International Journal of System Dynamics Applications
Volume 11 • Issue 2

Multi-Layer and Clustering-Based Security Implementation for an IoT Environment

Deena Nath Gupta, Jamia Millia Islamia, India
https://orcid.org/0000-0001-6323-411X

Rajendra Kumar, Jamia Millia Islamia, India

ABSTRACT

IoT devices have many constraints related to computation power and memory. Many existing cryptographic algorithms of security could not work with IoT devices because of these constraints. Since the sensors are used largely to collect the relevant data in an IoT environment, and different sensor devices transmit this data as useful information, the first thing that needs to be secured is the identity of devices. The second most important thing is the reliable information transmission between a sensor node and a sink node. While designing the cryptographic method in the IoT environment, programmers need to keep in mind the power limitation of the constraint devices. Mutual authentication between devices and encryption-decryption of messages needs some sort of secure key. In the proposed cryptographic environment, there will be a hierarchical clustering, and devices will get registered by the authentication center at the time they enter the cluster. The devices will get mutually authenticated before initiating any conversation and will have to follow the public key protocol.

KEYWORDS

Cryptographic Protocols, Device-to-Device Communication, Hierarchical Clustering, Information Security, Internet of Things, Lightweight Cryptography, Mutual Authentication, Random Number Generation

INTRODUCTION

Random numbers play an essential role in cryptographic applications. The journey started long back in 1983 when the scientists from the University of California presented their work on random number generation. This work is commonly known as the Blum Sub generator (Blum, 1986). IoT is also known as the constrained environment because devices used in this network are low powered. These devices are not capable of performing complex mathematical calculations because of the large number of Circuit Gates, more than 2000 Gate Equivalent (GE), used. The EPCglobal® restricts the GE to be less than 2000 for the use in constrained devices (GS1, 2013). Hence the researcher needs some sort of less complicated procedure for their calculations. Mathematicians find that the computational power required for shift operations needs much lower power than the other mathematical operations. The researcher can use any of the listed shift operations (left shift, right shift, circular shift, etc.) to permute their bit sequences (GUPTA et al., 2020).

DOI: 10.4018/IJSDA.20220701.oa3

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Some test suites are there to examine the randomness of generator functions. One can test RNG work on Diehard battery designed by Marsaglia or on TestU01 suite with 6 test batteries (Small Crush, Crush, Big Crush, Alphabit, and Rabbit batteries and a pseudo-NIST battery) designed by L'ecuyer and Simard, or on the NIST test suite having 15 tests. The National Institute of Statistics and Technology released SP800-90 (a, b, c) recently (Rukhin et al., 2010).

Here, the authors are following the specifications given by the National Institute of Standards and Technology. A uniform and independent distribution of both the digits (zero and one), is the prime requirement from an ideal random number generator. A random number generator used in current cryptographic applications is a sequence of 26-bit or 32-bit discrete values. One can further divide random number generators into two parts; True Random Number Generators (TRNGs) and Pseudo Random Number Generators (PRNGs). The natural source of randomnesses like oscillators or thermal noise is in use for the generation of exact random numbers. These sources are unpredictable because of entropy. This variation produces a random output. Pseudo Random Number Generators (PRNGs) or Deterministic Random Number Generators (DRNGs) are purely based on programming (Gupta & Kumar, 2019).

Peris et al. presented their work in 2007 in which they generated some random numbers and then applied genetic programming on them to create a large number of sequences. They, however, are not that efficient in terms of circuit gate count but somehow manage to be less than 2000 GE (minimum requirement to name any algorithm lightweight) (Peris-Lopez et al., 2009). In 2008, Che et al. proposed a new method of generating random numbers by using valid random physical sources, like low-frequency oscillators and thermal noise generators. As they create output bits using very little power, one can use it as a component in his/her RNG design (Che et al., 2008). Electronic Product Code (EPCglobal®) issues some specifications regarding the manufacturing details of tags and readers. One should follow these restrictions to make their security design compatible with lightweight cryptographic applications. Any random number generator should go through the NIST suite to test their randomness. Many other tests are also available like the ENT test, David Sexton's battery, Diehard suite to check the randomness in obtained sequences.

IoT devices are having many constraints related to computation power and memory etc. Many existing cryptographic algorithms of security could not work with IoT devices because of these constraints. Since the sensors are used in large amounts to collect the relevant data in an IoT environment, and different sensor devices transmit these data as useful information, the first thing that needs to be secure is the identity of devices. The second most important thing is the reliable information transmission between a sensor node and a sink node. While designing the cryptographic method in the IoT environment, programmers need to keep in mind the power limitation of the constraint devices. Mutual authentication between devices and encryption-decryption of messages need some sort of secure key. In the proposed cryptographic environment, there will be a hierarchical clustering, and devices will get registered by the authentication center at the time they enter the cluster. The devices will get mutually authenticated before initiating any conversation and will have to follow the public key protocol.

The organization of the study is as follows—section 2 surveys related works based on different technologies of the lightweight security scheme. Proposed public key protocol is described in section 3. Section 4 presents the layering and clustering of devices in an IoT environment. Section 5 describes the proposed method having four modules, namely, the BiBiSeG module, the RandKeyGen module, the KeyConversion module, and the EncDec module. In section 6, the authors show the implementation of the proposed method. It includes device registration, mutual authentication, public key protocol, and hierarchical clustering. Section 7 presents the experimental setup and results. Section 8 shows the security analysis. Section 9 describes the countermeasure of expected threats. Section 10 gives the conclusion and future work.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/multi-layer-and-clustering-based-security-implementation-for-an-iot-environment/281694

Related Content

Fault Tolerant Control of an AUV using Periodic Output Feedback with Multi Model Approach

Sneha Joshiand D. B. Talange (2016). *International Journal of System Dynamics Applications (pp. 41-62).*

www.irma-international.org/article/fault-tolerant-control-of-an-auv-using-periodic-output-feedback-with-multi-model-approach/150479

Indigenous Knowledge Management and Humanitarian Supply Chain for Disaster Mitigation and Sustainable Development in the Eco Communities of India: Holistic Systems Modeling Approach

Sanjay Bhushanand Saurabh Mani (2021). *Handbook of Research on Modeling, Analysis, and Control of Complex Systems (pp. 211-249).*

www.irma-international.org/chapter/indigenous-knowledge-management-and-humanitarian-supply-chain-for-disaster-mitigation-and-sustainable-development-in-the-eco-communities-of-india/271040

Exploration of Temperature Constraints for Thermal-Aware Mapping of 3D Networks-on-Chip

Parisa Khadem Hamedani, Natalie Enright Jerger, Shaahin Hessabiand Hamid Sarbazi-Azad (2013). *International Journal of Adaptive, Resilient and Autonomic Systems (pp. 42-60).*

www.irma-international.org/article/exploration-of-temperature-constraints-for-thermal-aware-mapping-of-3d-networks-on-chip/95746

Mathematical Preliminaries

(2013). *Decision Control, Management, and Support in Adaptive and Complex Systems: Quantitative Models (pp. 45-61).*

www.irma-international.org/chapter/mathematical-preliminaries/74433

Reliability-Aware Proactive Energy Management in Hard Real-Time Systems: A Motivational Case Study

Satyakiran Munagaand Francky Catthoor (2010). *International Journal of Adaptive, Resilient and Autonomic Systems (pp. 1-11).*

www.irma-international.org/article/reliability-aware-proactive-energy-management/48259