Chapter 37
A Survey of Blockchain-Based Solutions for IoTs, VANETs, and FANETs

Maroua Abdelhafidh
https://orcid.org/0000-0003-0626-5598
University of Sfax, Tunisia

Nadia Charef
Canadian University Dubai, UAE

Adel Ben Mnaouer
https://orcid.org/0000-0003-3617-7636
Canadian University Dubai, UAE

Lamia Chaari
University of Sfax, Tunisia

ABSTRACT

Recently, the internet of things (IoT) has gained popularity as an enabling technology for wireless connectivity of mobile and/or stationary devices providing useful services for the general public in a collaborative manner. Mobile ad-hoc networks (MANETs) are regarded as a legacy enabling technology for various IoT applications. Vehicular ad-hoc networks (VANETs) and flying ad-hoc networks (FANETs) are specific extensions of MANETs that are drivers of IoT applications. However, IoT is prone to diverse attacks, being branded as the weakest link in the networking chain requiring effective solutions for achieving an acceptable level of security. Blockchain (BC) technology has been identified as an efficient method to remedy IoT security concerns. Therefore, this chapter classifies the attacks targeting IoT, VANETs, and FANETs systems based on their vulnerabilities. This chapter explores a selection of blockchain-based solutions for securing IoT, VANETs, and FANETs and presents open research directions compiled out of the presented solutions as useful guidelines for the readers.

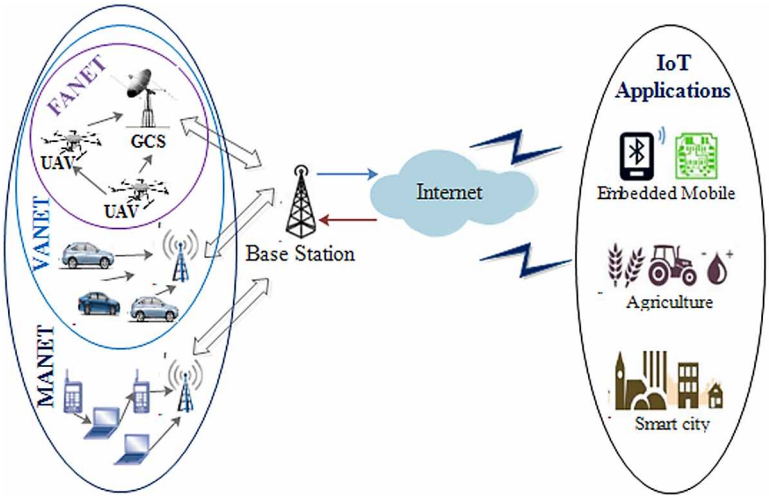
DOI: 10.4018/978-1-6684-7132-6.ch037

INTRODUCTION

Nowadays, Internet of Things (IoT) (Stoyanova et al.2020) has experienced tremendous opportunities and potential interest from various applications allowing a seamless connection of multiple and diverse devices to the internet in order to exchange efficiently collected data.

With the growth of IoT applications, a rise of Mobile Ad Hoc Networks (MANETs) (Tripathy et al.2020), Vehicular Ad Hoc Networks (VANETs) (Hamdi et al.2020) and Flying Ad Hoc Networks (Mukherjee et al.2018) applications is recognized. MANETs is a network of mobile nodes that are connected wirelessly and characterized by a dynamic network topology. FANET is another class of ad-hoc networks that is a subcategory of VANETs which is a sub form of MANET as illustrated in figure 1.

Figure 1. MANET, VANET, FANET and IoT



At present, IoT systems are often dependent upon a centralized architecture where information is sent from the connected devices and equipment to a proprietary cloud where the data is processed using analytics and then sent back to those tiny IoT devices to coordinate them as with all centralized systems. All devices are identified, authenticated and connected through cloud servers and the data collected by the devices is stored in the cloud for further processing (Ali et al.2018).

This centralized network architecture cannot be able to respond to the growing needs of the huge IoT ecosystems with the growth of connected devices that will be approximately 75.44 billion, as announced in (Alam2018). This gathered data, stored in centralized servers, can be tampered and consequently lacks traceability. Furthermore, through the current architecture, users have limited control over their data and are made to trust the cloud and have no choice but to rely on their promises of security. Accordingly, IoT security efforts mostly focus on securing point-to-point communication and fall short in addressing security during the lifecycle of data by thinking about this problem of trust. IoT devices need to confidently exchange data without having to rely on an intermediary which adds friction and costs reconciliation problems and all sorts of transactional challenges.