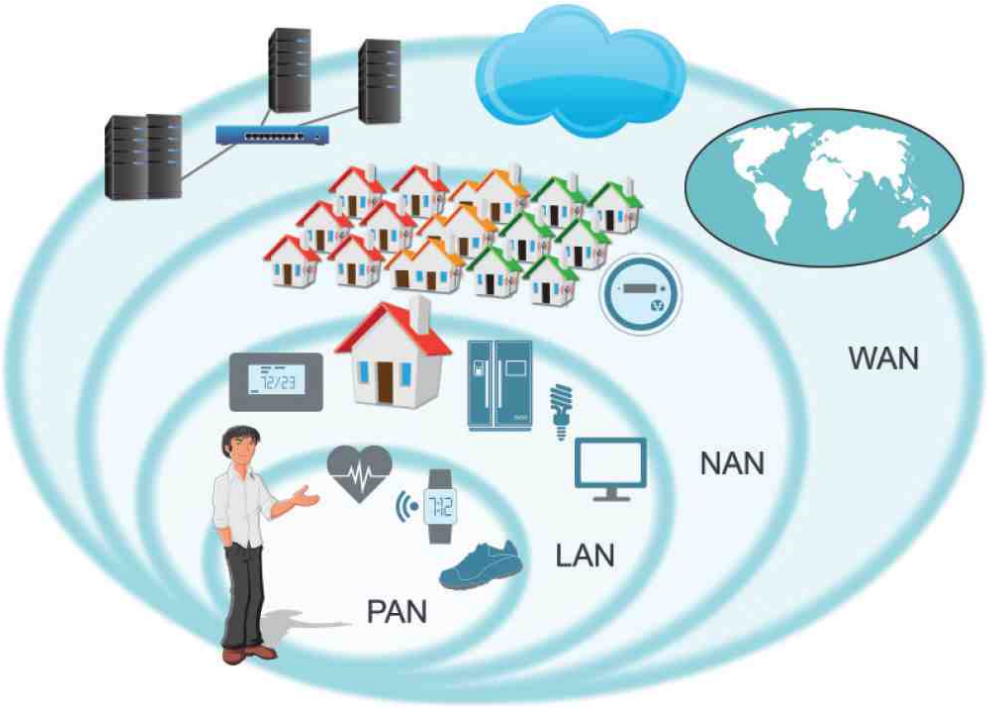

Fig. 1.6. Different Wireless Area Networks [5]

1.4.2 Wi-Fi Solution

The Wi-Fi wireless technology is one of the dominant solutions for the Internet of Things future connectivity. Based on the IEEE 802.11 standard, although the Wi-Fi defines the data link layer of the TCP/IP stack, it is so prevalent that the name Wi-Fi is always associated with TCP/IP wireless networks. The ubiquitousness of the Wi-Fi networks is due to the fact that firstly, almost all of the phones and laptops currently have integrated Wi-Fi modules, and secondly, the interoperability of applications designed by the Wi-Fi alliance.

This success rides on the fact that the Wi-Fi networks are already deployed as part of the infrastructures for homes and business buildings. A natural evolution of the Wi-Fi is to be an integral part of the Internet of Things connectivity [5].

Naturally, the TCP/IP implementation of the Wi-Fi software is complicated and large for the simple design of the Internet of Things and requires much memory and processing. Adding the Wi-Fi solution to the IoT wireless connectivity was not feasible until recently.

Latest silicon advancements made it possible to add Wi-Fi modules to the embedded solutions, the Wi-Fi stack is embedded into the devices and modules to reduce a large amount of the overhead from the micro processing units to allow the smallest micro controlling units to deploy the Wi-Fi connectivity. The increased integration level in those modules, also removes the radio design experience which facilitates the Wi-Fi integration [5].

In addition, in most cases, the IoT devices will need only a small fraction of the Wi-Fi offered bandwidth and data rates, thus with intelligent power management that turn the module on and off (sleep/wake up) to draw small bursts of battery currents, a drastic improvement in the battery life can be achieved. Some current products claim to maintain operation using two AA batteries for more than twelve months [5].

In conclusion, with the prevalence of the Wi-Fi networks, the development of the silicon technology, and smart efficient power management design make the Wi-Fi technology a very promising connectivity solution that helps the advancement of the Internet of Things rapid development [5].

1.4.3 Wi-Fi Use for Smart Cities

The technology keeps on changing our life. In the light of IoT we can picture the future cities as smart cities. In a smart city, several physical objects will be interconnected with each other. The inter-connectivity between billions and billions of devices will allow the smart city to integrate and analyze humongous data form these devices. Thus new services, and exciting solutions for today's problems can emerge. Fig 1.7 shows how huge data is collected from several technologies, and how this data is integrated and analyzed to provide new exhilarating services.

Fig. 1.7. Smart City Architecture and Possible Services [6]

Several examples can be thought of as services offered by smart cities, like health services, educations, traffic rerouting to avoid congestion and accidents, monitoring crime hotbeds to reduce criminal activities, help the city citizens to find parking spots, and help the people to take a more proactive part in contributing with their opinions to the government's officials [6]. As aforementioned, a very suitable infrastructure for the smart cities is the currently implemented Wi-Fi networks. Although the Wi-Fi is ubiquitous, however, there are still some blind spots, areas where there is no Wi-Fi coverage and for that a solution can be accomplished by using umbrella Wi-Fi hotspots to cover these blind spots, hence, ensuring that every spot in the smart city has a Wi-Fi coverage and thus citizens can move freely in the city without the fear of being disconnected.

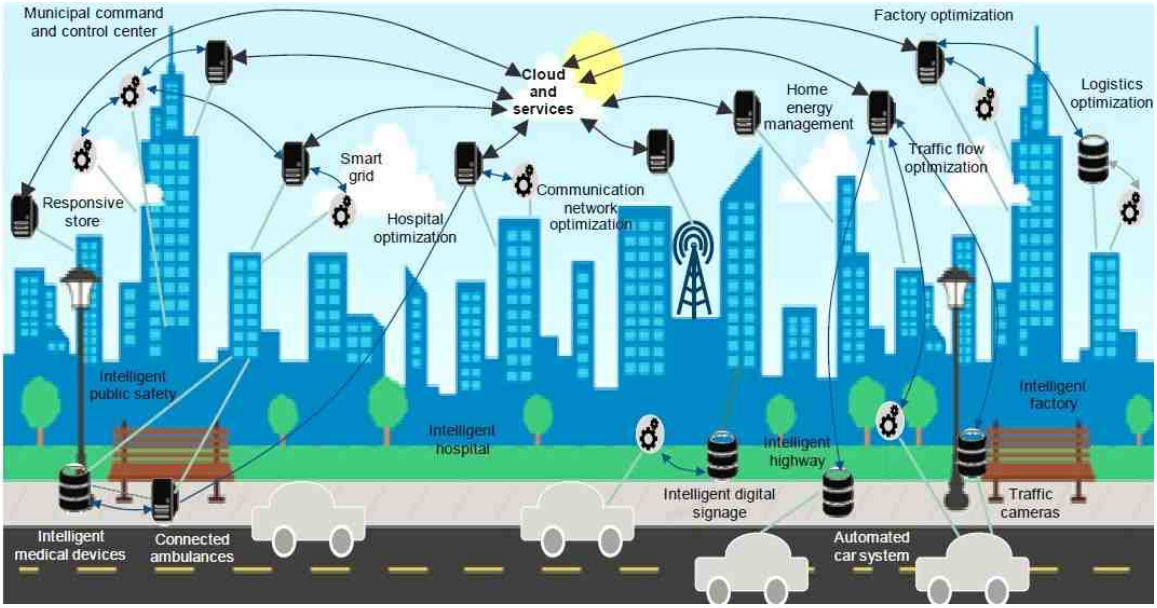

Fig. 1.8. Connectivity in Smart City Example [6]

1.5 Introduction to the Internet of Things Security

Computer security, also known as cybersecurity, defines secure network communication as the secure exchange of messages between two entities over an insecure medium or network [7]. Regular computer networks have many security requirements, yet, the Internet of Things networks and because of their intrinsic critical nature mandate even higher security measures. The IoT is an immense network of interconnected networks and those networks usually have devices that are resource constrained thus entail low power computations and low energy consumption. Such networks face numerous kinds of attacks ranging from simple physical attacks to sophisticated cryptanalysis attacks. Fig 1.9 shows a simple diagram for current known IoT attack types.

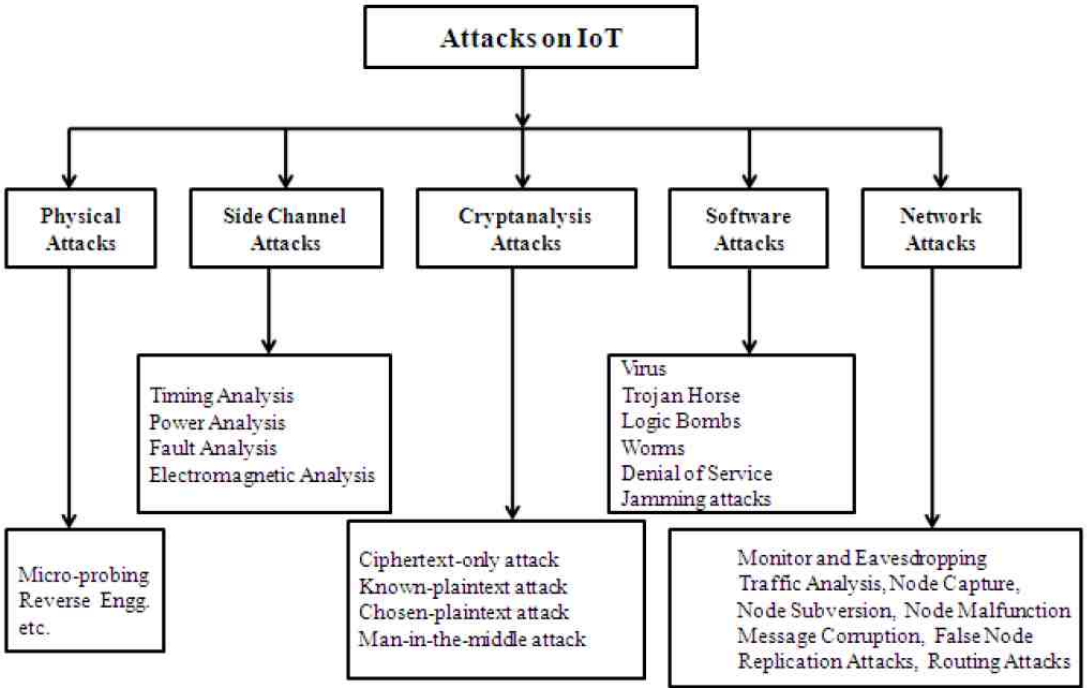

Fig. 1.9. Types of Attacks on IoT Networks [8]

1.5.1 Internet of Things Security Services

Cybersecurity in general has a number of services that the network administrator should keep in mind in order to protect the network from exploited vulnerability. Internet of Things networks should provide the below security pillar services because of the sensitivity of their applications.

Confidentiality the contents of the messages between the two host devices (client and server) should only be read by the authenticated devices. No other intermediate adversary should be able to sniff and then read those sensitive contents. Some kind of devices authentication and messages encryption are required.

Integrity The exchanged messages should not be tampered by any intermediate entity with or without purpose. Integrity helps in preventing the man-in-the-middle attacks where a middle device would inject packets into the network masquerading a legit host device. Replay attacks are considered an attack on system integrity since the attacker will record a transaction and then replay that transaction at a later time.

Availability The data that is supposed to be available to authenticated devices should be available to those devices at all times. This service is against denial of service attacks (DoS) where the attacker targets the availability of the provided services to the authentic users.

The above services are provided by different devices and layers in the network with the aid of symmetric key cryptography, public key cryptography, and hash functions that are briefly explained in the following section.

1.5.2 Introduction to Cryptography

Cryptographic techniques have gone hand in hand with secure message communication for a long time even before networking and computers were devised. A long

description of cryptographic history and evolution is explained in details in [9] [10]. With the emergence of computer networking, cryptography has become inseparable with Cybersecurity services like authentication, encryption, and integrity [7].

Cryptography enables a user to encrypt his message which is called a cleartext or plaintext and send it as an encrypted message which is labeled as ciphertext, those ciphertexts should be unfathomable to any intruder that intercepts those messages.

Hash functions are inextricable from cryptography. A hash function in general is a function that generates a fixed length output string for any given input, a cryptographic hash function, however, has more restrictions including that it should be infeasible to find two different inputs that result in the same output string.

Many standardized encryption algorithms and techniques are available in reference for comments like [RC 3447] and [RFC 1321] [7]. In this thesis, as in many cryptography sources, the two communicating entities are addressed as Alice and Bob and the intruder is labeled as Trudy. The algorithm that encrypts the messages, that is, changes a plaintext into a ciphertext, is referenced as a cipher. Some of those terms are illustrated in Fig 1.10. Usually the cipher is public knowledge but the secret is the keys Ka and Kb which can be the same in both sides in the case of symmetric key cryptography or different in the case of public key cryptography.

A simple cipher might encrypt a message (m) by using its key KA(m) and on the receiving side the cipher can decrypt the ciphertext with its secret key KB to recover the original message (KB(KA(m))=m) [7]. The cipher might be a simple bitwise XOR on both sides.

Symmetric Key Cryptography

In symmetric key cryptographic systems, both the communicating entities (Alice and Bob) use the same shared key (symmetric key) to encrypt and decrypt the messages. Where it is assumed that at some point before the communication starts, the two entities have agreed on a shared secret key through a secure communication

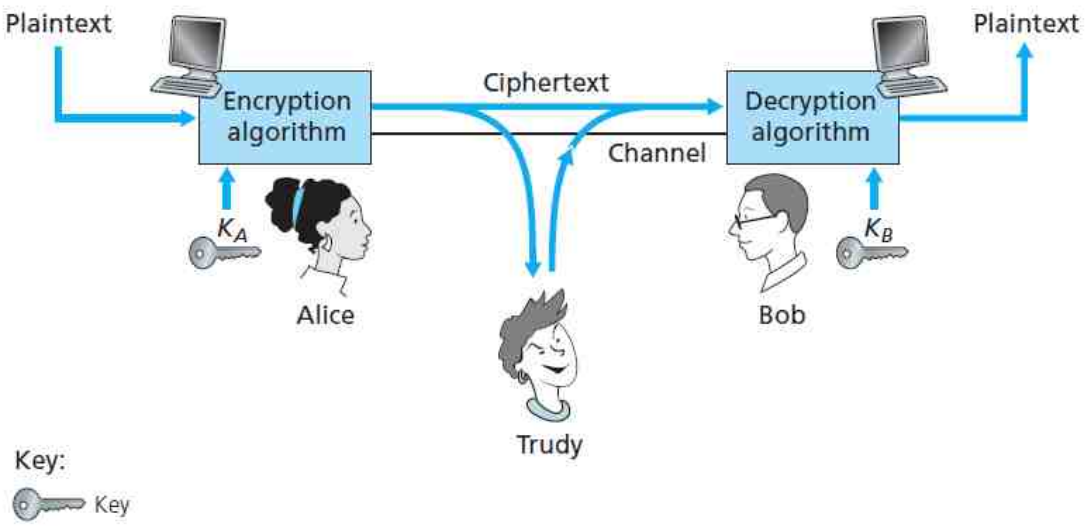

Fig. 1.10. Cryptography Terminology [7]

channel. Symmetric key cryptographic techniques are usually computationally faster than public key ones.

Public Key (Asymmetric) Cryptography

In public key cryptographic systems, a pair of keys which are mathematically related are used. A public key (K+) which is available to the public and a private key (K-) which is a secret to everyone but to the entity itself. In order to exchange messages, a sender (Alice) should encrypt a message with the receivers (Bobs) known public key (KB+) and send the ciphertext (KB+(m)) to Bob, then Bob, using his own private key (KB-), should decrypt the ciphertext (KB- (KB+(m)=m). It is interesting to note that if a message is encrypted by a public key (KB+) then it can only be decrypted by the same entities private key (KB-) and vice versa, thus the same key cannot be used for encryption and decryption. Many techniques target public key cryptography, and probably the most prevailed one is known as the RSA algorithm. Fig 1.11 shows a public key cryptography scenario.

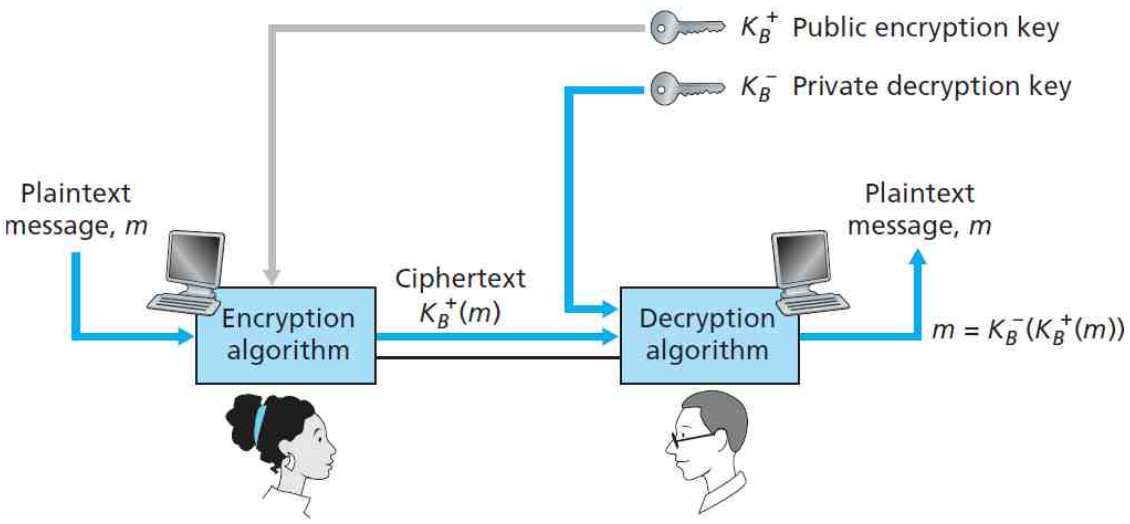

Fig. 1.11. Public Key Cryptography Scenario [7]

In the cybersecurity community, there is a wide diversity in the Internet of Things state-of-the-art works. Whereas all the works agree in terms that the Internet of Things -consisting mostly of embedded systems that generate sensed data- should have the messages carrying them encrypted before being sent, some of the work targets end to end encryption like the Secure Internet of Things Project (SITP) where the data is encrypted in the end device (sensor) and stays encrypted until it reaches the other side of the internet (server) where it gets decrypted [11], another work proposes and compares new light weight solutions for the IoT including link layer security, IP layer security (IPsec), and UDP datagram transport layer security (DTLS) and gives the pros and cons of each of them [12]. On the other hand, another work focuses on a specific part of the IoT solution that suggests a new wide area concept within the operators Long Term Evolution (LTE) macrocelullar network uplink for intermittent IoT traffic that works simultaneously with the normal LTE traffic in a way that do not greatly affect the overall efficiency of the system [13].

Those and other paradigms have advantages and disadvantages when it comes to cost, complexity, and efficiency. In order to devise a new solution, all of those points need to be addressed and considered in accordance with the Internet of Things core requirements in order to come up with a proposed new satisfactory solution for the Internet of things security.

2. SECURITY PROTOCOLS

In order to understand the current security implementations and their limitations, some network performance terms and protocols need to be defined.

2.1 Network Performance Measures

Network Performance: is the qualitative measure of how well a network service is provided to the end user. Each network is different when it comes to performance as it depends on the structure of that network and its nature. Below are some of the measures that are used to evaluate a network service implementation [14].

Bandwidth In telecommunication, a bandwidth (of a channel) is defined as the range of frequencies the channel provides and is measured in hertz, however, in computing, the bandwidth is the bit-rate available in bits per seconds.

Throughput It is the ratio between the amount of successfully transferred messages and the time it took to transfer those messages. Both the available bandwidth and the signal to noise ratio contribute to the maximum achievable throughput according to Shannons theory [14].

Bit Error rate (BER) The ratio between bits to the bits that have been altered due to interference, noise, or synchronization errors to the overall received bits and it is unitless [14].

Delay In computer networks, total delay is defined as the amount of time it takes the packet to travel from the source to the destination and that includes propagation delay which is the delay a packet experiences due to bits propagating through the medium, transmission delay which depends on the rate at which bits are

put into the medium, processing delay which depends on the rate at which the packets are being processed by the node, and the queueing delay which is the time for the packets to wait before being transmitted by the intermediate nodes. Round trip time (RTT) is a measure of the delay a message experiences when it is being sent from a source to a destination and back to the source.

2.2 Transport Vs Network Layer Security

Security protocols can be implemented in multiple layers of the TCP/IP stack. Although authentication, encryption , and data integrity techniques are available in various protocol suites standards, this section gives a brief explanation of the transport layer security (TLS) and Internet protocol security (IPsec) protocol suite which define the transport layer and network layer security respectively.

2.2.1 Transport Layer Security

Transport layer security and its predecessor secure socket layer (SSL) are enhancements to the transmission control protocol (TCP) and are implemented in the application layer. From development point of view, the TLS/SSL resides in the transport layer as shown in the Fig 2.1 below [7].

SSL enhances the TCP by providing the security services confidentiality, integrity, and client and server authentication. Since the SSL started to become more pervasive, it was used as a secure socket for HTTP application layer messages which made it as a good candidate for end to end IoT security for devices that use the TCP/IP stack. SSL starts with a simple TCP 3-way handshake and then proceeds to server and/or client authentication to exchange the public key. Fig 2.3 shows a typical control messages exchange between a client and a server prior to data message exchanges. In the SSL handshake, the two entities exchange their lists of cryptographic algorithms and hash functions they support and agree upon which ones they are going to use for the session, then they proceed to deriving the session master key from the servers

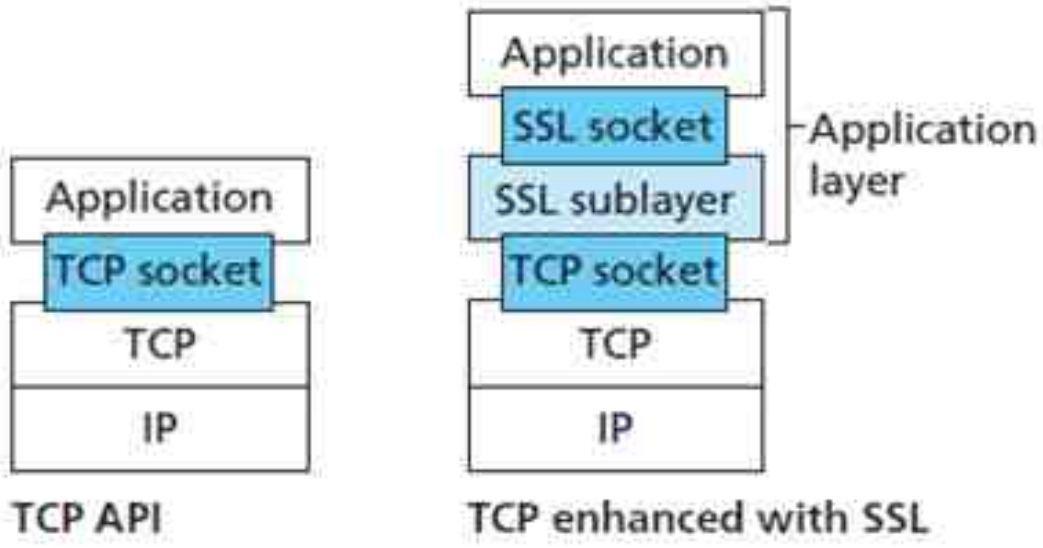

Fig. 2.1. SSL Technical and Development Perspective Layer [7]

public key. The type of messages whether they are handshake control messages, data messages, or connection closure control messages is explicitly mentioned in the header in the TYPE section as shown in Fig 2.2.

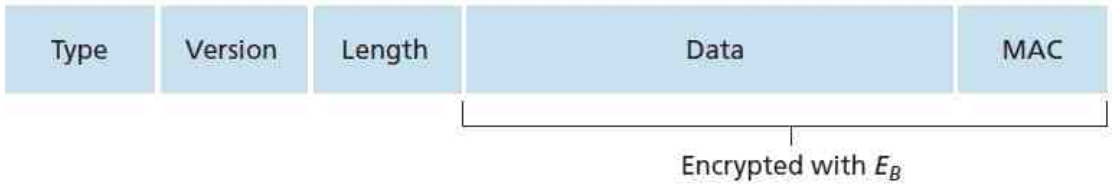

Fig. 2.2. SSL Record [7]

The actual data stream that is passed from the application layer to the SSL socket is divided into chunks called records. A message authentication code (MAC) is then added to each record for message integrity check. This MAC is generated by a hash function that takes the data record and a key as its input. The sender then encrypts

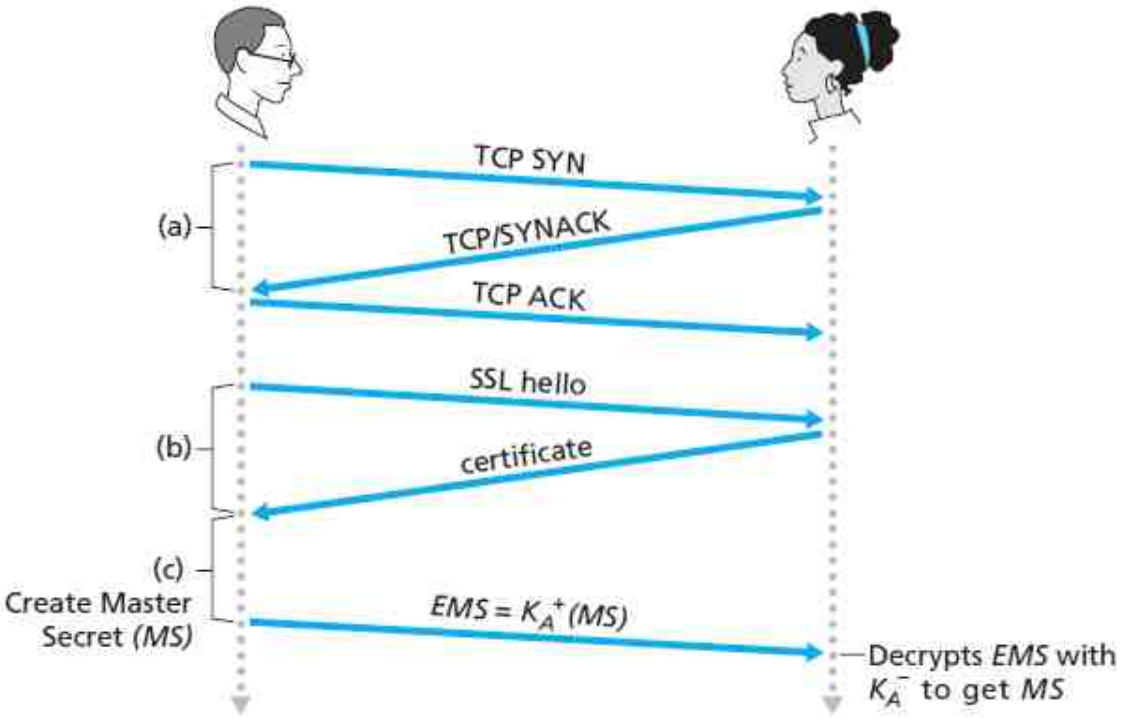

Fig. 2.3. Client-Server SSL Control Messages Exchange Prior to Data Exchange [7]

the data plus the MAC using an encryption key and an additional header at the beginning of the encrypted part to form the whole record format as shown in Fig 2.2.

2.2.2 Network Layer Security (IPsec)

While SSL provides security at the transport layer, Internet Protocol security, also known as IPsec, targets the network layer security. The IPsec does that by providing network layer confidentiality, that is encrypting the payload of the network layer packets and that leads to building a virtual private network (VPN) on top of a public network. Fig 2.4 shows a typical IPsec VPN model [7].

There are basically two IPsec protocols. The first one which is called the Authentication Header (AH) protocol which provides authentication and message integrity

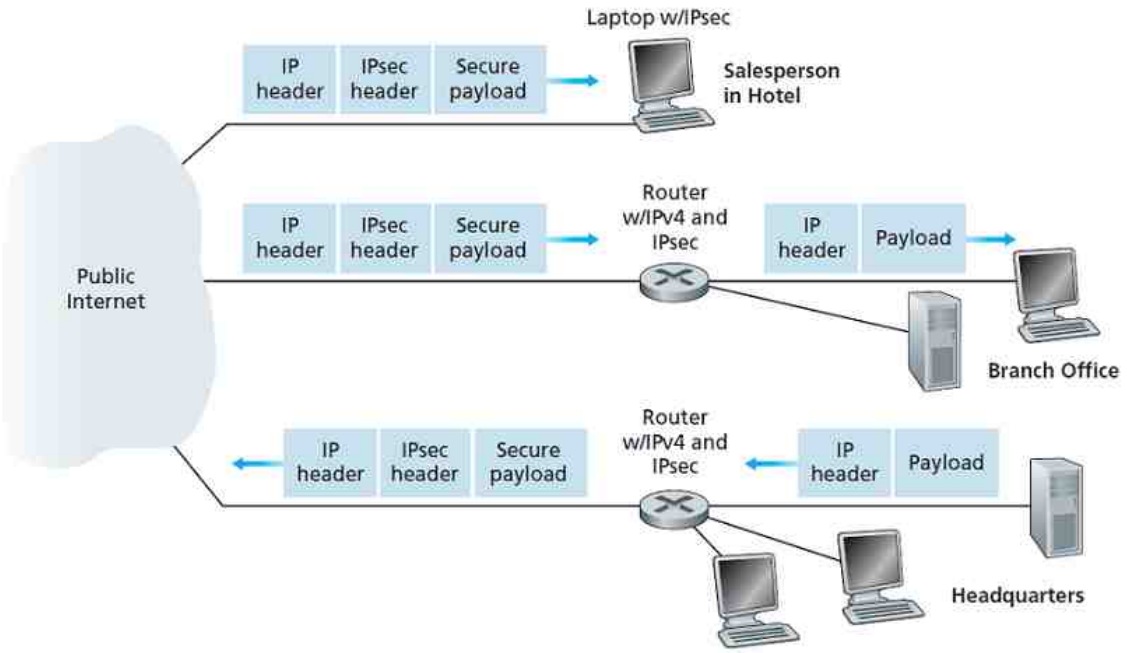

Fig. 2.4. Typical VPN Example [7]

but does not provide data payload encryption (confidentiality), and the second protocol is the Encapsulation Security Protocol (ESP) which provides authentication and encryption (confidentiality) and message integrity. Because of that the ESP is more widely used than the AH protocol [7].

The IPsec uses virtual connections between two entities. The virtual connections are called security associations (SA) and the entities can be any device that uses the network layer like an end host or an intermediate router. A security association is a uni-directional connection, so if bi-directional IPsec connections are required, 2 SAs should be created. Fig 2.5 shows a point to point SA created on intermediate routers R1 and R2 [7].

When a packet is sent from a host in the headquarters network to another host in the branch office network, the ESP protocol performs multiple steps to convert the traditional IPv4 packet to an IPsec packet. First an ESP trailer is appended at the

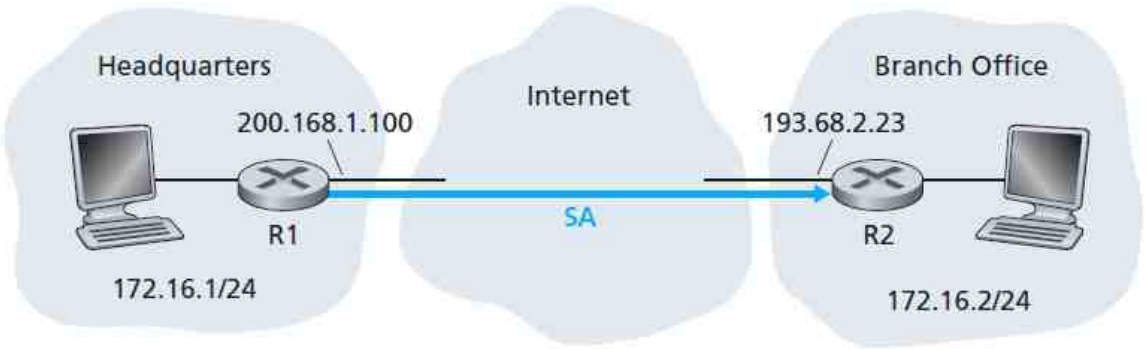

Fig. 2.5. R1 to R2 SA (uni-directional) [7]

end of the IPv4 packet and then the whole combination is encrypted, an ESP header is then appended at the beginning of the outcome and an overall MAC is added to the end for message integrity, the result is the payload of the new IPsec datagram. At last, a new normal IPv4 header is added to the beginning with the new IP source and destination addresses. The source and destination IP addresses are the IP addresses of R1 and R2 interfaces that are connected to the public networks respectively. An IPsec datagram is shown in Fig 2.6.

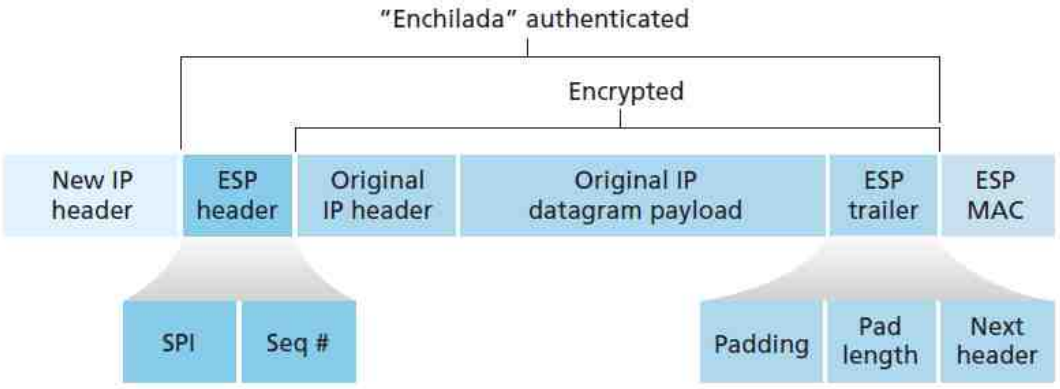

Fig. 2.6. Typical Tunnel Mode ESP IPsec Datagram [7]

3. AIM OF THE THESIS

3.1 Problem Statement

Internet of Things networks are currently being implemented in many enterprise and home environments. The opinions about the Internet of Things burst are vacillating and there is still no confidence in the available security solutions (see [15]). Some surveys like [16] show multiple security flaws that are deleterious to the development of the Internet of Things. There are currently numerous implemented and proposed solutions to secure the Internet of Things. Many of them are rather complicated or do not provide a robust solution for low power devices that use Wi-Fi connectivity. This emergence of the Internet of Things will be hindered without finding an easy, simple, and feasible solution that facilitates the ubiquity of such networks in every environment with minimum efforts.

3.2 Aim of Thesis

The aim of this thesis is to propose a new feasible easy-to-implement solution that uses the current infrastructure of the Wi-Fi networks to form a paradigm that proves secure, and saves bandwidth, delay, and energy consumption which are the main pillars for the Internet of Things applications.

3.3 Methodology

The proposed solution uses a DD-WRT router to manage the PWPA and IPsec security, a Thingspeak server on a Linux machine as a cloud application, and multiple Freescale K64f embedded systems to simulate a typical Internet of Things scenario. The three security services: confidentiality, integrity, and availability will be analyzed.

The data will be collected and statistically studied and compared with an end-to-end security solutions, Secure Socket Layer, for bandwidth, delay, and energy consumption improvements. It is important to note that it is assumed in this work that the adversary does not have physical access to the routers in which they can log in to the router or simply disconnect the connectivity or unplug it to remove the service as such actions will easily be noticed by the administrator.

4. PROPOSED SCHEME ARCHITECTURE

4.1 Introduction to Wi-Fi Wireless Networks

Local Area Network (LAN) is a group of computing devices communicating with each other through a communication link. This LANs shared communication channel can be anything from a simple coaxial cable to a wireless channel that devices can connect to through a wireless access point. While a wireless communication link offers easier installation and more flexibility, but without proper considerations it can be much more susceptible to attacks and security breaches.

The Wi-Fi is only one of the many wireless local area networking products and it follows the Institute of Electrical and Electronics (IEEE) standards to allow computing devices like Laptop devices, mobile phones, wireless sensors, gaming consoles, wireless sensors, etc. to communicate. It utilizes the 2.4 GHz or/and 5 GHz frequency bands.

These devices can get access to the Wireless Local Area Network by connecting to a wireless access point and upon authenticating, they can get access to the network resources whether it is a simple device in the network as a printer or a scanner or this resource can be as be any host that is connected to the Internet if this wireless access point routes the traffic to the Internet. Usually wireless access points have an indoor range of about twenty five meters and a much larger range in the outdoors where there are less obstacles to attenuate the signal. The access point can cover a limited area of a single room, floor, or a building depending on the strength of signal and how much blocking the walls impose, whereas if multiple access points with overlapping coverage a range of many miles could be achieved. Since the wired Local Area Networks require their signals to be transmitted in wires between the network elements, then they provide more security than the wireless where the signal

is transmitted as radio waves in the shared medium (air) and any adversary with a network interface card (NIC) can have access to the network and receive the wireless signal. So within this network, and hence the wireless access points usually operate on the network layer only, unless the communicating devices are using some kind of transport layer encryption like Secure Socket Layer (SSL) or Transport Layer Security (TLS) then the data is as secured as the network layer security used.

Since the 802.11 standard emerged, it used many security schemes. Starting with the Wired Equivalent Privacy (WEP) that uses an RC4 algorithm to encrypt the messages exchanged. The size of the seed plus the incorrect implementation of the cipher were the security weak link which made the WEP unreliable to secure the wireless traffic. Later, the 802.11i standard brought into light the Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). Those schemes basically have two modes of operation. First, the Enterprise model which demands a data base and an authentication server (AS) that usually uses 802.1x RADIUS or DIEMETER protocols to be setup and maintain which is a task that is usually costly and requires some expertise. The AS then does the authentication with the wireless devices by sharing a Master Key (MK) and then independently they derive a Pairwise Temporal Key (PTK) that both the access point (AP) and the wireless device will use for further messages encryption and authentication (integrity).

The second model is the WPA Personal model that uses for authentication a Pre-Shared Key (PSK). This key uses an 8 - 63 character phrase to crate the symmetric keys that are going to be used for further encryption. Depending on the strength of the password, it is possible that the key can be broken in a matter of hours by the use of offline brute force dictionary attacks after sniffing the messages exchanged between the AP and the client when the client gets de-authenticated and then tries to get re-authenticated. Several software utilities such as aircrack-ng and Cain and Abel, AirSnort, and Wifite can be used for such purpose. The efficiency of such utilities are bounded to the strength of the passcode used by the WPA personal model as the stronger the passcode the more time it takes to hack the network. Now, one issue with

the WPA personal model is that the symmetric key administration and its generation, renewal, and distribution in case of a network security breach cumbersome and is not easy to perform especially if the setup is of more than a couple of devices connected to the network. So a new improvement needs to be implemented to solve this problem.

The aim of this work is to propose and implement a new algorithm that solves, in a seamless way, the problem of WLAN WPA/WPA2 pre-shared key generation, distribution, and administration by changing the passkey proactively and automatically with the trusted clients without any required intervention from the users using only the same DD-WRT access point that is used to provide the connectivity in the first place.

The flow of the following sections is as follows: Section 4.1 is an introduction to wired and wireless local area networks and a brief introduction of the current wireless security schemes. Section 4.2 emphasizes the problem of the inefficient key management in the Wi-Fi WPA/WPA2 personal model. Section 4.3 surveys some of the related work in that area. Section 4.4 inaugurates the proposed algorithm meant to solve the problem in the security of Wi-Fi networks. Section 4.5 illustrates the complete system design. Section 4.6 assess the proposed solution by doing a case study that examines the enhanced scheme.

4.2 Key Administration and Management Problem

Since the security of the Wi-Fi WPA personal security model is as powerful as the strength of the symmetric pre-shared key used, hence, there are some scenarios where an adversary with modest resources can use offline dictionary attacks to recover the key and attack the wireless network. One possible solution is for the administrator to manually log in to the router when a suspicious activity occurs in the network and changes the password to a relatively long and hard password, then manually distributes the new pre-shared key with all the trusted devices.

This manual hideous process takes a lot of time and needs to be done again whenever another suspicious activity occurs. This solution is obviously time and resources consuming and leaves the wireless network open for attackers.

Even if a new password is generated, during the process of distributing the new key to all the trusted users and with the current implementations like QR codes, a mouth word, or paper-printed passwords can easily be misused and hence defeats the whole goal of changing the passkey in the first place as the network supervisor will have to re-do the process all over and that can be frustrating.

4.3 Related Project Work

Many of the current works target the alleviation of the wireless Wi-Fi network management and key administration problem but less success has been achieved to date. Maybe one of the best work is the WPS (Wi-Fi Protected Setup) which was introduced in 2006 as a simple Wi-Fi configuration setup. This scheme allows key distribution to simple users who do not know much about security approaches and get annoyed by entering long strong passkeys by using a pin, push button, near field communication (NFC), or the USB methods. This implementation is vulnerable to multiple offline and online brute force attacks where the PIN and hence the encryption key can be cracked. While the WPS helps a little with the key distribution, it does not by any means solve the trigger for key generation and change in which the case all the users will have to go physically to the AP to get the new code.

There are other recent solutions that try to assist with the network security management like the KissWiFi that manages the connected users by using MAC (Medium Access Control) access list and binds them to NFC tags and choosing the first user as an administrator. Such mechanism can lead to many flaws including the simple traffic dump then MAC address spoofing by the adversary to masquerade as a legitimate user and sometimes as an administrator.

Another recent work is the FlexiWi-Fi security manager which uses an Android application, an Infrared (IR) transceiver, Bluetooth (BT) transceiver, and an embedded system to control a DD-WRT router to generate a new key and then distribute it to legitimate users. While it is a good proposal for the problem solution, it still requires some user intervention and extra hardware to be added to the system.

4.4 Proposed Security Solution

The proposed scheme is to use a proactive WPA/WPA2 approach. The DD-WRT router generates a new fixed length random password every preset time interval (two hours by default) then uses this strong password as the new pre-shared key. Before the password change occurs, every connected user will automatically open a TCP connection over the same secured Wi-Fi link and fetch the new password and the time until the new password will be applied (current password timeout). In that case, when the timeout occurs, all the wireless devices in that network will seamlessly change the password and hence no need for any user intervention. For simplicity, the first time the users get connected to the router should use either a Bluetooth transceiver [16] or a simple NFC then after that the proactive WPA/WPA2 scheme will take over to change the password in the router and all the trusted already connected devices Fig 4.1 and Fig 4.2 show the flowchart of the router and a trusted connected client.

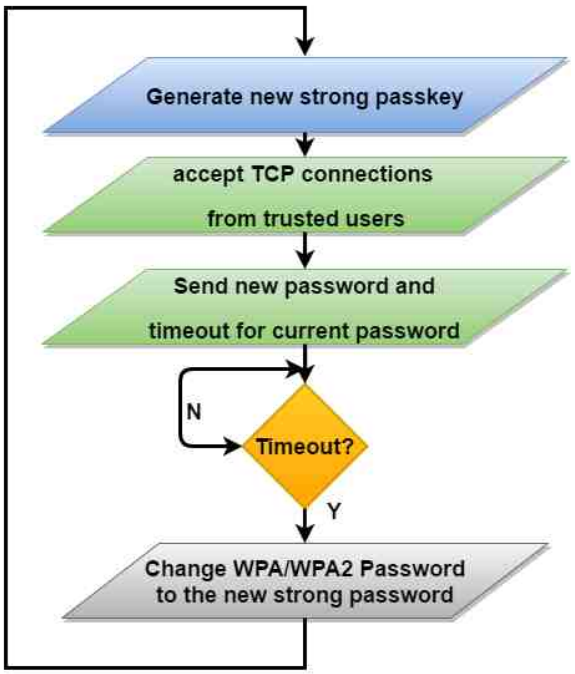

Fig. 4.1. DD-WRT Router Simplified Flowchart

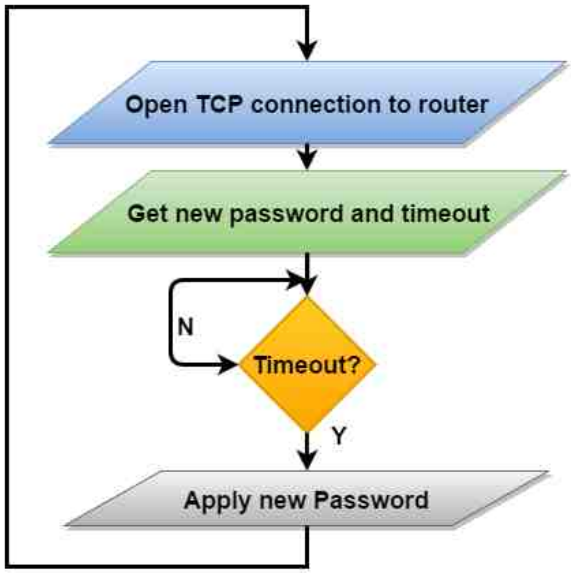

Fig. 4.2. Trusted Client Simplified Flowchart

4.5 Detailed System Design

The hardware system design is very simple as no explicit extra hardware needs to be added unless the router does not support DD-WRT software in which an embedded system is needed. To get connected for the first time, users can simply enter the current password or use an NFC to get authenticated and connected. Then the router generates a predefined length (15 characters by default) strong random password that incorporates multiple techniques for strong passwords generation like mandating the choice of some special characters and different upper and lower case letters. Each of the connected users then open a TCP connection to the listening server which provides the new password and a timeout for the current password expiration. The router can be set to accept connections to as many users in the network so that no TCP SYN connection initiation request will be rejected. The router and clients operate normally after that until the timeout occurs. When the timeout occurs, the DD-WRT router applies the new distributed password and all the clients apply the new one as well. All the operations are seamless and in case any of the devices gets disconnected, it will try to connect with the newly advertised password from now on. The above explanation shows that except for the first time connection (Mandated by the WPA personal model) everything else is done automatically by the code on the DD-WRT router and the connected clients and no user intervention is required.

The code used for this implementation was written using C/C++ programming language and an online compiler. The router used in the implementation of the suggested solution is a Buffalo router but any simple DD-WRT with enough space to receive TCP connections can be used.

4.6 Schemes Security Analysis

Since the proposed solution does not change the basics of the WPA/WPA2 personal model, it uses all the strength points of that model and adds to that some enhancements to target its weaknesses. The proactive approach for changing the

password for the whole network eliminates the possibility of an attacker capturing a handshake messages exchange and trying to use offline dictionary attacks to get the password. Taking into account the considerable amount of resources (Including time) that requires an adversary to get the password, by then our system had already generated and distributed a new strong password along with a new timeout and thus it would be meaningless for an attacker to perform offline dictionary attacks.

Our scheme uses the already secured WPA/WPA2 connection to distribute the next-to-use symmetric key and its timeout over the TCP connection. This approach eliminates the need for public key cryptography protocols like Diffie-Hellman for unsecure channel secret key exchange and thus simplify the overall system design. Compared to the other related works (except FlexiWiFi manager), this approach can treat the weaknesses of the WPA/WPA2 personal model instead of partially increasing the security level that is done by simpler defense techniques like MAC address filtering and hidden SSID. While this design is way simpler than the FlexiWi-Fi manager as it does not require any extra hardware such as BT, IR, and an embedded system, the two systems can actually work together to form a whole administration system for the WPA/WPA2 wireless network by using the IR commands to trigger manual password changes while the automatic proactive approach continues in the background. Nevertheless, this scheme can be used as a standalone scheme for secure Wi-Fi networks.

4.7 WPA Versus WPA2

The encryption and message authentication methods used in WPA2 are more advanced than the ones used in WPA. WPA2 uses advanced encryption standard (AES) with CCMP (Counter mode with Cipher-Block-Chaining Message Authentication protocol) which takes more processing power and require a hardware and software upgrades from WEP designed devices while WPA uses TKIP for encryption and MIC. The TKIP encryption takes a few processing cycles (less than 5 instructions/bytes [17]) and thus consumes less processing power, and devices that support

WEP can easily support WPA with a firmware upgrade. There are multiple attacks on WPA implementations but most of them require some conditions to be met, for instance the Hole196 [18] is a man in the middle attack that requires the adversary to have the passphrase to recover another devices shared key with the access point. Other attacks like Michaels and Beck and Tews attack requires the quality of service (QoS) setting to be enabled in the network to facilitate the attack, in that case an administrator can easily disable this setting to render those attacks unfeasible [18].

The choice of WPA or WPA2 depends entirely on the available devices in the network as some devices have the AES implemented in the hardware and can efficiently make use of the processor without a large overhead.

Whether the Internet of Things access network uses PWPA or PWPA2, it can be created as a separate network in the current infrastructure. To avoid the disturbance with the non-IoT users in the network with the proactivity of the WPA/WPA solutions, a separate and maybe isolated network should be used with the PWPA/PWPA2 implementation. In that scenario, the IoT device can be set only once and then left for the PWPA to take over the security management while the other normal users who are connected to the original network remain intact.

4.8 Proactive WPA/WPA2 Plus IPsec for the Internet of Things Security

To provide an end to end Internet of Things security, an additional component which is IPsec is added. The proactive Wi-Fi Protected Access (PWPA) was suggested as a counter measure to the weaknesses of the 802.11i standard to protect the wireless access network, which means that the data on the rest of the public Internet is still vulnerable.

The Internet protocol security (IPsec) should be implemented between the two access routers (Sensors router and the cloud server router) to achieve end to end security. Depending on the application and the available bandwidth in the end to end network, either the encapsulation security protocol (ESP) transport or tunneling mode can be implemented to provide end-routers data security. Fig 4.3 shows the actual proposed IoT security solution.

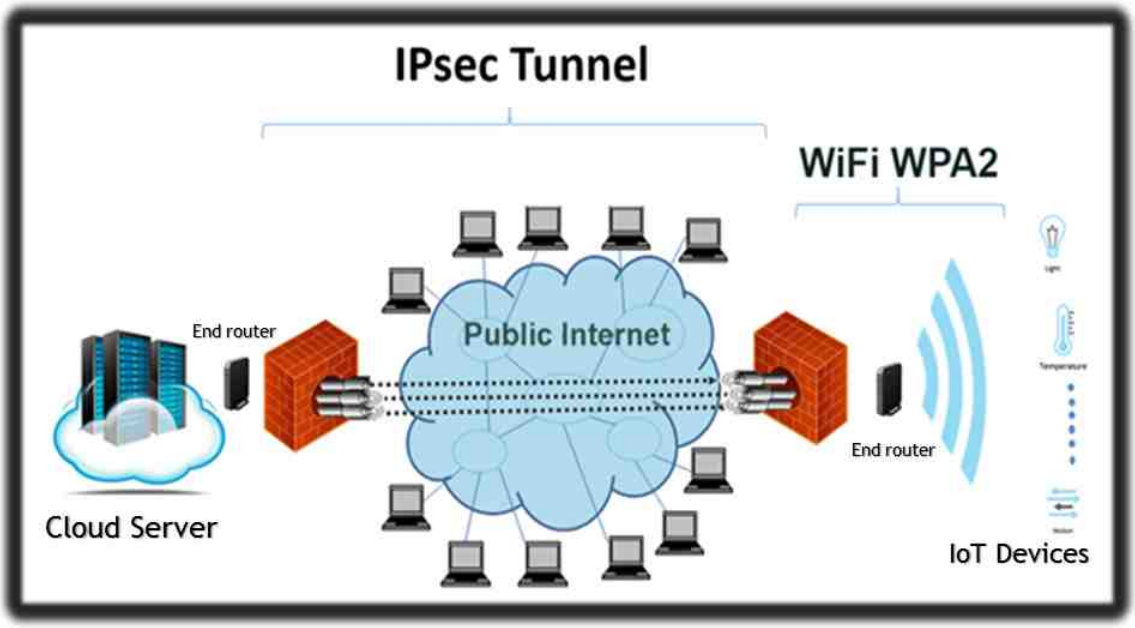

Fig. 4.3. Proposed Security Implementation Solution

5. RESULTS AND DISCUSSION

In order to demonstrate the efficiency of the solution, this chapter illustrates the solution connectivity, configuration, test parameters, and the process by which the data was collected and processed to show the results.

5.1 PWPA Connectivity and Configuration

Fig 5.1 shows the PWPA IoT solution connectivity and its components

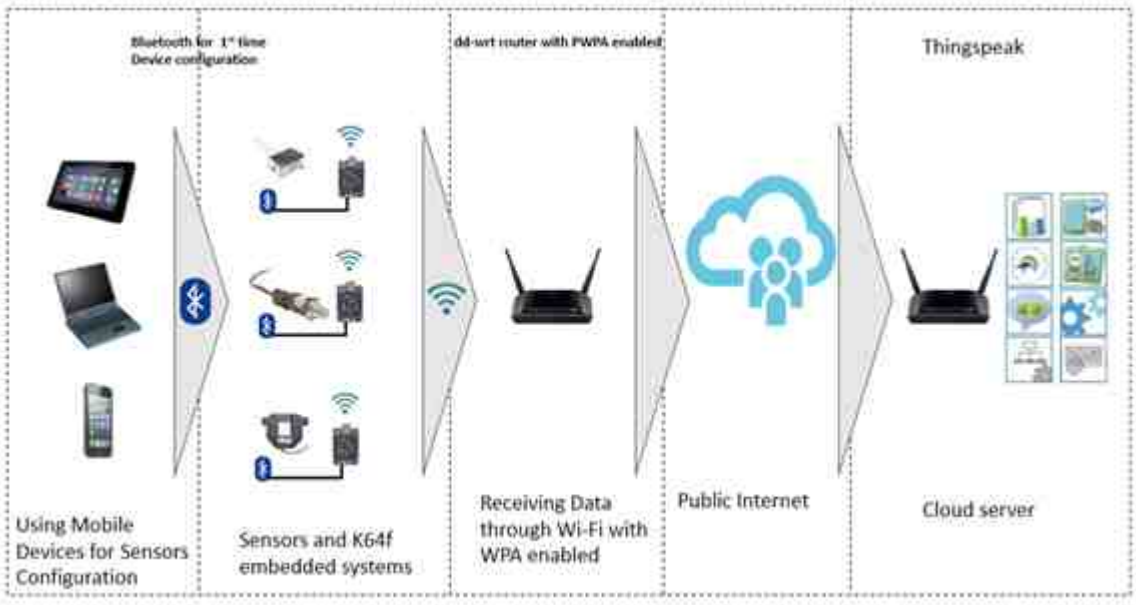

Fig. 5.1. PWPA Solution IoT Connectivity

To setup the IoT sensors and embedded systems for the first time, an Android application was developed and used to fetch the current WPA password and install it in the embedded system using the IR and BT interfaces (see [16]). The security control

is passed to the PWPA solution where the password change will take place between the AP and the connected devices in private channels using the WPA2 security model. Table 5.1 shows the solution configuration and the test parameters used and Fig 5.2 and Fig 5.3 show the embedded system setup and the Android application interfaces, respectively.

Table 5.1
Solution Test Materials and Parameters

Item	**Value**	**Number**
Router	BUFFALO AirStation Extreme AC 1750	1
Router	GL.iNET	1
Router software	dd-wrt	n/a
IoT sensors	Temperature	1
IoT sensors	Pressure	1
IoT sensors	Current	1
IoT embedded system	Freescale K64f	1
Configuration Interface	Bluetooth HC HC-05	1
Data Link Layer	802.11	n/a
Transport layer protocol	Transmission Control Protocol (TCP)	n/a
application layer protocol	HTTP (Persistent and Non-persistent)	1
Access link security mode	Proactive WPA2	1
Password change interval	120 minutes	n/a
Internet security	IPsec	n/a
Cloud application	Thingspeak	1
Packet sniffer	Wireshark	n/a

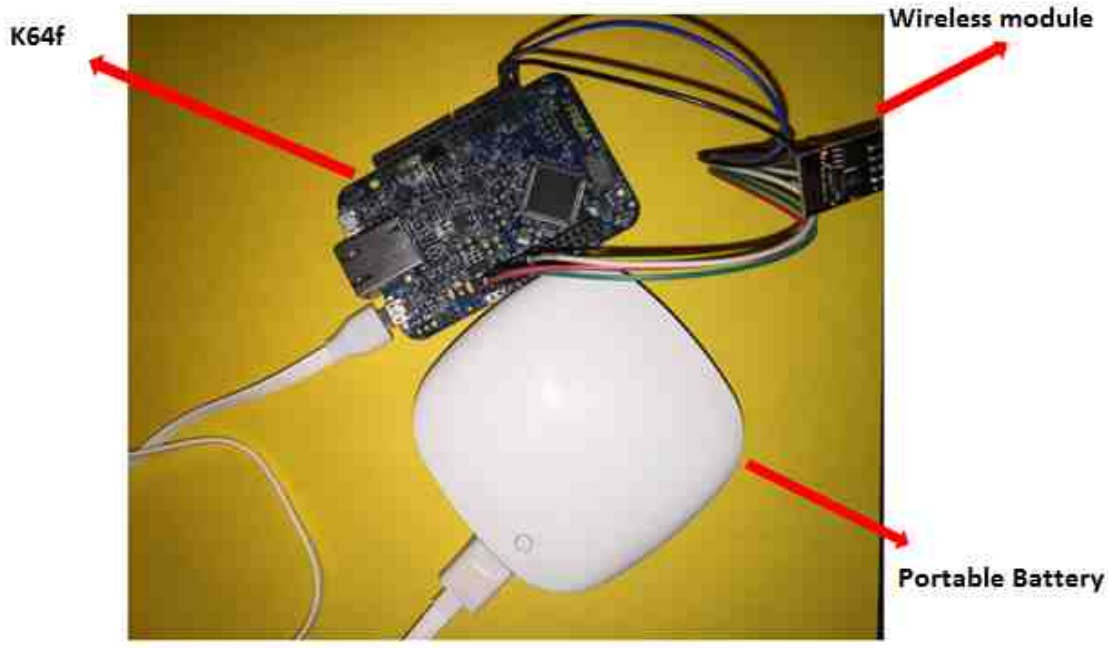

Fig. 5.2. Freescale K64f Embedded System with Portable Battery

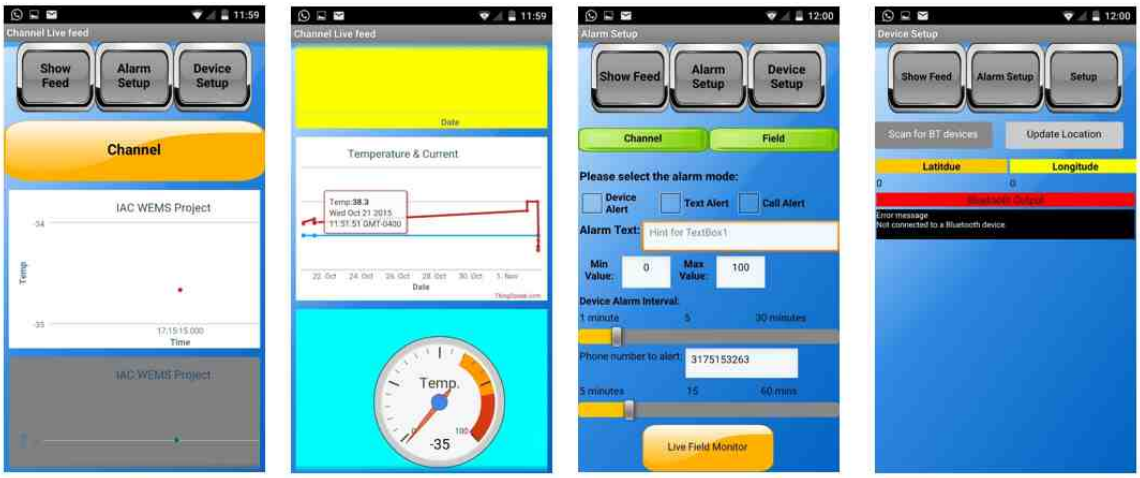

Fig. 5.3. Android Application Used for First Time Configuration

To showcase the solution, the test was run in two scenarios. The first scenario used SSL end to end security where a separate SSL session is initiated between each device and the cloud application. The second scenario used PWPA and IPsec to provide end to end security. The two scenarios were tested with both persistent and non-persistent HTTP as some IoT servers do not support persistent HTTP protocol.

The test was run until the amount of about 5000 HTTP request/response pairs were collected and then processed and analyzed. Fig 5.4 and Fig 5.5 show the two tested scenarios. For simplicity, the dd-wrt router management was handled via a Telnet session by a separate entity (Raspberry Pi) that is connected via an Ethernet cable, however, in practical situations, all the management can be done internally within the dd-wrt router itself.

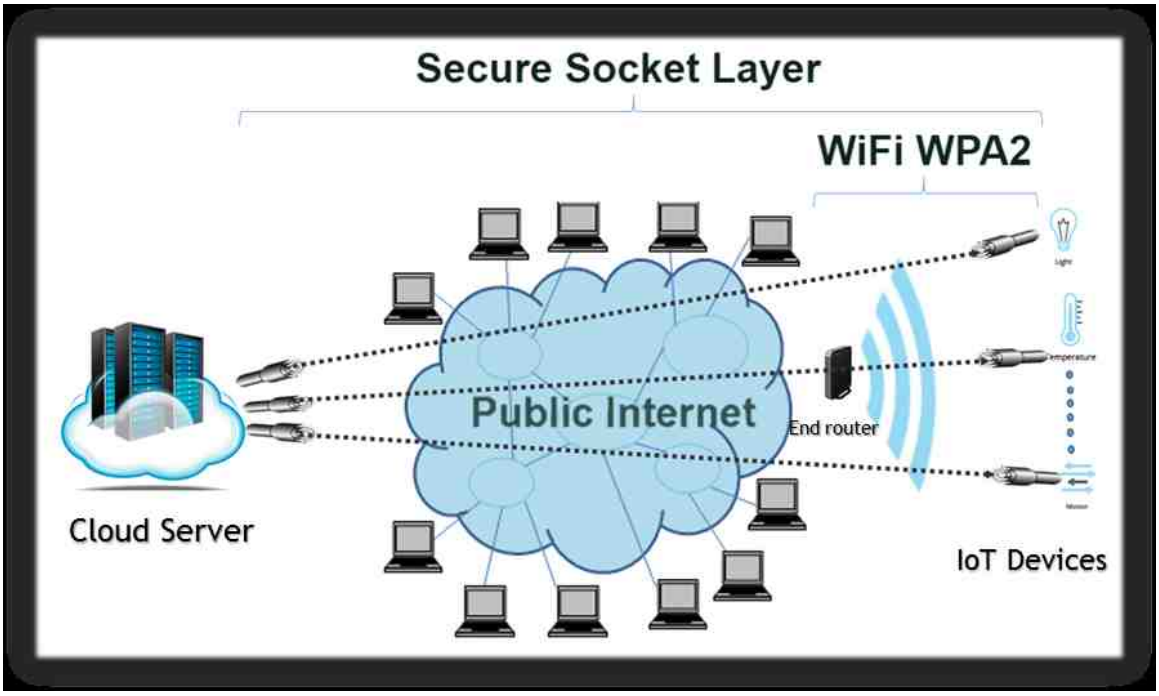

Fig. 5.4. Scenario One Using End to End SSL Security

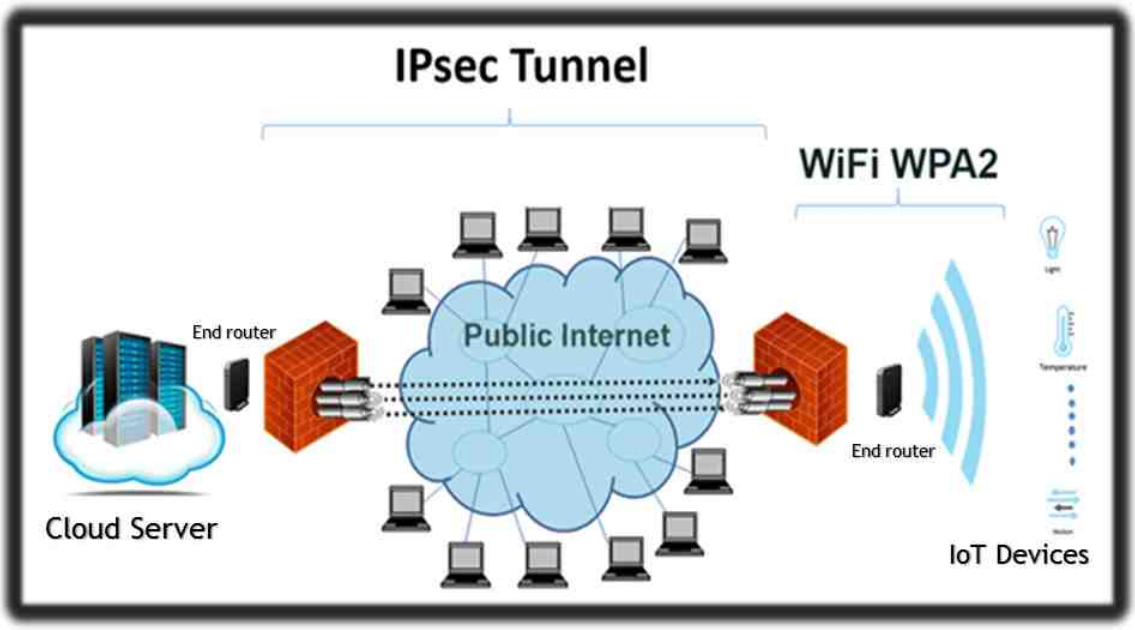

Fig. 5.5. Scenario 2 Uses PWPA and IPsec

5.2 Results and Discussion

5.2.1 Solution Security

To prove the solution to be secure, a brief evaluation of the three cybersecurity pillars: confidentiality, integrity, and availability is discussed both on the PWPA side (access network) and the IPsec side (public Internet). On the PWPA side the confidentiality is achieved by either the TKIP (WPA) or AES (WPA2) encryption and pre-shared key authentication.

Integrity is achieved by using the message authentication codes to make sure that the data is not being tampered along the way. Although the availability has less consideration in WPA and WPA2 networks, some countermeasures can be taken as mentioned in section 4.7 for WPA and in [13]. From the IPsec (end routers) side, the confidentiality is secured by first by mutual authentication and then messages encryption depending on the initial cipher suites negotiation. Integrity is achieved by

using the ESP MAC as well. And since IPsec depends on the Internet for message transfer, an attack on availability (DoS) should be done by attacking the routers themselves, a scenario that will not be covered in this work as mentioned in section 3.3.

5.2.2 Network Performance Improvement

Delay

Depending on the processing power of the device, the processing time and power consumption will vary from a device to another, a multi-core processing unit will perform a function faster but will consume more energy but a device with little processing power will consume less battery life. IoT devices should have a balance between the two to perform efficiently. According to the test parameters mentioned in section 5.1, the IoT devices used are sensors with FRDM k64f embedded systems which have moderate processing capability, the amount of processing reduction when the PWPA solution is implemented will be loosely measured by the amount of delay difference the HTTP requests encounter when compared to the end to end SSL solution (instead of calculating the number of machine language instructions and multiply that number by the bus cycle duration). Although the data was gathered by initiating subsequent HTTP requests and recording their responses, Fig 5.6 and Fig 5.8 illustrate the average delay for both scenarios. To make the graph easier to read, each x-axis values represent a collection of 100 HTTP requests, while the corresponding y-axis values represent the average delay experienced by that request bundle. Fig 5.7 and Fig 5.9 illustrate the overall average delay experienced by both SSL and PWPA/IPsec scenarios.

When persistent HTTP is used, Fig 5.6 and Fig 5.7, a considerable reduction delay (including processing delay) is noticed, as an average of 23.76 milli seconds delay is experienced for each request. While in the case of non-persistent HTTP, Fig 5.8 and Fig 5.9, the overall average delay is decreased by 191.3 milli seconds, which is a substantial delay when sensitive IoT applications are implemented.

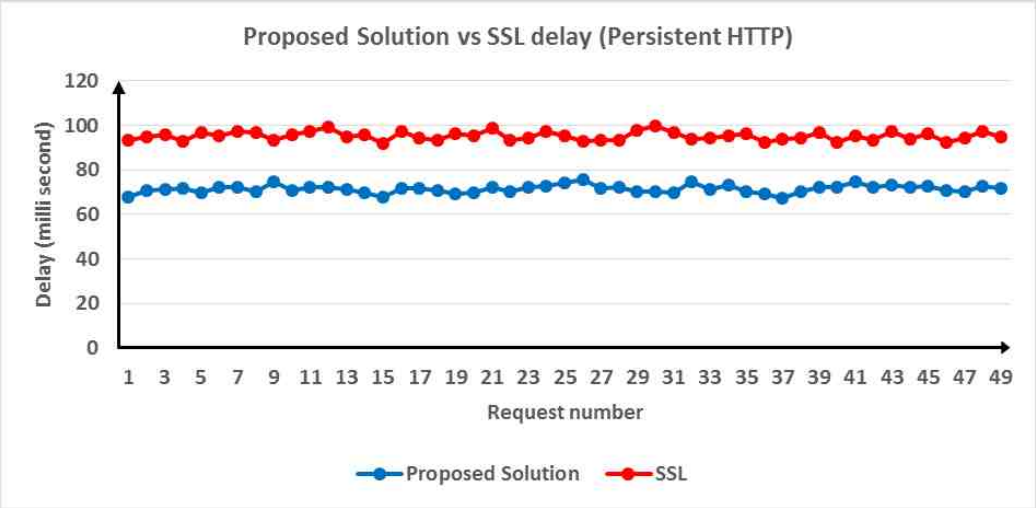

Fig. 5.6. SSL vs Proposed Solution Delay (persistent HTTP)

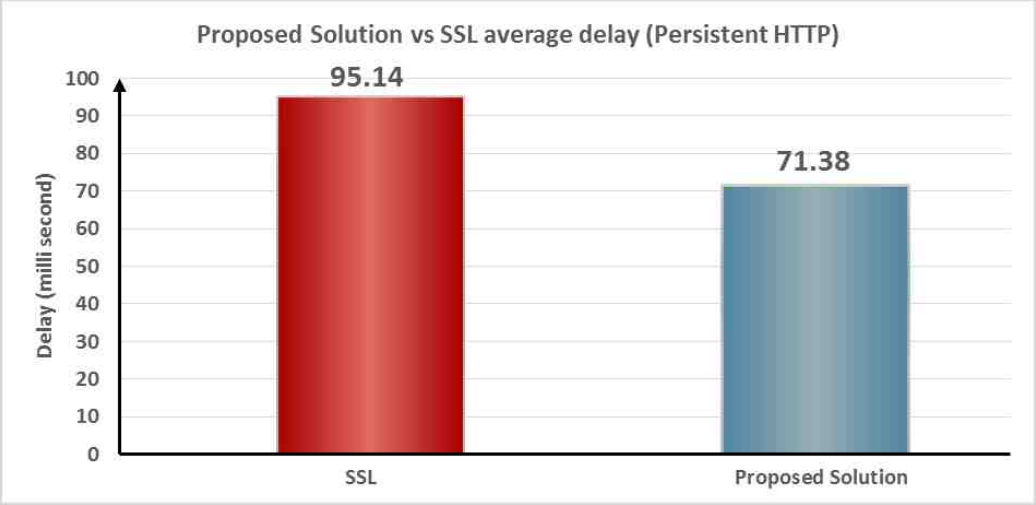

Fig. 5.7. SSL vs Proposed Solution Average Delay (persistent HTTP)

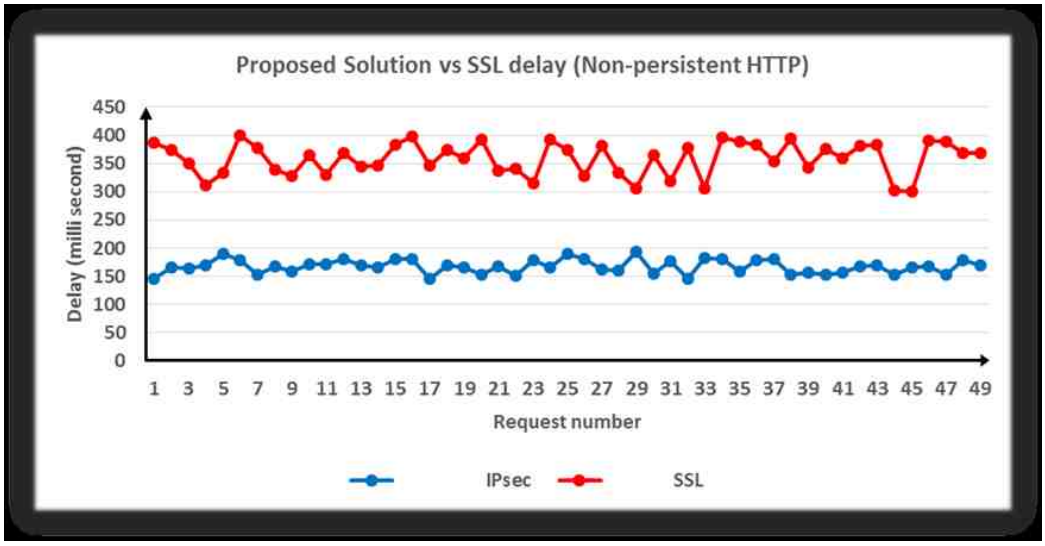

Fig. 5.8. SSL vs Proposed Solution (non-persistent HTTP)

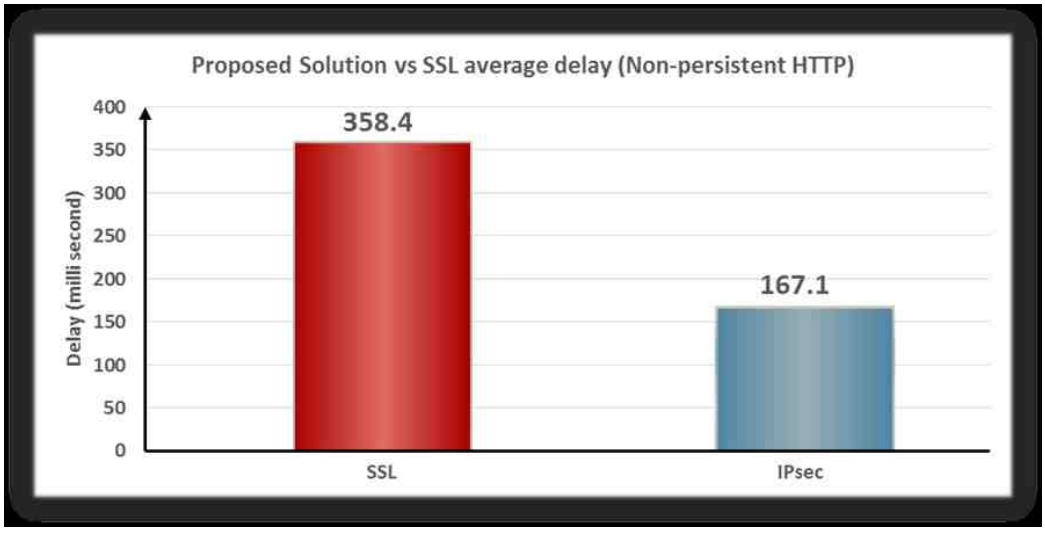

Fig. 5.9. SSL vs Proposed Solution Average Delay (non-persistent HTTP)

Bandwidth Efficiency

Since the end to end SSL scenario uses separate connections between each device and the cloud server (Thingspeak), then there is a separate SSL header for each connection, and that affects the bandwidth utilization in both the access network and the Internet, while in the second scenario (proposed solution see Fig 5.5), IPsec overhead only affects the Internet side and there is no extra headers in the access link side. Fig 5.10 and Fig 5.12, illustrate the average bandwidth efficiency for each 100 HTTP requests by calculating the actual throughput and dividing it by the bandwidth for the persistent and non-persistent HTTP respectively.

It can also be noted from Fig 5.11 case, there is a 2% improvement in the Internet and an even bigger improvement, 12%, in the access link side bandwidth efficiency.

On the other hand, Fig 5.13 shows that when non-persistent HTTP is used, bigger enhancements are achieved when it comes to bandwidth efficiency. This is due to the messages exchanges shown in Fig 2.3 that take place for each SSL connection initiation. Even though the IPsec contains a handshake and connection initiation as well, but it is only a single end router to end router connection instead of separate device to server SSL connection, the messages exchanged when an IPsec security association is initiated are shown in Fig 5.14.shows that the improvement between the two scenarios, a 344% increase in the internet links bandwidth efficiency and 373% increase in the access link efficiency.

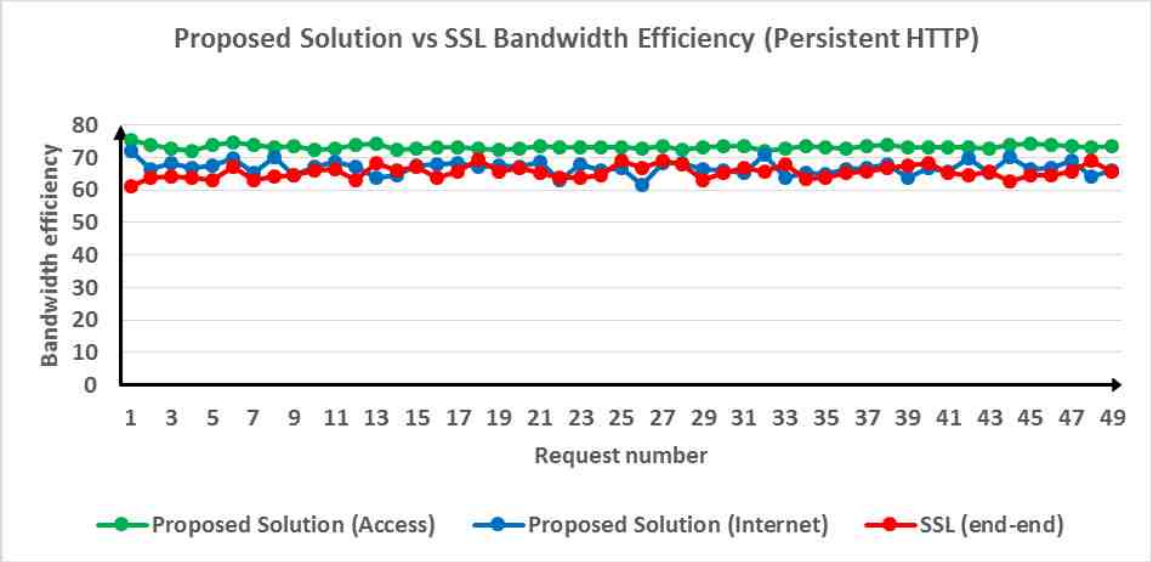

Fig. 5.10. SSL vs IPsec Bandwidth Efficiency (persistent HTTP)

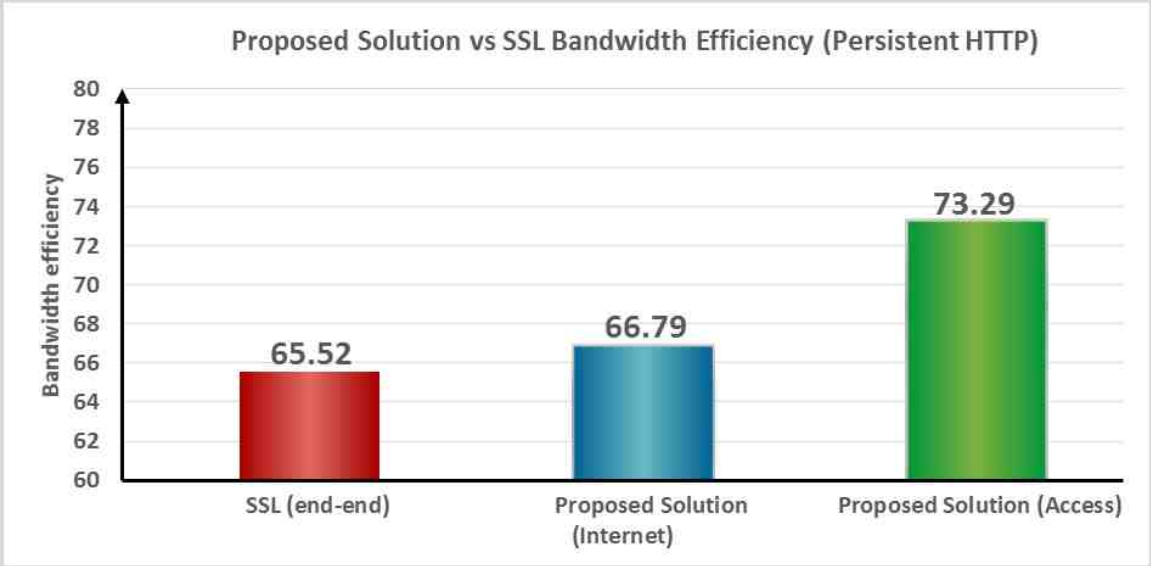

Fig. 5.11. Solution vs SSL Average Bandwidth Efficiency (persistent HTTP)

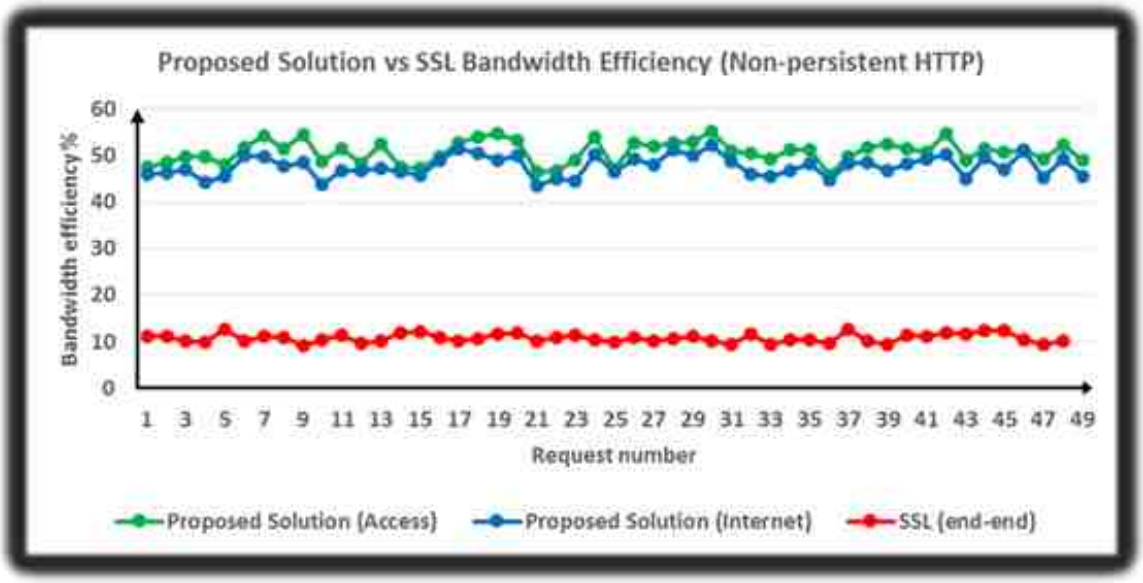

Fig. 5.12. Solution vs SSL Bandwidth Efficiency (non-persistent HTTP)

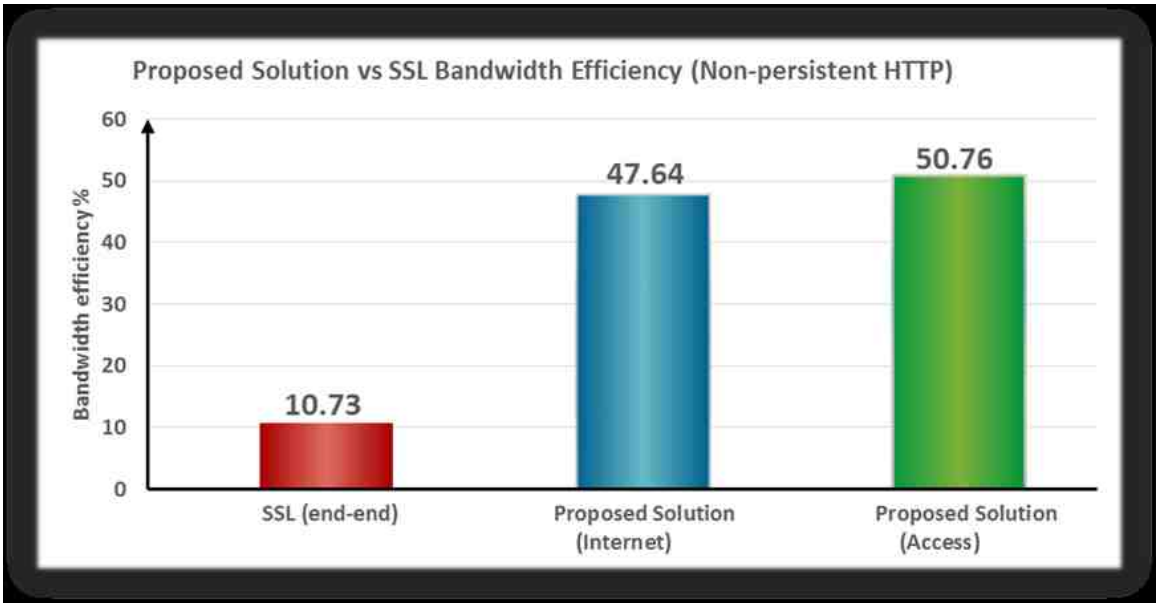

Fig. 5.13. Solution vs SSL Average Bandwidth Efficiency (non-persistent HTTP)

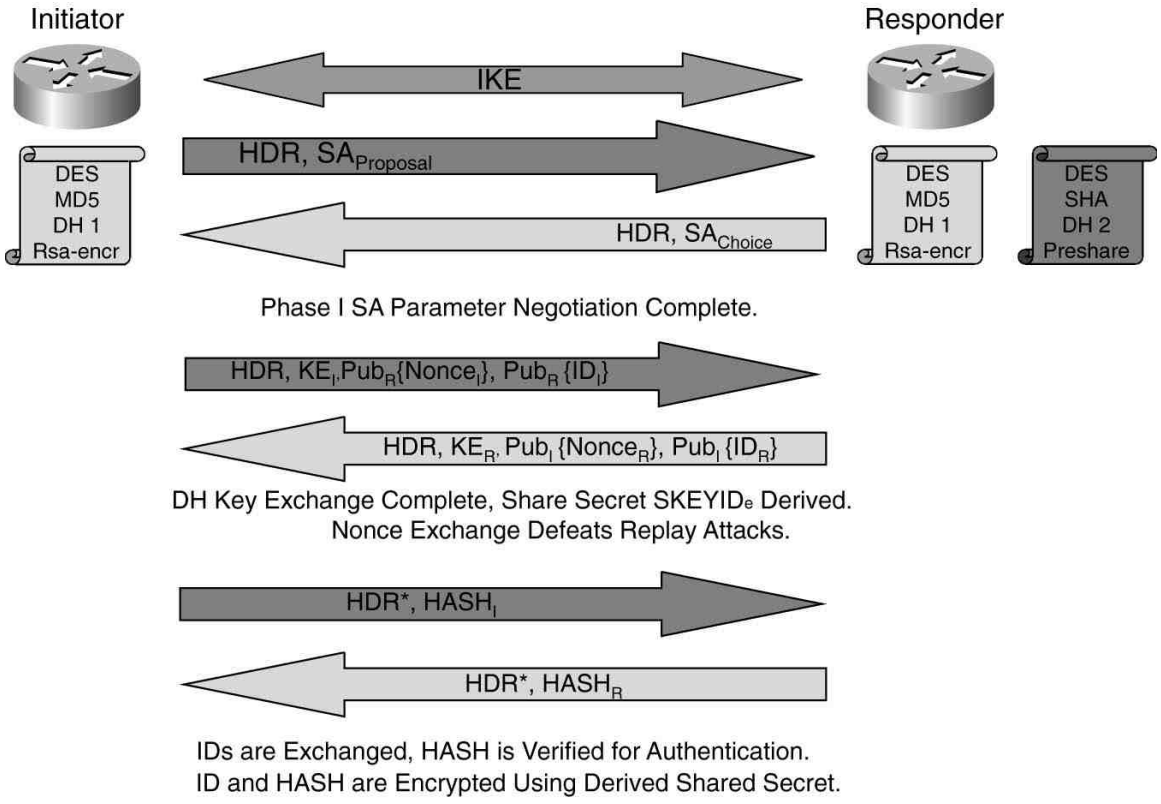

Fig. 5.14. Messages Exchange Between IPsec End Routers

As shown in Fig 5.15, in the case of secure socket layer (SSL), the encryption occurs on top of the transport layer, so an adversary on the internet can see what is inside the transport layer and network layer headers since they are sent in the plaintext. While in the case of IPsec, the original packet is encrypted and then encapsulated in a new packet, which makes all the headers on top of the data link layer encrypted, and that is added security by the proposed solution.

It is important to note here that changing the password on the device after the timeout might require a 1-5 seconds to occur, and although this situation happens once every multiple hours the data can be stored locally and then sent to the cloud after reconnecting, if the product requires real-time sensitive operation then consideration should be taken in regard of such events.

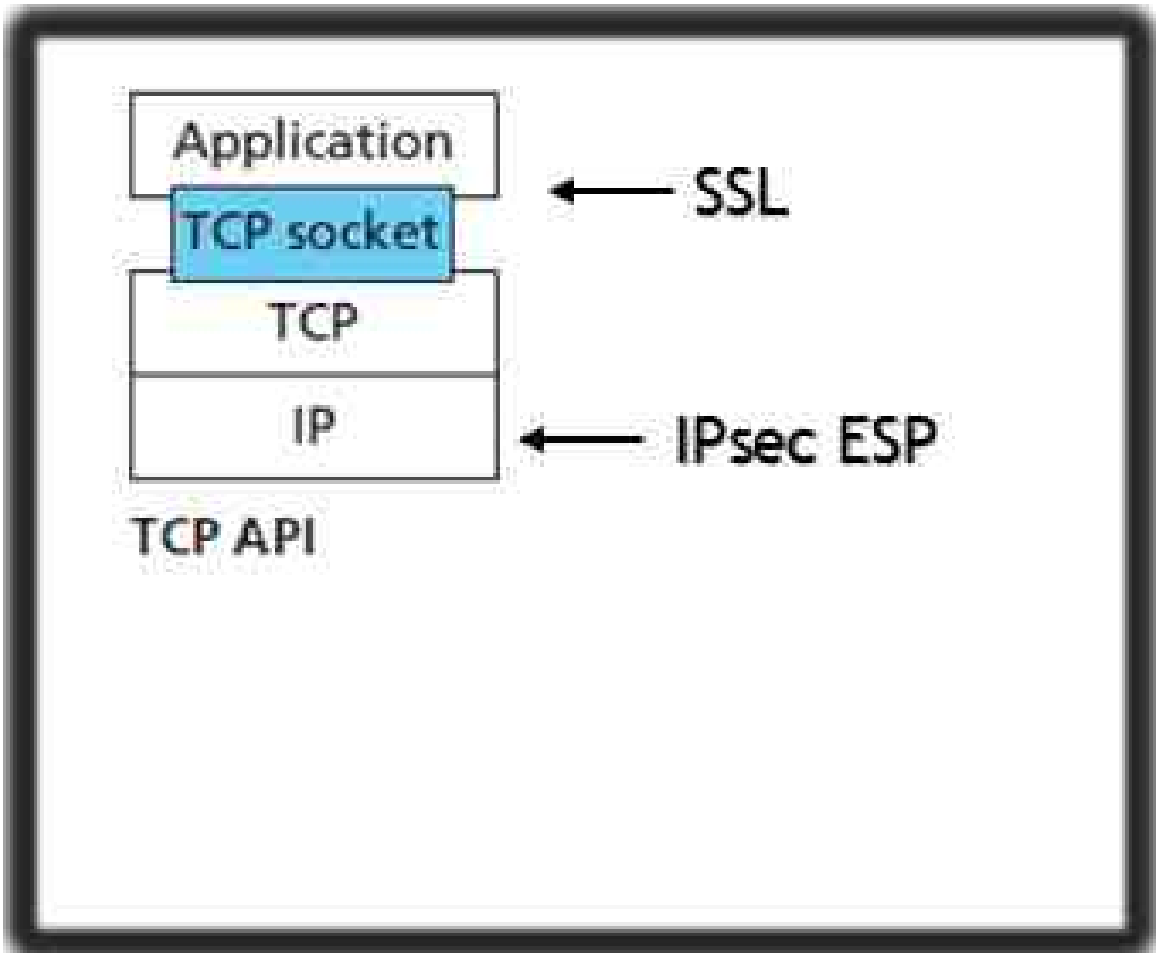

Fig. 5.15. SSL vs IPsec Encryption Layer

6. CONCLUSION AND FUTURE WORK

6.0.1 Conclusion

The Internet of Things is the natural evolution of the Internet. Its fast growing nature and being an integral part in daily sensitive services like industrial, enterprise, home networking, and education raises some security concerns. While the Internet of Things connectivity can be any of the wired or unlicensed wireless technologies like Bluetooth, Bluetooth low energy (BLE), ZigBee, and Wi-Fi, the target of this thesis is to find a security solution for the pervasive wireless technology, the Wi-Fi.

The proposed solution in this thesis is to use a proactive WPA/WPA2 approach in order to secure the access link side of the Internet of Things. The proactive approach is controlled by a dd-wrt router which changes the password proactively after a specific time interval after instructing the connected devices to do so as well. The solution uses an IPsec security on the end routers to ensure the data security on the public Internet side of the connection.

This simple solution allows to use a simple Wi-Fi setup or even better, to use the current Wi-Fi infrastructure which is available in almost every enterprise or home environment where the Internet of Things is needed. A separate Wi-Fi network will be created for the Internet of Things devices so that the current normal users experience will not change.

The solution proved to be secure by evaluating the three security pillars: confidentiality, integrity, and availability. More even, the solution improved the overall network performance by reducing the amount of delay experienced, and increasing the bandwidth efficiency when compared to the end to end security solution using SSL.

By shifting most of the encryption processing from the low power IoT devices to the router which is connected to the mains, the solution reduced the amount of processing done by those devices and thus greatly increases their battery life which is a major concern in the Internet of Things industry.

6.0.2 Future Work

The proposed solution in this thesis used the proactive WPA/WPA2 to protect the access link and IPsec security to secure the data on the Internet side. A possible future work can target the availability aspect of the WPA/WPA2 access networks. While the 802.11i standard has strong measures for both confidentiality and data integrity, but very little work targeted the defense against DoS attacks. Although some intrusion detection systems or other solutions can be implemented, but an integral solution that is part of the Wi-Fi standard should exist.

LIST OF REFERENCES

LIST OF REFERENCES

[1] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, pp. 1–11, 2011.

[2] J. Chase, "The evolution of the internet of things," *Texas Instruments*, 2013.

[3] C. T. Fingar, *Global trends 2025: A transformed world*. DIANE Publishing, 2009.

[4] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1389–1406, 2013.

[5] G. Reiter, "Wireless connectivity for the internet of things," *Europe*, vol. 433, 2014.

[6] R. Y. Clarke, "Smart cities and the internet of everything: The foundation for delivering next-generation citizen services," *Alexandria, VA, Tech. Rep*, 2013.

[7] J. F. Kurose and K. W. Ross, *Computer networking: a top-down approach*. Addison-Wesley, 2007.

[8] S. D. Babar, *Security Framework and Jamming Detection for Internet of Things*. Videnbasen for Aalborg UniversitetVBN, Aalborg UniversitetAalborg University, Det Teknisk-Naturvidenskabelige FakultetThe Faculty of Engineering and Science, 2015.

[9] S. Singh, *The code book: the science of secrecy from ancient Egypt to quantum cryptography*. Anchor, 2011.

[10] D. Kahn, *The codebreakers*. Weidenfeld and Nicolson, 1974.

[11] P. Levis, "Secure internet of things project (sitp)," 2015. Online: http://iot.stanford.edu, accessed 11-April-2016.

[12] S. Raza, *Lightweight Security Solutions for the Internet of Things*. PhD thesis, Mälardalen University, Västerås, Sweden, 2013.

[13] C. S. Bontu, S. Periyalwar, and M. Pecen, "Wireless wide-area networks for internet of things: An air interface protocol for iot and a simultaneous access channel for uplink iot communication," *Vehicular Technology Magazine, IEEE*, vol. 9, no. 1, pp. 54–63, 2014.

[14] Wikipedia, "Network performance," 2016. Online: https://en.wikipedia.org/w/index.php?title=Network performance&direction=next&oldid =716301444, accessed 11-April-2016.

[15] "boycottbenetton," 2016. Online: http://www.boycottbenetton.com/, accessed 11-April-2016.

[16] M. Kamoona and M. El-Sharkawy, "Flexiwi-fi security manager using freescale embedded system," in *Information Science and Security (ICISS), 2015 2nd International Conference on*, pp. 1–4, IEEE, 2015.

[17] N. Cam-Winget, T. Moore, D. Stanley, and J. Walker, "IEEE 802.11 i overview," in *NIST 802.11 Wireless LAN Security Workshop*, 2002.

[18] J.-L. G. Matthieu Caneill, "Attacks against the wi-fi protocols wep and wpa," 2010. Online: https://matthieu.io/dl/wifi-attacks-wep-wpa.pdf, accessed 11-April-2016.