Chapter 21
An Analysis of Cryptographic Algorithms in IoT

Samed Bajrić
Jožef Stefan Institute, Slovenia

ABSTRACT

The underlying vision of the internet of things (IoT) is to create a world where the real and the virtual realms are converging to create smart environments that makes energy, transport, cities, and many other areas more intelligent. With the IoT, the physical world is being interfaced through the things to the virtual world in heterogeneous environment. In heterogeneous environment, privacy and security are the major challenges. The secure information exchange is most critical pitfall to ensure the system security. This chapter gives a detailed analysis of cryptographic algorithms in IoT. A comparison of lightweight cryptography algorithms on basis of block size, key size, gate equivalents, and throughput is given. Moreover, the various security issues in IoT are discussed along with possible solution.

INTRODUCTION

The internet as we know it is always evolving, and in recent years an enormous increase in number of devices connected to the internet has occurred. It is estimated that by 2020, there will be 50 to 100 billion devices connected to Internet (Perera, Zaslavsky, Christen, & Georakopoulus, 2013). Now, ordinary objects like TVs, watches and smoke detectors are given the feature to connect to the Internet. From a sensor that enables us to configure the heating of our house when driving back home to devices that are placed inside our garden to measure the amount of rain. This is what we call the Internet of Things (IoT). The concept of IoT gives a new chapter in the history of the Internet giving the possibilities for cars, cameras, medical equipment to communicate through wired or wireless medium. With more and more devices being connected to the Internet, it can be expected that many of our day to day tasks will be aided by small connected computers, and probably be executed without any human intervention. While the technology itself might not be brand new, now is the time when it can be implemented in almost any object to create a network of things. Some of these devices use powerful processors and can be expected to use the same cryptographic algorithms as standard desktop computers.

DOI: 10.4018/978-1-7998-5351-0.ch021

The distributed nature of IoT necessitates secure communication with and between billions of devices. This relies on cryptography, whether for authenticating devices, protecting confidentiality and integrity of communications or for distributing digitally signed firmware updates. Many applications, such as smart cars and industrial control, require very high levels of security, as a successful attack could endanger not only sensitive data but human life. However, many of them use very low power micro controllers which can only afford to devote a small fraction of their computing power to security. For instance, sensor networks are intended to connect vast amount of very simple sensors to a central hub. These sensors would run on batteries and generate their own energy using for example solar panels. Cryptographic algorithms must be used on the messages sent by sensors to their hub in order to secure them and provide their authenticity and integrity. Because of their very low energy, the cryptographic algorithms have to be as 'small' as possible. On the other hand, the general method for ensuring the confidentiality of information is through the use of cryptography but most cryptographic mechanisms require a significant amount in terms of processing power and energy. This is quite a challenging issue to overcome and has received a lot of attention in the academic community.

Similarly, Radio Frequency Identification (RFID) technology uses radio waves to automatically identify objects, people and perhaps other information on a microchip that is attached to an antenna. The antenna enables the chip to transmit the identification information to a reader. In order to prevent an eavesdropper from learning the identification to a chip, this information has to be encrypted. Because of the very small number of logical gates and very little energy available, specially designed algorithms are necessary. Hence, the conventional cryptographic algorithms may perform well in computers, servers, and some mobile phones, but might not be suited for low-resource smart devices. It is well-known that the 1024 bit RSA algorithm cannot be implemented in RFID tags. Therefore, security is a significant issue in constrained devices. The number of commercial IoT systems deployed without adequate security mechanisms is growing exponentially. The large number of devices with relatively high computational power makes them an attractive target for attackers seeking to compromise these devices and use them to create large scale botnets. For instance, in 2017 thousands of insecure IoT devices were infected by malware and controlled for use in a massive Distributed Denial of Service (DDoS) attack (Jerkins, 2017). These insecurities have lead to a lack of trust in IoT in some spheres, somewhat limiting confident growth in the industry. Moreover, the tight constraints inherent the mass developments of smart devices that impeding the requirements of developing a new cryptographic algorithm, which performs strong security mechanism, encryption and decryption, with low power applications and other functionalities for the pervasive computing.

This new research area is referred as lightweight cryptography, and there are two main reasons for adopting it. The first one is efficiency of end to end communications where some smart devices have an implementation of a lightweight symmetric key algorithm. The second one is adoptability in low resources smart devices where for instance the footprint of lightweight cryptographic primitives is smaller than the conventional cryptographic ones. Many researchers have proposed lightweight symmetric (Hatzivasilis, Fysarakisloannis, Papaefstathiou, & Manifavas, 2018) and asymmetric security algorithms (Kumar & Singh, 2016) for IoT. Symmetric algorithms provide confidentiality and integrity, have small key size and are less complex, but they do not offer authenticity and distribution of keys in them is a challenging task. On the other hand, asymmetric algorithms provide confidentiality, integrity and authenticity, but their key size is too large which make them more complex for constrained devices. It is imperative that research in security keeps up with the fast-paced ongoing developments in other aspects of IoT. In this work we try to contribute towards better understanding of security lightweight encryption algorithms that