Securing IoT Devices- Bluetooth Low Energy: A Survey

Ganesh Baleri[#1], Chaitanya Bapat[#2], Shivani Inamdar[#3]
#Department of Computer Engineering, Sardar Patel Institute of Technology
Andheri, Mumbai
[1]baleri.ganesh@gmail.com
[2]chai.bapat@gmail.com
[3]shivani.i164@gmail.com

Abstract- After the rise of e-commerce, social media and messenger bots, the next generation of internet belongs to connecting things, gadgets and devices : Internet of Things(IoT). These things range from sensors, security cameras to vehicles, household appliances and machines. In today's fast paced lifestyle it is very difficult to maintain multiple keys for various locks. With more number of keys, comes the possibility of misplacing a key. To connect a lock with a key in IoT we need to use Bluetooth Low Energy(BLE) protocol. BLE protocol is designed to be power efficient and has been popular for transporting data between smartphones and IoT devices, smart homes, medical equipment and physical access control devices. One such vulnerability of BLE protocol is the Man in the Middle (MITM) attack. Ensuring security over BLE is an ongoing challenge and a major research area. This survey aims to analyze different security schemes applied to IoT. We examine different techniques that are aligned with BLE to ensure fundamental security requirement and protect communication and some research challenges. As a possible solution, we propose combination of Image Steganography and Cryptography to overcome vulnerabilities of BLE protocol.

Keywords: Internet of Things, Bluetooth Low Energy, Man-in-the-Middle, Steganography, Cryptography, Smart Locks

I. Introduction

Internet of Things (IoT) is among the emerging technologies that would be the greatest agents to change the modern world. It involves machine-to-machine communications with mobile, virtual and instantaneous connections. Not just typical computing devices, IoT system consists of household devices and many other data-gathering sensors. With IoT, people may control their household appliance with just a touch on their smart devices. In addition, Cisco's Internet Business Solutions Group had predicted the amount of IoT devices to be double (50 billion devices) by 2020.[1]

Although IoT devices may make people's life a whole lot easier, security experts had mentioned their concerns on the potential security problems (The Insecurity of Things), which make the IoT devices among top five security threats in 2015 [2].

Mobile devices that connect to Smart Locks using the Bluetooth Low Energy protocol are vulnerable to various security attacks such as the Man in the Middle attack. Bluetooth Low Energy is designed to be power efficient and has been popular for transporting data between smartphones and IoT devices , smart homes, medical

equipment and physical access control devices. This survey aims at investigating the working of Bluetooth Low Energy Protocol, it's vulnerabilities and techniques that can be applied as a future scope for securing BLE.

Our article is organized as follows, Section II focuses on the architecture of BLE. In Section III we discuss the vulnerabilities existing in BLE. In Section IV we throw more light on the Man-in-the-middle attack and it's relevance in BLE protocol. Section V presents existing solutions in the sphere of IoT devices and BLE protocol. In Section VI we review Steganography as a possible solution to existing problems in BLE protocol. In Section VII a combination of Steganography with Cryptography as a possible solution is proposed and we conclude the article on this in Section VIII.

II. Bluetooth Low Energy Protocol

Bluetooth Low Energy is a wireless technology that is based on low-power consumption and short range communication. As per ABI Research forecasts, there will be a flood of new Bluetooth-enabled devices with a total shipment of 5 billion such devices, and BLE alone constituting 27% of all shipments.[2]

BLE has been widely utilised for applications in the IoT world. While other low power technologies such as Zigbee, 6LoWPAN and Z-wave have made their mark in the market, BLE has greater deployment expectations. [1]

Frequency Hopping is a concept that provides protection against interference from other signals. Pseudo-random frequency switches avoid third party devices from eavesdropping, thus making the conversation secure.

Security at the Link Layer

In this mode, authentication and encryption is done using the Cipher Block Chaining-Message Authentication Code (CCM) algorithm and a 128-bit AES block cipher. When encryption and authentication is used for connection, a 4-byte Message Integrity Check (MIC) is appended to the payload of the data channel PDU. The Payload and MIC fields are then encrypted. Authenticated data is passed over unencrypted channel by using digital signatures. The signature is computed by applying an algorithm that uses 128-bit AES as the block cipher [1]. One input to the algorithm is a counter, which is used in order to provide protection against replay attacks. If the receiver verifies the signature, it assumes that the data have been sent by the trusted source.

Each mode has different levels which describe the kind of pairing that is required (Table 1)[1]

.

Table 1. Security services and features for the security modes and levels defined in BLE.

		Pairing	Encryption	Data Integrity	Layer
LE Security Mode 1	**Level 1**	No	No	No	Link Layer
	Level 2	Unauthenticated	Yes	Yes	
	Level 3	Authenticated	Yes	Yes	
LE Security Mode 2	**Level 1**	Unauthenticated	No	Yes	ATT layer
	Level 2	Authenticated	No	Yes	

For communication over BLE, pairing is an important task. Pairing in BLE is done in 3 phases.

PHASE I- Devices announce their input output capabilities
PHASE II- Generation of STK (Short Term key) which is used to secure distribution of key materials in Phase III. Initially, an agreement is made by both devices on the TK (Temporary Key)
This is done by 1 of the 3 methods:

1. Out of Band communication- eg NFC
2. Passkey Entry- user passes a six numeric digits as the TK
3. JustWorks- not safe from MITM attacks.

Based on the TK and random values generated by both the devices, STK is generated.
PHASE III- Each end-point sends to every other end-point , three 128-bit keys:

1. Long-term key: used for Link Layer Encryption and authentication
2. Connection Signature Resolving Key: used for data signing performed at ATT layer
3. Identity Resolving Key: used to generate a private address based on the public address of the device

The STK generated in PHASE II is used for encryption while distributing these 3 keys
The Security Manager Protocol (SMP) carries out the message exchange of the three phases.

III. Vulnerabilities in BLE protocol

Though BLE provides modes of security, it is still prone to number of vulnerabilities.Let us take a look at few of them.

Potential threats:
Eavesdropping:
Although BLE consists of security modes to protect it against vulnerabilities, there are still some loopholes in the pairing phases. A BLE device is susceptible to being tracked by third party and subsequent eavesdropping. Consider a Bluetooth headset, for instance. It is almost certain that a trust relationship already exists between the headset and a mobile phone. An attacker could use the headset unit number for impersonation and pave the way to gain connection to more powerful Bluetooth---enabled devices. Even if the victim were to delete the encryption/decryption keys on the mobile phone, an attacker could still communicate with the phone by using the ID of the device, which could also be used to brute force the PIN number *offline* using a Bluetooth sniffer. Once an attacker arrives at the correct PIN, it is not difficult to derive the the link key and eventually go on to hijack the device.[3]

Man-in-the-Middle Attacks: Bluetooth devices are prone to man-in-the-middle attacks. When an attacker secretly relays and possibly alters the communication between two devices that believe are communicating with each other, an MITM attack occurs. A 2010 paper by lecturers at the Marthandam College of Engineering and Technology showed that if one could somehow trick the devices to assume that they have been disconnected from each other, then one could use two Bluetooth

modules to act as the master and slave devices, which would in turn make possible packet injection and authentication attacks. In fact, they were able to do so by jamming all frequencies. This experiment demonstrated that vulnerabilities need not always be in the Bluetooth encryption mechanism itself. In this case, a vulnerability was discovered in how devices handle disconnections and reconnections, and by recognizing and exploiting this weakness, the lecturers were able to connect their devices to the victim devices instead of allowing the victim devices to connect to each other. We will further look into MITM attacks in the next section.

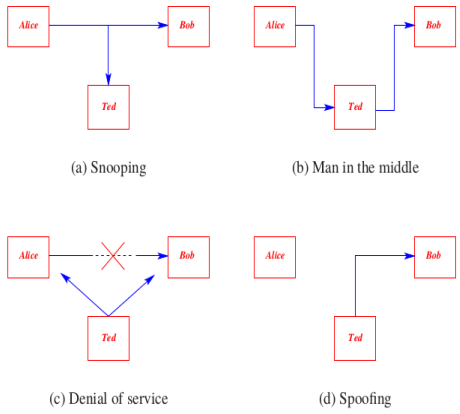
Denial of Service & Fuzzing Attacks

Denial of service attacks make devices unable to receive any phone calls and the battery life is reduced by as much as 97%, a study at the University of Utah has found. They coined this as Battery-Draining-Denial-of-Service Attack. In DoS attacks, a server or system providing some service is attacked with a large number of requests, which subsequently overwhelms the server, resulting in the crash of the system and the eventual draining of battery life.

IV. Man-In-The-Middle attack

According to the book “Introduction to Computer Security” by Hugh Anderson, Threats to Computer System are of following 4 types -

1. disclosure: unauthorized access (snooping)
2. deception: acceptance of false data (man-in-the-middle)
3. disruption: prevention of correct operation (denial-of-service)
4. usurpation: unauthorized control (spoofing). [4]



In order to better understand the working of MITM attacks, the paper “A Survey of Man In The Middle Attacks” was reviewed.[5] The Man-In-The-Middle (MITM) attack is one of the most well known attacks in computer security, representing one of the biggest concerns for security professionals. MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself.

In the MITM attack, the common scenario involves: two endpoints (victims), and a third party (attacker). The attacker has access on communication channel between two endpoints, and can manipulate their messages. The MITM attack can be visualised as shown on Figure 1. In particular, victims try to initialise secure communication by sending each other public keys (messages M1 and M2). Attacker intercept M1 and M2, and as a return sends its public key to the victims (messages M3

and M4). After that, victim 1 encrypts its message by attacker's public key, and sends it to victim 2 (message M5). Attacker intercepts M5, and decrypts it using known private key. Then, attacker encrypts plaintext by victim 2's public key, and sends it to victim 2 (message M6).
As a result, the attacker has convinced both victims that they use secure channel, but in reality it has access to all encrypted messages.

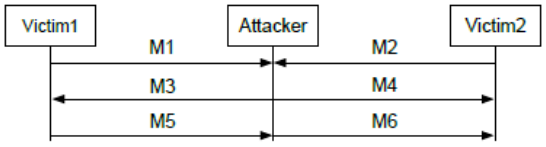


Fig. 1. Exchanged messages in a typical MITM attack.

MITM attack can be executed in different communication channels such as GSM, UMTS, Long-Term Evolution (LTE), Bluetooth, Near Field Communication (NFC), and Wi-Fi.

MITM attack aims to compromise [6], [7]:
Confidentiality, by eavesdropping on the communication.
Integrity, by intercepting the communication and modifying messages.
Availability, by intercepting and destroying messages or modifying messages to cause one of the parties to end communication.

We can identify at least three ways of characterising MITM attacks, leading to three different categorisations:
1) MITM based on impersonation techniques.
2) MITM based on the communication channel in which the attack is executed.
3) MITM based on the location of attacker and target in the network.

V. Existing solutions

Internet Banking is another field where security holds prime importance and similar to IoT devices is vulnerable to security attacks. The paper "Stepping Up Internet Banking Security using Dynamic Pattern Based Image Steganography" highlights the categories of attacks relevant to Internet Banking.[8]

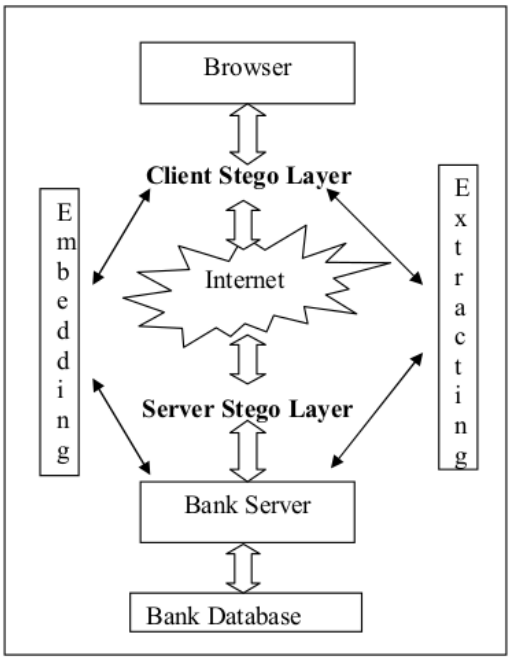
1. Phishing
2. Injection of commands
3. User credentials guessing
4. Use of known authenticated session by attacker.

Man in the middle attack falls under the Injection of commands category. In this attack, attackers intrude into an existing connection to interrupt the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying data. Such attacks are usually selected by hackers against public-key cryptosystems. Quite often in such cases, the victim parties are made to believe that they remain safe in communicating with each other.

AES is the most commonly used encryption algorithm [9] for high end security applications. Recently it has been proven by cryptographers that the AES is breakable [10].

The paper proposes a ‘stego-layer’ method provides solution for Man in the middle attack and Session hijacking. In proposed method a new layer called ‘stego-layer’ was introduced both in client and server side. Any critical data passing to and from the client and server will pass through the ‘stego-layer’. The ‘stego-layer’ uses Dynamic Pattern based Image Steganography algorithm for embedding and extracting message.

Steganography is the art of hiding secret information in media such as image, audio and video [11]. The purpose of steganography is to conceal the existence of the secret information in any given medium.



The functionality of the layer is to hide the information sent between the communicating parties in an image before being transferred.

Geeta et.al [12] in her paper enhances the security level of Mobile banking using Steganography. In this method pixels are chosen according to the key generated and secret message bits are embedded at constant rate in the chosen pixel. This method does not ensure that significant color do not suffer from data embedding and bits are embedded sequentially in all selected pixels which may pave way for steganalyst to easily crack the method. [12]

Hiltgen et.al [13] in his paper targets Man in the middle attack by Short-time password solutions based on a password generating hardware token which are available from various manufacturers such as RSA Security, Active Card or VeriSign. The RSA’s SecureID solution is the most prominent example. It consists of a small device including a LCD display and one button the user can press to initiate the calculation of the next short-time password. [14]

Vulnerabilities with SMS OTP - such as Wireless interception, mobile phone Trojans, SIM Swap Attack through which he can obtain this OTP.

AES encryption algorithm[9] along with Steganography ensures secure and guaranteed delivery of OTP to the intended user. Thus, sending an OTP which is embedded in an image makes it difficult for an attacker to detect the presence of private information. By sending OTP to the intended user through e-mail will protect it from criminals who try to gain the same by

attacking SMS. However, still exposed to phishing attacks via e-mail and cumbersome task of generating OTP.

Short Message Service (SMS) [15] based One-Time Passwords (OTP) were introduced to counter phishing and other attacks against authentication and authorization of Internet services. The attacker's goal is the acquisition of the OTP, and for this he has several options such as wireless interception or mobile phone Trojans. Less known attacks such as the SIM Swap Attack [16] can also be used.

Several studies conducted on mobile malware [17,18] show that authentication credential stealing mobile malware exists in the wild.

VI. **Steganography**

History

Steganography as a principle isn't new. It has been in wide use ever since the Greek messengers existed. The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples in his *Histories*. [19]
Thus in ancient Greece, people wrote messages on wood and covered it with wax that bore an innocent covering message. This practice ensured confidentiality by hiding the message in such a way that it was not immediately apparent, a technique so clever that it was used again by German spies in the 1914-1918 war. This sort of information-hiding is now called steganography, and is the subject of active research. [20]

In contrast to cryptography, steganography does not imply changing the form of the message but rather hiding it in such a way that its existence cannot be perceived. There are several types of steganography – the difference between them being given by the way in which the message is hidden. We cannot speak of the best form, as each method has its role and place accordingly to the type of system to which it is being applied.

Defined as the art of hiding a message, steganography has been used for a very long time and for a while it seemed to be taking a backseat to the new emerging security methods such as cryptography. However, during the past years, the continuous development of the information systems and their increasing need for solid security has brought steganography back into researchers' attention. All the issues that are involved in society, are reflected in similar fashion in industry worldwide. For example, confidentiality problems result in concerns about locks, and encoding and integrity problems result in concerns about signatures, and handshakes.

There are many ways to hide a message. It is mostly common to divide steganography in two types: technical and text. The technical one involves hiding the secret information in stego-files such as images, audio or video.
Text steganography, the method chosen in the present paper, refers to hiding

information within a text. Linguistic methods are divided into several categories depend on how the stego-text is manipulated in order to hide the message. One such category are format-based methods. They use the physical formatting of text and usually modify the text by adding white spaces, deliberate misspelling or resizing the text. Another method is the random and statistical generation, which is used to avoid comparison with the original text and practically means generating your own cover text.

VII. **Proposed Solution**

The security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use.

Cryptography and steganography are the two popular methods available to provide security. One hides the existence of the message and the other distorts the message itself. [21]

Using cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted. In steganography, the data is embedded in an image file and the image file is transmitted. This paper focuses on the strength of combining cryptography and steganography methods to enhance the security of communication over an open channel.
A rather new approach in terms of system's security and also the one used in this paper is to combine cryptography with steganography. When using cryptography alone, the message is encrypted, its form is changed and a key is needed to decrypt it.
Once that key is found by a malicious third party, the information is compromised. With steganography, the message's existence is hidden but the form is not changed. Once someone realizes there is a hidden message in whatever file was used to hide it, the information is again compromised.
However, if the two methods are combined, the security level is much higher as both steganalysis and cryptanalysis need to be performed in order to find the original data.

Combining these methods within the same system is a relatively new direction but we can find several outstanding works in Literature. One such work is presented in paper [22]. The authors
propose a system that will improve the least significant bit (LSB) method, which is probably the most popular steganographic method. The described system has a private key transmitted between the sender and the receiver and used to extract the hidden message.
In the area of combining steganography with cryptography is the system described in [23]. This time, the key necessary to decrypt the message will also be embedded in the steganographic file. The authors of paper [24] propose a security system with three modules: one module for cryptography, another one for steganography and finally a third module for the security of the system as a whole. The encryption algorithm used is AES. In short, the idea is to first encrypt the

data and to later hide the encrypted form in a steganographic file. The same technique, but with different algorithms can be found in papers [25][27][26].
In paper [28] the method used for securing data depends on the type of the communication. Thus, in the case of self-communication – storing digital data, using only steganography is considered to be sufficient. For one-to-one communication or the exchange of information between two parties both
cryptography and steganography are used.
Paper [29] uses linguistic steganography, more specifically the word shift coding protocol, which is combined for better security with the well known encryption algorithm AES. The idea behind the paper is simple – providing an additional layer of protection to a communication network.

VIII. Conclusion

This paper is an effort to review existential security threats in the sphere of IoT, vulnerabilities of BLE protocol and related work around MITM attacks. Having studied the BLE protocol, various issues were found including the possibility of Man-in-the-middle attack. Although existing solutions involve SMS One-Time-Password, Cryptography, Steganography, still few vulnerabilities persist. To tackle the security threats while not compromising on cost and performance, we propose a combined solution of Cryptography with Steganography. According to the study of these techniques, a combination ensures elimination of the disadvantages of the individual methods while retention of the advantages that these principles possess. An implementation of such a methodology can possibly aid research in the field of Security in IoT and fortify the future of BLE enabled IoT devices.

IX. References

[1] Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology. Sensors, 12(12), 11734–11753. doi:10.3390/s120911734
[2] Patel, M. (2016, December 14). Bluetooth low energy (BLE)– the future of retail technologies. Retrieved January 20, 2017, from https://www.einfochips.com/blog/k2-categories/retail/bluetooth-low-energy-ble-the-future-of-retail-technologies.html.
[3] O'Sullivan, Harry. "Security Vulnerabilities of Bluetooth Low Energy Technology (BLE)." *Tufts University*.
[4] Anderson, Hugh. "Introduction to Computer Security." (2004).
[5] Conti, Mauro, Nicola Dragoni, and Viktor Lesyk. "A Survey of Man In The Middle Attacks." *IEEE Communications Surveys & Tutorials* 18, no. 3 (2016): 2027-2051.
[6] CAPEC. (2014) Capec-94: Man in the middle attack. [Online].
Available:
http://capec.mitre.org/data/definitions/94.html
[7] I. Green. (2005) Dns spoofing by the man in the middle. [Online].
Available:
http://www.sans.org/rr/whitepapers/dns/1567.php
[8] Thiyagarajan, P., G. Aghila, and V. Prasanna Venkatesan. "Stepping up internet banking security using dynamic pattern based image steganography." In *International Conference on Advances in Computing and Communications*, pp. 98-112. Springer Berlin Heidelberg, 2011.

[9] Seleborg, S.: About AES – Advanced Encryption Standard (2007), http://www.axantum.com/axcrypt/etc/About-AES.pdf
[10] Biryukov, Alex, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. "Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds." In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 299-319. Springer Berlin Heidelberg, 2010.
[11] Bailey, Karen, and Kevin Curran. "An evaluation of image based steganography methods." *Multimedia Tools and Applications* 30, no. 1 (2006): 55-88.
[12] Navale, G.S., Joshi, S.S., Deshmukh, A.A.: M-banking Security a futuristic improved Security approach. International Journal of Computer Science Issues 7(1,2) (January 2010)
[13] Hiltgen, A., Kramp, T., Weigold, T.: Secure Internet Banking Authentication. IEEE Security and Privacy 4(2) (2006
[14]A. Karia, A. B. Patankar, and P. Tawde, "SMS-Based One time Password vulnerabilities and safeguarding OTP over network," vol. Vol. 3 - Issue 5 (May - 2014), no. Vol. 3 - Issue 5 (May - 2014), Jan. 2017. [Online]. Available: http://www.ijert.org/view-pdf/9806/sms-based-one-time-password-vulnerabilities-and-safeguarding-otp-over-network. Accessed: Jan. 20, 2017.
[15] Mulliner, C., Borgaonkar, R., Stewin, P. and Seifert, J.-P. (2013) 'SMS-Based One-Time passwords: Attacks and defense', in *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer Nature, pp. 150–159.
[16] icici Bank: What is SIM-Swap fraud?, http://www.icicibank.com/online-safe-banking/simswap.html
[17] Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A Survey of Mobile Malware in the Wild. In: Proceedings of the ACM Workshop on Security and Privacy in Mobile Devices, SPSM (2011)
[18] Zhou, Y., Jiang, X.: Dissecting Android Malware: Characterization and Evolution. In: 33rd IEEE Symposium on Security and Privacy (May 2012)
[19] Petitcolas, FAP; Anderson RJ; Kuhn MG (1999). "Information Hiding: A survey" (pdf). *Proceedings of the IEEE (special issue)*. **87** (7): 1062–78. doi:10.1109/5.771065. Retrieved 2008-09-02.
[20] Rawlinson, Henry Creswicke, and John Gardner Wilkinson. *The history of Herodotus*. Vol. 1. 1861.
[21] Joseph, A., and V. Sundaram. "Cryptography and Steganography–A survey." (2011).
[22] Mamta Juneja, Parvinder Sandhu, "An improved LSB based Steganography with Enhanced Security and Embedding/Extraction", 3rd International Conference on Intelligent Computational Systems, Hong Kong, China, January 2013
[23] Chander Kant, Rajender Nath, Sheetal Chaudhary, "Biometrics Security using Steganography", International Journal of Security, Volume 2, Issue 1
[24] Dipti Kapoor Sarmah, Neha Bajpai, "Proposed System for Data Hiding using Cryptography and Steganography", International Journal of Computer Applications, 2010
[25] Arun Kumar Shakar, "Enhancing the Data Security Features of Communication by Means of Media Files through Improvising the Cryptographic and Steganographic Techniques", ASM's International E-Journal of Ongoing Research in Management and IT, 2013
[26] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography", International Journal of Emerging Technology and Advanced Engineering, Aprilie 2013
[27] Partha Pal, Rich Shantz, Kurt Ruhloff, Joseph Loyall, "Cyber-Physical Systems Security – Challenges and Research", BBN Technologies, Cambridge, Available at: http://cimic.rutgers.edu/positionPapers/CPSS_BBN.pdf
[28] Tayana Morkel, "Image Steganography Applications for Secure

Communication", Dissertation Thesis, University of Pretoria, May 2012
[29] Abdelraham Altigani, Bazara Barry, "A hybrid approach to secure
transmitted messages using advanced encryption standard (AES) and
word shifting protocol", International Conference on Computing,