Chapter 8
Secure D2D Transmission Using Lightweight Cryptography for 5G IoT Networks

Vijaya Lakshmi M.
https://orcid.org/0009-0005-2415-4930
Bharath Institute of Higher Education and Research, India

V. Ganesan
Bharath Institute of Higher Education and Research, India

ABSTRACT

Device-to-device (D2D) communication contributes to increased radio frequency reuse and cell coverage expansion in a 5G network by directly connecting devices without an intermediary node. Millions of smart gadgets with limited retention, battery life, and processing power are interconnected in a worldwide computing environment. One major environmental motivator has been the development of 5G. The unique characteristics of the 5G cellular network make it an ideal choice to serve as the backbone network for the Internet of Things in the future. On a 4G network—a common telecom network—standard communication between devices raises various security concerns, though. Furthermore, IoT devices have limited resources, so these security issues become even more important and challenging to solve when 5G networks are applied mMTC and URLLC applications. Safety issues in a 5G IoT environment must be addressed by a thin, safe D2D network able to provide safe verification, data integrity and privacy.

DOI: 10.4018/979-8-3373-4672-4.ch008

INTRODUCTION

D2D communication offers several benefits in mobile networks as it is a communication technique among devices without an intermediary node. A cellular network can increase each cell's coverage by acting as an interface to send data to nodes not inside the phone's area. Furthermore, by sending data straight among equipment, D2D communication lowers the core station's energy usage. Finally, there is a boost in the efficacy of utilizing the same radio frequency. The gap between equipment in D2D communication is significantly smaller than between the equipment and a center station. Owing to these benefits, D2D communication technologies like the LTE-advanced (4G) network are also a part of the 5G network (Tehrani et al., 2014). However, there are several security issues with standard D2D interaction on a mobile network. Furthermore, message verification and encryption are not used in D2D connections to maintain connection integrity and secrecy (Jeong and Ahn, 2017). This implies the attacker can use deception techniques, including position phishing, security snooping, and reckless behavior. We require a secure D2D communication system with an appropriate device verification procedure to address the security issues with D2D interaction in the 5G IoT network. Lightweight encryption can be an appropriate way to protect devices with limited resources (Doppler et al., 2009).

Elliptic Bend Cryptography (ECC) is becoming more broadly recognized as an extremely fruitful security arrangement. It functions admirably for gadgets with restricted assets, such as those in the quickly extending Web of Things (IoT) space. This acknowledgement results from the way that, as opposed to additional traditional strategies like RSA, ECC can offer a similar level of cryptographic security utilizing more modest keys (Chen et al., 2017). Specifically, a 256-cycle ECC key can give security like a 3072-bit RSA key, requiring less memory and figuring power — two indispensable advantages for Web of Things (IoT) gadgets with obliged handling and battery duration. The way that ECC is coordinated into the foundation of contemporary correspondence frameworks, including 5G organizations Lin et al. (2016); Wang et al. (2022); Daoud et al. (2019), which structure the premise of the Web of Things biological system, accentuates the innovation's convenience in this day and age significantly more (Zhang et al., 2019).

In this respect, our exploration presents a clever utilization of ECC for safe D2D (Gadget to Gadget) correspondence on a 5G Web of Things organization. Our methodology comprises a Validated Encryption with Related Information (AEAD) figure and an ECC-based lightweight encryption framework. The reason for this mix is to ensure the honesty and security of information moved between Web of Things gadgets. To forestall undesirable access, the ECC part scrambles the information and converts it into a solid organization that must be decoded by the planned recipient (Abro et al., 2019). Meanwhile, a solid strategy for affirming the