ABSTRACT

The Internet-of-Things (IoT) that is a whole of inanimate objects is being designed with built-in wireless connectivity, that monitored, controlled and linked over the Internet, but as with any new technology, IoT can be confusing for the normal consumer, especially as debates swirl around standardization, security and privacy. Furthermore, the IoT has many applications like Home automation, Healthcare, Smart grid, Smart city and Smart car. The application based on the IoT technology that is generating huge amount of data which these devices created. It leads to many security concerns like how to secure these devices, data and communication from unauthorized access. An authentication is a fundamental building block to provide the mutual authentication between user and devices in the IoT environment. However, the IoT consists of constrained devices in its computational capability, network bandwidth, packet size and memory such as sensor nodes. Therefore, in this thesis, a proposed an enhanced lightweight authentication key exchange protocol based on the elliptic curve that provides the users and devices authentication in IoT environment.

The proposed protocol uses an implicit certificate that has a significant potential advantage over a traditional certificate. Therefore, an implicit certificate allows the proposed protocol to use a small size of transmitted packet during the proposed protocol run, which it leads to save bandwidth, memory and energy. Meanwhile, the proposed protocol is based on an elliptic curve cryptosystem that allows using a small key size, which saves network resources and reduces the computation complexity.

The proposed protocol provides an explicit key authentication with the session key confirmation that can withstand denial of service attack in the IoT applications, and it has a verification mechanism in its block design to verify partner identity from calculating its static

public key. In addition, the Scyther tool used as a formal automatic verification method to analyze and verify the proposed protocol security claims, and the results show that the proposed protocol is a secure in the eCK model. We compare the proposed protocol an Enhanced Lightweight Authenticated elliptic curve key exchange Protocol for securing Internet of Things (ELAP) with other existing schemes in our study in terms of security and performance, we show that the proposed protocol satisfies desirable security properties in IoT environment and obtains computational efficiency in the sense that the smart mobile phone performs 3-point multiplications and the sensor node performs 2-point multiplication therefore fitting the constrained devices in the IoT application.

Keywords: Authentication; Cryptography, Elliptic curve cryptosystem; Internet-of-Things; IoT Framework; Scyther tool; Security model; Sensors; Wireless sensor network.