Performance Evaluation of Secure Asymmetric Key Exchange Mechanisms for 4G Networks

Niharika Singh
Department of I.T, CEC
Landran, Mohali

Mandeep Singh Saini
Department of I.T, CEC
Landran, Mohali

ABSTRACT
The 4G network are cellular network which provides higher bandwidth and fast speed but there are few security flaws and thus to protect the users privacy,a very well defined security support is mandatory. The attacker can launch a variety of active and passive attacks. Thus security mechanism is to be defined for call security in 4G/LTE network. The existing schemes includes both plain-text and cryptographic key exchanges. The cryptographic key exchange schemes can effectively establish the secure communications between the two nodes and protect against the node emulation attacks. In this paper the traditional key exchange models of 4G/LTE network and hybrid cryptographic key exchange model and the security provided by these are evaluated. The proposed model will protect the 4G network during the initial call setup phase, periodic time based key exchange to ensure the call security and the seed exchange for the other end integrity check. The proposed model will use a pre-shared key group to ensure the security during the call setup phase and will use the random table based non-predictive key exchange model for the purpose of in-call security assurance and receiver integrity check by the caller. This performance evaluation survey will evaluate these two authentication methods for various scenarios in the 4G network. The conclusion after the comparison would throw light on appropriate scenarios of both the schemes used in 4G/LTE security.

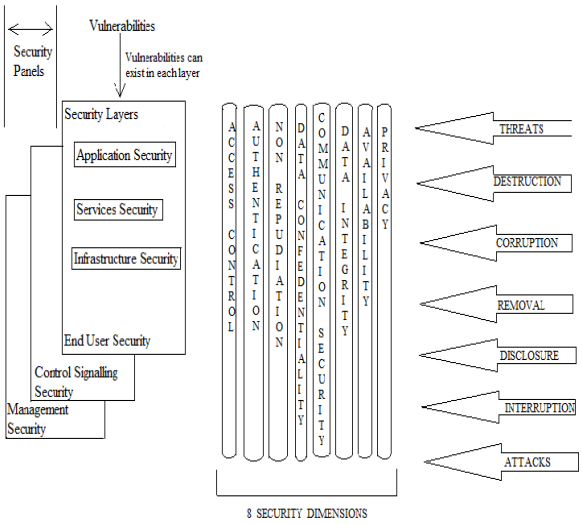
General Terms
Communication, Performance Evaluation, Security, Plain-Texts, Generations, Wireless Systems, etc.

Keywords
4G networks, cellular security, performance evaluation, key exchange models, key management, predictive key management, cryptographic key exchange, etc.

1. INTRODUCTION
Anytime while travelling by a car in some metropolitan city with a small wireless handheld device, a person can perfectly see the entire front of the environment (such as buildings, streets, roads and centres commercial) which also allows to follow different vehicles that come in way to avoid accidents at same time. Era of the next generation of intelligent wireless systems come, actually 4G is the next generation of intelligent wireless systems, is taking shape to do such, the highly intelligent service focused on personalized user as virtual navigation a reality. Industry and research throughout the world, different organizations such as DoCoMo, Vodafone, Nokia, Micromax, Airtel, Ericsson, WWRF, ITU, IEEE, to name a few, advances the 4G wireless systems to hit the first commercial market in 2010. From 1970, the evolution of network systems when the design of analog systems oriented first generation voice (1G) began. The transition to the second generation (2G) data, systems-oriented digital voice in 1991 and thus began multi-service mono prior service time platform.

Low data rate and mono-media systems such as GSM, cdmaOne, TDMA IS-95 and are still in force in many parts of the globe. Between 2G and 3G ,the 2.5 G systems (GPRS) act as an intermediate step, providing increased capacity channel, much better throughput and data rate and data transmission by Internet service packages optimized improving different devices wireless. The advanced multimedia era began when the transition to 3G systems were sold in 2002 where more person interactions are widespread. Packet core network systems such as cdma2000 and WCDMA offer higher channel capacity,2 Mbps data which is a high speed, also transmission through multimedia is of high speed and international roaming through a cellular network. This period marked the beginning of e-commerce and generation of full revenue through huge multimedia Internet applications. The situation for 3G systems has become more complicated as there do exists some positives and negatives of HIPERLAN, WLAN, Bluetooth and various short-range communication systems such and broadcast communications systems with different characteristics covered during this time each which targeted different types of users and different types of services.

As the mobile has become more handy and also its use is increasing day by day such services completely user-centric, multimedia services, high speed Internet streaming (telemedicine, tele-geoprocessing, and virtual navigation VoIP),good quality of service unhindered and the coverage of network ubiquitously for seamless global roaming support 3G began to show their limits with between the different networks by lack of seamless transport, the availability of bandwidth, frequency allocation, the interference of standards air. These limitations and disadvantages have generated the need for a universal framework encompassing all wired systems without existing heterogeneous wireless in use. MAGIC based on IPv6 is a framework of 4G potential, (mobile multimedia, Anytime Anywhere Access, mobility support globally, the integrated wireless solution and also the personal services are customised) can prove to be highly dynamic and manage significantly the shortcomings of 3G systems. Thus, on various consolidated solutions that can work, diverse networks migrate to 4G environmental to fulfill the plethora of dream visualizations on the implementation Next Generation architecture without an open transparent thread (OWA), have to be designed . This obviously calls for new challenges at every step and researchers around the world are facing a difficult task to design appropriate solutions. Such a vision 4G is shown in Figure 1.



The recent expansion of wireless network technologies and the emergence of new applications such as mobile led to the standardization of the (pre-4G) Long Term Evolution (LTE) to become

operational protocol with the 3rd Generation Partnership Project(3GPP).3GPP has also begun studying the standard future development, called Evolution Architecture System (EAS), set to move into the new era of 4G. LTE is in fact, the latest standard in the mobile core network technology which now accounts for over 85 percent of all mobile subscribers.The mobile telecommunication system of the next generation, universally recognized as 4G is prototyped for increased safety and reliable communication. Yet 4G wireless technologies have several key differences with respect to the 3G and other previous versions. A basic difference is that wireless networks 4G function entirely on TCP / IP Suite architectural and become fully IP. This decision represents the effort to work more with interoperability between heterogeneous network environments, both wired and wireless, thus solving many problems in terms of compatibility architectural design. However, one consequence of make this transition to a suite of open communication protocols is that it poses greater risks in terms of Safety and reliability.

1.1. Security Enhancements in LTE/SAE Standard

For most security attacks, many critical security features came up with the normalization of the security LTE / SAE. Many of these requirements led to the EPS security architecture is quite different from the 3G security architecture. Some design decisions are as follows:

1.1.1. Permanent Safety Association –

A crucial security principle that must be kept in EPS is that the permanent key used in the AKA protocol must never be visible outside of the security module.

1.1.2. Require mutual authentication mechanisms.

Mutual identity-verification of both the terminal and the network, the additional shared encryption material between them enables confidentiality and integrity protection of data transmitted.

1.1.3. Authorization.

Permission is required for connection for basic networks and software integrity.Although the EPS security architecture has changed from 3G architecture, there is still room for improvement, particularly when considering the possibility of following changes in the wireless network security.

1.2. Vulnerabilities of LTE/SAE Security Algorithms and Procedures

Several EPS-specific threats that affect all EPS architecture and trust model emerged with asking the radio interface characteristics and great risks to environmental integrity standards.

We classify further major categories of threats and risks that degrade EPS the reliability of the safety as follows:

1.2.1. Threats against the user identity and privacy.

A common threat category is defined by the illegal use users and mobile devices access the network identities services. In particular, the evil potential user could access and illegal use of the security procedure keys to access network services. Another example could be malicious modification of EU parameters lock out the user to the rest services.

1.2.2. Threats from base stations and transfers.

An example this would force a transfer to a compromise base station via a strong signal.

1.2.3. Threats to broadcast or multicast traffic.

A method for this is to disseminate false information system across the network, which causes trouble in the signaling plane.

1.2.4. Threats related to a denial of service (DoS).

An example DoS threats could cause DoS attacks against other UEs.

1.2.5. Threats against handling control plane data.

A high-risk cases data manipulation is changing the EPS data signaling protocol to become understandable or others can be modified in transit.

1.2.6. Threats of unauthorized access to the network.

In case there was an illegal access to the basic network EPS users can establish communication with evil the system further deterioration of security.

1.3. Target Objectives

Transition to the next generation (4G) LTE security technology will be derived from practical aspects of applied cryptography 3G loyalty and reliability of algorithms. Focus should be on 3G telecommunication systems in accordance with the availability, confidentiality, and integrity of key security objectives.

1.3.1. ITU X.805 Framework

A relevant research effort to reveal the security challenges emerging in 4G networks has been the development the International Telecommunication Union X.805 standard as a tool of systematic analysis based on security model. Bell Labs Based on the philosophy that threats to cellular systems can occur in any layer, as well as architectural plans, the X.805 built a structured framework that examines and improves multilayer, characteristics to-end network security across eight dimensions of security, as protection against all possible attacks and vulnerabilities. In X.805, the security of the network is, as illustrated in 3, organized in three layers (application, services, and infrastructure), three aircraft (end user, control, and management) and eight dimensions (access control, authentication, non-repudiation, data confidentiality, the communication security, data integrity, availability and confidentiality).

1.4 Background

Works on an investigation of advanced 4G wireless network security and its challenges. Presents safety advances and challenges associated with emerging 4G wireless technologies. There are a number of contributions to the field. First, examines the development of safety standards in the different wireless standards generations. Second, standards, architecture related to the safety and design for LTE and WiMAX technologies are analyzed. Third, security issues and vulnerabilities in the top of the 4G standards are discussed. Finally, potential areas for future vulnerabilities and assess the areas of security that need attention 4G and future work of the research industry and advanced technology.[13]

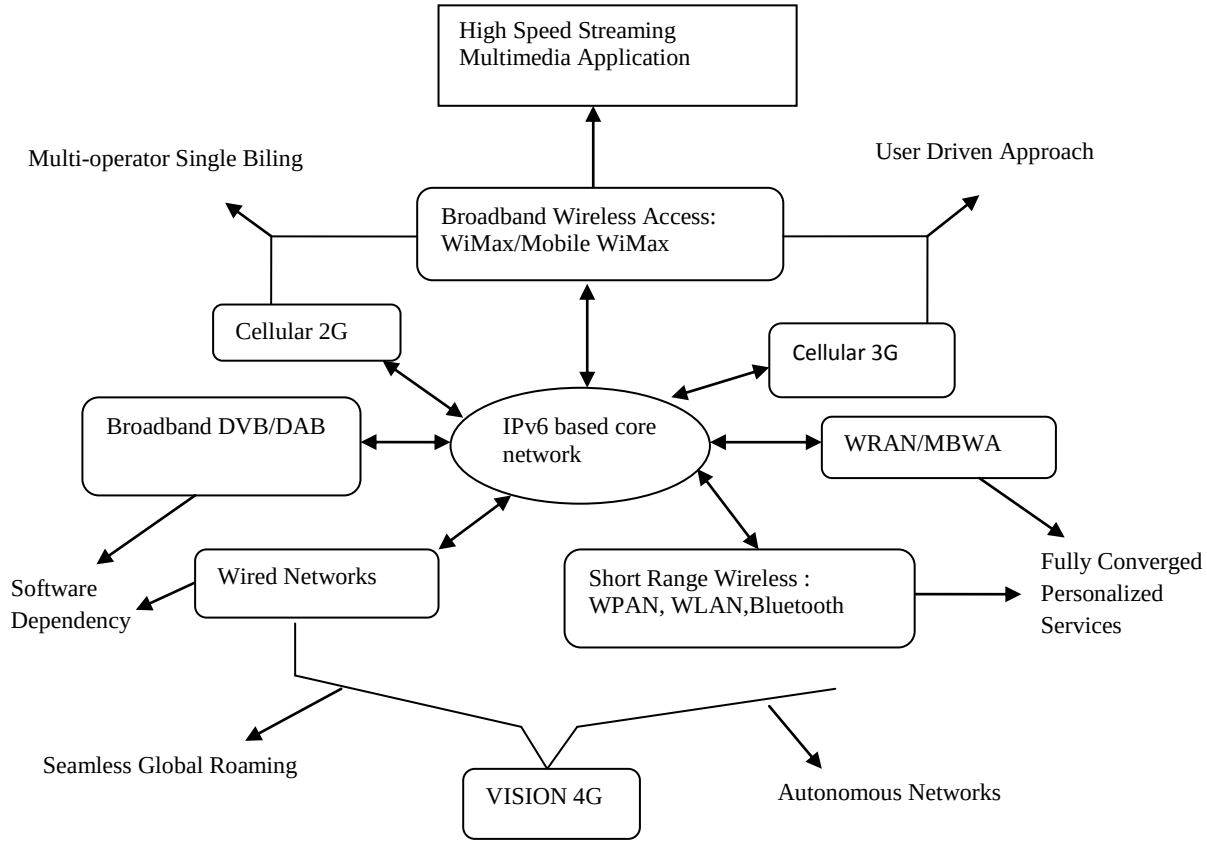
In order to protect the privacy of the user and the network used, security support is mandatory for all communication. Unilateral authentication between the subscriber and the base station (BS) was one of the IEEE 802.16 security leaks. IEEE 802.16e, some security vulnerabilities are resolved, while there is dearth of research on the safety of Mesh topology as some vulnerabilities are always present. A number of security vulnerabilities and proposes a new protocol to strengthen security in mesh mode. The protocol is based on biocryptosystems providing solutions to secure the initial network entry, and achieve privacy between two different nodes in the network. In addition, the protocol integrating Advance Encryption Standard and biometric digital key (AES-BDK) for other network messages and key distribution.[6]

"A method of secure key management for cloud computing environments. Shows the safety levels on the basis of what they can and what they can not get into the security models. And after studying it is proposed a lightweight protocols ensure maximum safety, and to report on their practical performance. They felt, totally alone servers that pass between periods and offline without communicating with anyone outside of the cloud, and semi-autonomous servers that need a limited type of aid from outside the cloud when you make the transition.[5]

The WSN application scenarios including industrial applications and factory automation.In which Time Division Multiple Access (TDMA) is generally used for data communication between the sensor nodes. However, networks of TDMA-based sensors are particularly prone to selective Jamming attack a specific form of denial of service to network reliability seriously thwart.An adaptive and decentralized MAC layer solution against selective interference in network TDMA-based sensors which does not require a central entity, sensor nodes need to rely solely on local information and allows them to join and leave the network without affecting other activity nodes.[16]

On the Cluster secure routing protocol based (CBSRP) is a MANET routing protocol that provides secure key management and communication between mobile nodes. It uses digital signatures and hash Technical one way to secure communications. According CBSRP, it forms a group of small groups consist of 05/04 knots after the communication takes place between the mobile nodes. Inside a cluster, there is always a node cluster or cluster head. The cluster head in the cluster is not permanent as other nodes remain in the queue and on the basis of the new cluster node cluster head or priority is elected rest of node. Inside a cluster, mobile nodes are authenticated using a hash Way concept and the digital signature is not required within the cluster communication. For authentication Cluster-Cluster we proposed to use the digital signature. CBSRP provides secure communication to be energy efficient we segmented the entire network in a small set of clusters. [10]

Also we have an architecture based on smartphones to secure user access to web services that require password entry.The architecture takes advantage of biometric sensors that are present in today's smartphones when authenticating a smartphone user to ensure that his identity can not be masked by someone else. The user can then access web services using a complex password stored in its smartphone, but without having to manually enter the complex password. Therefore, the architecture overcomes many of the password security limitations on the basis of today's authentication methods, particularly to solve the current dilemma associated with the use of passwords complexes. The architecture not only works seamlessly with web services today because it does not require modification of existing authentication mechanisms used by servers, but can also be extended to use the data directly Biometric someone credentials instead of passwords to access web services and cyber-physical systems in the future.[12]



2. DRAWBACKS IN EXISTING SYSTEM

The existing solutions are generally based upon the predictive key exchange schemes for the 4G/LTE networks. The existing schemes includes both plain-text and cryptographic key exchanges. The plain-text key exchanges are the most insecure schemes for the purpose of authentication, whereas the cryptographic key exchange schemes are more secure than the plain-text key exchange. The cryptographic key exchange schemes can effectively establish the secure communications between the two nodes and protect against the node emulation attacks, etc. The plain-text schemes, which produce the similar keys at each rotation, can be also considered secure in comparison with the cryptographic key exchange. A comparative analysis is required for the purpose of the getting the best scheme out of the two schemes for 4G/LTE platforms. The performance analysis must be performed on the basis of the various performance parameters in order to get the best level comparison between the two key exchange schemes for the 4G/LTE networks.

3. PROBLEM DEFINATION

The problem of security in 4G LTE networks has been addressed in the base papers. The higher number of vulnerabilities are found in the MAC layer, where attacker can launch a variety of active and passive attacks. The call security becomes an important issue in today's world. Specifically, our call security concern is attached with the calls made between important persons of the nation (Higher-level politicians, Military officers, Officers from national security agencies). Any kind of breach in these calls can compromise the national security at large. Hence, it becomes very important to secure these calls. In this research, we are proposing a security mechanism for the call security in 4G/LTE.

3.1 Proposed System

The 4G/LTE networks are coming to existing in almost all regions of the worlds. The popularity of the 4G/LTE has been rising every year and many new users are being added to the network. This is enhancing the risk of the security of the user information. The user information must be protected in the most secure environment. There are several existing solutions available for the purpose of the 4G/LTE security. The multiple techniques or key exchange based solutions are not possible in the same network. The key exchange schemes are majorly divided into two classes. The first is the simple key exchange using the predictive or dynamic key management schemes. The other key exchange scheme is based on the cryptography and called the crypto key management scheme. This study is based upon the performance evaluation of the duo listed above. After the performance evaluation in the proposed scheme the opinions would be given for the use of the two schemes under the different environments, regional specification and requirements, network bandwidth, user count, etc.

Popular key exchange models for 4G / LTE networks are secure basic key exchange programs and the hybrid model of cryptographic key exchange. The basic key exchange scheme comprises the encryption key decryption using the existing public cryptographic algorithm. The hybrid system of cryptographic key exchange includes a multi-level encryption with public-private key based data encryption algorithms.

Both algorithms listed above are evaluated for their performance. The performance evaluation process will be divided into different stages or scenarios. Both plans would be evaluated under various scenarios and different perspectives. 4G / LTE key exchange schemes would be assessed for the level of security, network performance, life cycle of key exchange, key generation and verification speed and key generation and complexity audit. The shortcomings of the existing models will be overcome using the improved model for the higher order of security for the 4G/LTE networks. The proposed model will utilize the hierarchical multi-level key exchange approach for the purpose of hardening the security level of the existing models. The proposed key management approach will be a hybrid approach which will be made capable of protecting the 4G network on all of the network stages. The proposed model will protect the 4G network during the initial call setup phase, periodic time based key exchange to ensure the call security and the seed exchange for the other end integrity check. The proposed model will use a pre-shared key group to ensure the security during the call setup phase and will use the random table based non-predictive key exchange model for the purpose of in-call security assurance and receiver integrity check by the caller. The third scheme will be used to ensure the caller integrity on the receiver's end.

4. METHODOLOGY

The security model 4G / LTE is being developed under this research project in the network simulator 2 (popularly known as NS-2). 4G networks are cellular networks fourth generation, which offer high bandwidth and fast speed. The 4G network provide users with the ability to access the internet application along with a voice or video call. The risk of attack information active or passive diversion is always there when a higher bandwidth link is used for communication. The lightweight key management system is the best solution than other alternatives because it offers a fast and secure transmission by adding a minimum design overhead. The mathematical equation faster and predictive being key generation scheme is used for the proposed security 4G calls. The data for the voice is the most sensitive information shared between two users, where attacks can be targeted. Secure text-based communication applications can come with pre-built security mechanisms. Voice calls are never offered with pre-integrated security architecture. The key sharing based on the architecture time is used to protect the voice calls 4G. Therefore, there is a significant need for secure key management between the two nodes. Key sharing rules will be shared between the call ends (both nodes to make a call) during the initial handshake. After the end caller will generate a key using a fixed mathematical equation, which will be a pre-treatment. Pretreatment steps include the mixing of bytes, bit shift operations, scramble key and another mechanism to create a unique and secure key. The key when received at the end of call termination, he will suffer the exact reversal process as pretreatment order. The original key will be obtained and matched for integrity. If the key matches, the data would be exchanged between the two nodes, if the call is terminated flashing message integrity violation on the end of the spammer.

The shortcomings of the existing models will be overcome using the improved model for the higher order of security for the 4G/LTE networks. The proposed model will utilize the hierarchical multi-level key exchange approach for the purpose of hardening the security level of the existing models. The proposed key management approach will be a hybrid approach which will be made capable of protecting the 4G network on all of the network stages. The proposed model will protect the 4G network during the initial call setup phase, periodic time based key exchange to ensure the call security and the seed exchange for the other end integrity check. The proposed model will use a pre-shared key group to ensure the security during the call setup phase and will use the random table based non-predictive key exchange model for the purpose of in-call security assurance and receiver integrity check by the caller. The third scheme will be used to ensure the caller integrity on the receiver's end.

5. CONCLUSION

This performance evaluation survey will evaluate the cryptographic key exchange scheme and predictive key exchange schemes with hybrid approach. Both of the key exchange schemes would be examined under various scenarios with the different user densities and different desired levels of security. After the performance evaluation, the results and opinions would be formed and published in order to spread the correct and most adaptable use of these schemes in the different environments or scenarios. The results would be evaluated using various performance evaluation parameters like transmission delay, throughput, level of security, etc.

6. FUTURE WORK

In the future, the comparative analysis can be performed with higher level of performance analysis using the higher number of parameters. Also, the techniques under the survey can be improved or mixed in order to improve the overall performance of the scheme.

7. REFERENCES

[1] Alezabi, Kamal Ali, et al. "An efficient authentication and key agreement protocol for 4G (LTE) networks." *Region 10 Symposium, 2014 IEEE*. IEEE, 2014.

[2] Bikos, Anastasios N., and Nicolas Sklavos. "LTE/SAE security issues on 4G wireless networks." *Security & Privacy, IEEE* 11.2 (2013): 55-62.

[3] Chandramouli, Ramaswamy, Michaela Iorga, and Santosh Chokhani. *Cryptographic Key Management Issues and Challenges in Cloud Services*. Springer New York, 2014.

[4] Chen, Fatang, and Jinlong Yuan. "Enhanced Key Derivation Function of HMAC-SHA-256 Algorithm in LTE Network." *Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on*. IEEE, 2012.

[5] Damgård, Ivan, et al. "Sescure key management in the cloud." *Cryptography and Coding*. Springer Berlin Heidelberg, 2013. 270-289.

[6] Elramly, Salwa, et al. "SMSHM: Secure Mesh Mode Protocol to Enhance Security of 4G Networks." *IT Convergence and Security (ICITCS), 2013 International Conference on*. IEEE, 2013.

[7] Han, Chan-Kyu, and Hyoung-Kee Choi. "Security analysis of handover key management in 4G LTE/SAE networks." *Mobile Computing, IEEE Transactions on* 13.2 (2014): 457-468.

[8] Leu, Fang-Yie, et al. "Improving security level of LTE authentication and key agreement procedure."

Globecom Workshops (GC Wkshps), 2012 IEEE. IEEE, 2012.

[9] Ma Ma, Maode. "Security Investigation in 4G LTE Wireless Networks." *School of Elecrical and Electronic Engineering, Nanyang Technological University, Singapore* (2012).

[10] Morshed, Md Monzur, and Md Rafiqul Islam. "CBSRP: Cluster Based Secure Routing Protocol." *Advance Computing Conference (IACC), 2013 IEEE 3rd International*. IEEE, 2013.

[11] N. Suganthi, N., and Sumathy Vembu. "Energy Efficient Key Management Scheme for Wireless Sensor Networks." *International Journal of Computers Communications & Control* 9.1 (2014): 71-78.

[12] Sanzziri, Ameva, et al. "SESAME: Smartphone enabled secure access to multiple entities." *Computing, Networking and Communications (ICNC), 2013 International Conference on*. IEEE, 2013.

[13] Seddigh, Nabil, et al. "Security advances and challenges in 4G wireless networks." *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*. IEEE, 2010.

[14] Sharma, Madhu J., and Victor CM Leung. "IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks." *Human-Centric Computing and Information Sciences* 2.1 (2012): 1-19.

[15] Sithirasenan, Elankayer, et al. "EAP-CRA for WiMAX, WLAN and 4G LTE Interoperability." *Selected Topics in WiMAX* (2013): 978-953.

[16] Tiloca, Marco, et al. "SAD-SJ: A self-adaptive decentralized solution against Selective Jamming attack in Wireless Sensor Networks." *Emerging Technologies & Factory Automation (ETFA), 2013 IEEE 18th Conference on*. IEEE, 2013.

[17] Zhou, Zongwei, et al. "KISS:"Key It Simple and Secure" Corporate Key Management." *Trust and Trustworthy Computing*. Springer Berlin Heidelberg, 2013. 1-18