# Enhanced Symmetric Cryptography for IoT using Novel Random Secret Key Approach

Gopinath Sittampalam
*Department of Physical Science*
*Vavuniya Campus of the University of Jaffna*
Vavuniya, Srilanka
s.gopi89@vau.jfn.ac.lk

Nagulan Ratnarajah
*Department of Physical Science*
*Vavuniya Campus of the University of Jaffna*
Vavuniya, Srilanka
rnagulan@univ.jfn.ac.lk

***Abstract*—The deployment of IoT devices in different domains enables technical innovations and value-added services to users but also creates multiple requirements in terms of effective communication and security. IoT devices are constrained by less computing resources and limited battery power. Generally, the TLS/SSL protocol is used to provide communication security on IoT and the protocol utilizes important encryption algorithms like RSA, Elliptic Curve Cryptography, and AES. However, these conventional encryption algorithms are computationally and economically expensive to implement in IoT devices. Lightweight Cryptography (LWC) algorithms were introduced recently for IoT and the aim of the algorithms is to provide the same level security with a minimal amount of computing resources and power. This paper proposes a novel Random Secret Key (RSK) technique to provide an additional security layer for symmetric LWC algorithms for IoT applications. In RSK, IoT devices do not transmit keys over the network; they share a random matrix, calculate their own RSK, encrypt, and transmit the cipher text. When a random matrix lifetime expires new matrix published and RSK resets. Regular change in the RSK makes the IoT networks resistant to brute-force/dictionary attacks. The RSK added one more simple and effective secure layer to strengthen the security of the original secret key and is successfully implemented in a smart greenhouse environment. The outcomes of the experiments prove that the RSK provides enhanced and efficient protection for symmetric LWC algorithms in any IoT systems, consume a minimum amount of resources and more resistant to key-based attacks.**

***Keywords—IoT, Security, LWC, Random Secret Key***

## I. INTRODUCTION

Internet of Things (IoT) is the interconnection of physical devices that contain sensors, actuators, microcontrollers, and network interfaces to interact with the environment and communicate with each other and to humans. IoT devices collect useful data from the environment by using sensors and the data is transmitted over the internet for processing and automated action will be taken by actuators based on the decision provided by the processing unit. In recent years, IoT technologies have been applied to many fields such as smart homes, healthcare, transport, agriculture, and industries. The total number of IoT connected devices will reach nearly 27 billion by the year 2020, and 75.44 billion by 2025 [1]. These big numbers of interconnected IoT devices are undoubtedly vulnerable to security and privacy threats.

Wireless technologies mostly used as a communication medium in IoT. IoT enables Machine to Machine (M2M) communication, which means communication between devices without or with less involvement of the user. M2M networks use various wireless technologies such as Wi-Fi, ZigBee, 6LowPAN, and Bluetooth. However, if any wireless technologies used by IoT devices, all the devices should make their data available on the internet [2]. There are some specially designed application protocols available to handle communication among IoT devices in middleware domains and application domains [3], such as Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), Message Queue Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), Web socket, and Data Distribution Service (DDS) [2,7]. Table I briefly describes the features of application layer protocols. The selection of the application protocols depends on the IoT system requirements; MQTT is the best for M2M protocol because MQTT runs on top of the Transmission Control Protocol (TCP) stack which requires less bandwidth and computational resources [3,4,7].

TABLE I. DETAILS OF THE APPLICATION LAYER PROTOCOLS.

| Protocol | Architecture | Transport layer | Security |
|---|---|---|---|
| CoAP | Request/Response | UDP | DTLS |
| MQTT | Publish/Subscribe | TCP | TLS/SSL |
| XMPP | Publish/Subscribe<br>Request/Response | TCP | TLS/SSL |
| AMQP | Publish/Subscribe | TCP | TLS/SSL |
| DDS | Publish/Subscribe | TCP/ UDP | TLS/SSL |

In the IoT systems, large amounts of sensor nodes are deployed to collect the data. The collected data analyzed and autonomous actions performed by an actuator. If one of the sensor network data falsified, the analysis process produces an incorrect result and the incorrect result caused a malfunction in actuators. A security breakdown, therefore, can lead to serious system damage. Each layer of an IoT system is vulnerable to many security threats. The device or hardware layer includes CPU, memory, and ports of IoT devices, which are opened to many attacks and vulnerabilities such as tampering, physical damage, removal of Secure Digital (SD) cards, reset to insecure state, through ports gaining terminal access, install backdoor accounts, and malicious firmware update. IoT devices are connected to applications through the communication layer. It widely uses lightweight wireless protocols [7]. The possible attacks on the communication layer are Denial of Service (DoS), Distributed DoS, ICMP attack, address spoofing, Man-in-the-middle attack (MITM), session hijacking, TCP SYN Flood attack, UDP flood attack, and attacks on cryptography key [6,8]. IoT application layer protocols enable access among IoT devices, web applications, mobile apps, databases, and clouds over the internet. The possible attacks on application layers are DoS, MITM, Eavesdropping attack, SQL Injection, routing attack, cross-site Scripting, cross-site Request Forgery, and attacks on cryptography key [5,6,8].

## II. IOT AND LIGHTWEIGHT CRYPTOGRAPHY

Encryption has been used in different protocols of the OSI reference model, such as Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) in the application layer, Transport Layer Security/ Secure Sockets Layer (TLS/SSL) in

978-1-7281-8412-8/20/$31.00 ©2020 IEEE