International Journal of Interdisciplinary Telecommunications and Networking
Volume 14 • Issue 1

Secure Protocol for Resource-Constrained IoT Device Authentication

Vincent Omollo Nyangaresi, Tom Mboya University College, Kenya*
Anthony Joachim Rodrigues, Jaramogi Oginga Odinga University of Science and Technology, Kenya
Ahmad A. Al Rababah, King Abdulaziz University, Saudi Arabia

ABSTRACT

Wireless sensor networks (WSNs) are crucial components of internet of things (IoT) and have been deployed in numerous fields such as battlefield surveillance. The exploitation of broadcasts in WSNs renders these networks susceptible to numerous attacks. Consequently, to boost security, reliability, and successful cooperation, trust must be established among the sensor nodes. Unfortunately, the current authentication and authorization approaches exhibit high key management overheads, depend on static digital signatures or trusted third parties, and have both high communication latencies and computational complexity that render them inefficient. In this paper, challenge-response mutual authentication protocol is proposed for enhancing security in WSN-based IoT environment. The simulation results showed that the proposed protocol has the least transaction costs, time complexity, end-to-end delays, and energy consumptions. It is also resilient against dictionary, side channel, cloning, man-in-the-middle (MitM), denial of service (DoS), and next password prediction attacks.

KEYWORDS

Attacks, Authentication, IoT, Privacy, Protocol, Security, Sessions, WSN

INTRODUCTION

WSNs are crucial components of IoT and as explained by El-hajj et al. (2019), IoT application spectrum includes smart cities, homes, wearables, e-health among others. These devices are smart enough to collect, analyze and even make decisions devoid of human interaction. In this environment, security and specifically authentication is critical owing to the devastating effects of malicious unauthenticated device in an IoT system. Depending on the type of application, IoT security requirements may include authentication, confidentiality or integrity (Nyangaresi et al., 2020). As pointed out by El-hajj et al., (2019), authentication is key since trusting devices making up an IoT network is crucial for the better operation of the network. For instance, if one sensor node (SN) is compromised, then the entire network can be brought down or result in disasters. Fadi and David (2020) explain that IoT offers connectivity to internet devices that provide interactivity between physical and cyber objects. This facilitates data observation and measurement of physical entities. As explained by Harbi et al., (2019), both WSN and IoT are characterized by decentralization where security measures and authentication procedures are deployed at both device and network levels to enhance network reliability. However, Kouicem et al., (2018) explain that IoT devices are resource constrained owing to limited battery power. Their communication and information access is via open wireless channels, which renders them susceptible

DOI: 10.4018/IJITN.302118 *Corresponding Author

to threats such as eavesdropping. To boost smart manufacturing and increase productivity, Industrial Internet of Things (IIoT) has been developed to address the complexity and sophistication of the manufacturing process. As such, the entire manufacturing process consists of a number of diverse administrative IoT domains where devices from dissimilar domains collaborate on a similar task. This brings forth security and privacy issues regarding device to device communications. Worse still, the current authentication schemes exhibit high key management overheads (Nyangaresi et al., 2020) or depend on a trusted third party (Shen et al., 2020). Consequently, security and privacy issues during IoT device communication still present some challenges.

According to Kumar et al., (2020), the development of mobile Internet of Things (IoT) has led to the invention of many smart mobile services. Unfortunately, Zeng et al., (2018) point out that owing to their explosive growth and connectivity, malicious attacks can result in an unauthorized access to these devices. As such, the provision for security has become a very crucial design consideration for IoT systems that support heterogenous, machines, devices and industry processes. As discussed by Fang et al., (2020), current authentication and authorization protocols rely on static digital techniques and have high computational complexity. Therefore, they are insufficient for IoT environment. In addition, these security designs for diverse layers and link segments are desolate and disregard the overall protection, causing high communication latencies, overheads and cascaded security risks. Alladi and Chamola (2020) point out that the application of IoT in healthcare leads to sensitive patient data being sent over the networks, which calls for the deployment of robust security techniques to thwart cyber attacks.

It is explained by Mabodi et al., (2020) that due to wide distribution, relatively high processing power and wide openness, IoT devices are susceptible to gray hole attacks where an adversary masquerades as being the shortest path to the destination. In addition, Husamuddin and Qayyum (2017) identify authorization, authentication, integrity, non-repudiation, confidentiality, availability, and privacy as the main IoT security issues. In terms of the IoT layers, security issues can be at the perception layer, network layer, or application layer and hence there is need for a multi-layer security approach. The contributions of this paper include the following:

I. A hardware assisted authentication protocol is developed using Physical Unclonable Function (PUF) and True Random Number Generator (TRNG).
II. Challenge-response pairs (CRPs) are deployed to secure the transport layer traffic.
III. Dynamic multi-keys coupled with nonce for session keys and CRPs are introduced during mutual authentication process.
IV. It is shown that (I)-(III) above thwart node falsification, DoS, side-channel and dictionary attacks.

The rest of this paper is organized as follows: Section II discusses related work while Section III outlines the system model of this protocol. Section IV presents results and evaluation of this protocol while Section V concludes the paper and gives future work.

RELATED WORK

A number of schemes have been developed to secure WSN IoT communications. For instance, Mughal et al., (2019) developed a logical tree-based security mobility management (LTSMM) to minimize rekeying issues in WSN supported IoT. Since it employs group keys for authentication, management of group keys becomes complicated when the number of WSN devices increases or when one entity becomes malicious. To prevent DoS attacks in WSN routing for IoT, Lyu et al., (2019) proposed an entropy-based selective authentication scheme in WSN routing for IoT. Although it ensures data integrity and also boosts data delivery rate, its focus was only on DoS prevention, ignoring other attacks.