Quantum-Elliptic curve Cryptography for Multihop Communication in 5G Networks

A.S. Khan, J. Abdullah, N. Khan, AA Julahi, S Tarmizi

Network Security Research Group, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak

ABSTRACT

The Internet of Things (IoT) depicts a giant network where every "thing" can be interconnected through the communication network. The communication can be initiated between people-people, people-things, and things-things. Meanwhile, the fifth generation (5G) mobile communicating systems are the mainspring to power the IoT concept in the upcoming future. However, the heterogeneous environment in 5G networks as well as the high dependency on radio spectrum have raised deep concerns about the security assurance against network attacks such as eavesdropping. In this paper, we propose an end-to-end security mechanism to ensure the multi-hop relay communications in 5G based IoT networks to stay secured. We design a scenario to explain the insecure multi-hop relay communications which involves Base Station (BS), Subscriber Station (SS) and Relay Station (RS). Next, we utilize Quantum Cryptography between BS to RS and RS to RS as well as adopting Elliptic Curve Cryptography between BS to SS or RS to SS to mitigate the network against typical replay attacks. By using the concept of integrating both cryptographic methods, the secret key that yield from Quantum Cryptography will be used in Elliptic Curve Cryptography to secure the transmission of information across IoT networks. Thereupon, extensive discussion has been carried out and it shows that the suggested mechanism has potential to ensure confidentiality, integrity, availability and non-repudiation in the proposed scenario. In the final part of this paper, we conclude our study by a comparison analysis between the two proposed cryptographic solutions. The comparison analysis illustrates the performance of each proposed strategy in terms of the achievable level of secrecy in IoT networks.

INDEX TERMS

Internet of Things (IoT), fifth generation (5G) network, cryptography, Quantum cryptography, Elliptic Curve cryptography.

1. Introduction

As the technology is continuously evolving, the definition for the Internet of Things (IoT) keeps expanding. Originally, IoT focuses on the connectivity as well as the sensory necessities for entities to be involved in ordinary IoT environments [1]. Along with the evolution of technology, the concept of IoT in current modern world provides more value to the demand for ubiquitous networks and secured information exchange among a variety of smart objects [2]. IoT illustrates that physical and virtual objects are accessible without time and place limitations. Among all existing and evolving communication technologies, the techniques for the fifth generation (5G) mobile communicating systems will be essential to accomplish the concept of IoT. However, the 5G system which is much better and faster than current 4G system will not be rolled out until year 2020 [3]. Although 5G system is yet to be launched, it is believed that 5G networks can achieve higher data rates, lower end-to-end latency, lower energy consumption, lower cost per information transfer, ubiquitous, uninterrupted and consistent connectivity [4]. Moreover, 5G system is much easier to manage as compared to previous generations and this indicates 5G system is more effective and efficient [5][6-12].

In the near future, the advancement in IoT and 5G technologies will bring a lot of significant changes to the public. IoT, the global infrastructure for the information society will enable a variety of objects to be recognizable and integrated into the communication networks. With such advanced objects being integrated into different industries, the quality of human's daily lives as well as the world's economy are believed will be boosted to a higher level. Soon, the communication services will be highly pervasive and distributed which in turn create a decentralized pool of resources interconnected through a dynamic network. Other than that, 5G technologies are also one of the hot issues being discussed due to its capability to create a seamless connection for massive things at a faster speed. 5G technology is able to power a huge number of connected devices that will reach out to different locations via a wireless communicating network. In short, it is a leading-edge technology which collects all networks into one platform in order to offer ubiquitous connectivity across the world.

Although the actualization of IoT is beneficial to numerous fields such as industry, education, healthcare, transportation and market, it brings up many issues related to security. When up to billions of smart devices are connected, it is difficult to assure the information being transmitted stays secured. Furthermore, 5G system is considered as heterogeneous network [13] and its properties of relying on radio propagation for broadcast

Manuscript received May 5, 2017
Manuscript revised May 20, 2017