Chapter 54
Blockchain Advances and Security Practices in WSN, CRN, SDN, Opportunistic Mobile Networks, Delay Tolerant Networks

Eranda Harshanath Jayatunga
https://orcid.org/0000-0001-9435-7761
Faculty of Engineering, University of Ruhuna, Sri Lanka

Pasika Sashmal Ranaweera
https://orcid.org/0000-0002-4484-2002
Faculty of Engineering, University of Ruhuna, Sri Lanka

Indika Anuradha Mendis Balapuwaduge
https://orcid.org/0000-0003-1792-2645
Faculty of Engineering, University of Ruhuna, Sri Lanka

ABSTRACT

The internet of things (IoT) is paving a path for connecting a plethora of smart devices together that emerges from the novel 5G-based applications. This evident heterogeneity invites the integration of diverse technologies such as wireless sensor networks (WSNs), software-defined networks (SDNs), cognitive radio networks (CRNs), delay tolerant networks (DTNs), and opportunistic networks (oppnets). However, the security and privacy are prominent conundrums due to featured compatibility and interoperability aspects of evolving directives. Blockchain is the most nascent paradigm instituted to resolve the issues of security and privacy while retaining performance standards. In this chapter, advances of blockchain technology in aforesaid networks are investigated and presented as means to be followed as security practices for pragmatically realizing the concepts.

DOI: 10.4018/978-1-6684-7132-6.ch054

INTRODUCTION

All the discussed variants of this chapter are the pioneer technologies that govern the emerging communication based services and their applications. These directives were formed to address lacking aspects of different existing technologies with an improved perspective for elevating performance standards. Though, each distinct directive has limitations in security, where application of cumbersome but tamper-proof security mechanisms would obviously degrade the performance of them. Thus, there is a clear trade-off between latency and applicable security level. In addition, similar to most existing communication technologies or protocols, verifiable security is only credible with Trusted Third Parties (TTPs), or certificate authorities. Blockchain, in contrast, offers a decentralized approach that eliminates the TTP dependency. Moreover, the transparent yet tamper-proof mechanism in blockchain is enabling it to be adopted for diverse applications to secure their transactions. Thus, this chapter is focusing on the technologies of WSN, oppnets, SDN, CRN, and DTNs for adopting blockchain to their security limitations. The chapter is mainly categorized into the sections of WSN, SDN, CRN, DTN and oppnets, where various prevailing blockchain adaptations are discussed summarizing the best security practices.

BACKGROUND

Wireless Sensor Networks (WSNs) are basically ad hoc networks, amalgamating small devices embedded with sensing capabilities deployed to monitor physical activities in the surrounding area of interest. These sensor nodes should have the characteristics of large coverage area, monitoring with high precision, self-organization, random deployment and fault-tolerance, etc. Due to the possibility of providing low cost solutions, nowadays Wireless Sensor Networks (WSNs) are getting more and more attention in many real-world applications. However, the dense deployment of many sensor nodes cause unique security challenges in its management. In the meantime, adaptation of many security protocols to overcome those challenges are not straightforward because of inherent limits for energy consumption at sensor nodes as well as availability of lower memory and storage space. Therefore, it is timely important researchers to discuss the trade-off between resource consumption minimization and security maximization in WSNs.

Flexibility is the key feature of Software Defined Networks (SDNs) that elevate its standards beyond the conventional networking infrastructures (Kreutz, Ramos, & Verissimo, 2013). This concept offers advanced network management capabilities to the network administrator by enabling configuration of networking instances independent of the hardware layer. Infact, diversification exhibited in networking devices and their plethoric aggregate are contriving compatibility and interoperability debacles. In SDN, homogeneity of the both core and access networks are improved with standardizing the hardware specifications; and higher reliance on hardware based processing is transformed into an autonomous processing approach with software integration (Kumar et al., 2017). In fact, SDN envisages solutions for complex issues in traditional networking topologies and routing algorithms by integrating intelligence to the control plane. In addition, this is a paradigm shift for network operators that eases their issues with hardware layer and the ability to advance networking features with novel requirements to broadened avenues. Apart from flexibility, main benefits of SDN can be specified as: cost effectiveness (monetary), centralization, higher throughput, dynamic nature that support higher mobility, low communication latency, optimum network utilization, rapid and efficient load-balancing, fault tolerance, and