Mentor: KOBBANE Abdellatif
ETTIACHE Ikrame
EL-FAKIR Mohamed

IOT SECURITY AND DESIGNING MECHANISMS

Abstract *Low power communication is a major milestone for the Internet of Things (IoT). Low-Power Wide-Area Network (LPWAN) technologies seek to provide a large coverage area and long battery life at the cost of a reduced bandwidth compared to traditional networks. The deployment of the Internet of Things (IoT) has led to an expansion of the attack surface, requiring end-to-end security mitigation measures. IoT applications range from critical dilemmas (e.g. smart grids, intelligent transport systems, video surveillance, e-health) to business-oriented applications (e.g. banking, logistics, insurance, and contract law). Full support for IoT security is required, especially for mission-critical and downstream business applications. Many technologies and security methods have been proposed and used. The blockchain mechanism plays a role in protecting many IoT oriented applications by becoming an integral part of security integration. A blockchain is a database that stores all processed transactions or data in chronological order. This data or data is stored in a set of tamper-proof computer memory. Then all participating users share these transactions. The information is stored and published in a public register which cannot be modified; each user or node in the system keeps the same registry as all other users or nodes in the network. This article focuses on some IoT environments where blockchain plays an important role and highlights that blockchain mechanism is only one part of the IoT Security Solution.*

Keywords Iot, Blockchain, LPWAN

1. Introduction

Low-Power Wide-Area Network (LPWAN) is one of the enabling technologies of the Internet of Things (IoT). An LPWAN is a network designed to allow long-range communications among smart devices, at low bit-rates. This type of network applies to IoT scenarios where low-cost devices need to transmit small messages over long distances (a few kilometers) and transmission delay is to lerableby the application. In LPWANs, end-devices are connected to a gateway node in a direct manner,thus forming a star topology. The simplified design of LPWANs and duty cycling provide a significant reduction in power consumption. Moreover, the great majority of communications in an LPWAN occur from the end-node to the gateway. This enables end-devices to enter in sleep mode after sending a message, and remain sleeping for long time intervals. Currently, several LPWAN solutions are available, among them LoRa stands out as one of the most promising LPWAN technologies.In LPWANs, especially for LoRa, security is a major concern. In the literature, several works have exposed the susceptibility of LoRa to attacks, in the phases of key management, network connection,and communications. Although many security improvements have been added to the architecture of LoRa in more recent specifications, much work still needs to be done in this regard.Blockchain is a disruptive technology that offers many benefits that can be used in IoT scenarios to address several challenges. Such benefits include decentralization, scalability, security and privacy. Blockchain eliminates the necessity for a central authority, since it works as a distributed database capable of storing every single operation performed by participating parties in a given system. All this is done with extensive use of consensus-based techniques and cryptography, in order to provide important features such as data securityand anonymity.

2. Technical differences: LORA, SIGFOX, NB-IOT and DASH7

In order to overcome the limitations of short range protocols Low Power Wide Area Networks (LPWAN) are introduced, which offer a long range connectivity in the order of kilometers. LPWAN [1] is getting wide acceptance in industrial and research communities due to its low power long range characteristics. LPWAN technologies (e.g: LoRa, Sigfox, NB-IoT and DASH7) each has its own advantages and limitations in term of IoT factors. NB-IoT and Sigfox offer long range connectivity and low cost devices. Most of the technologies offer long battery life, reliable communication. Among them NB-IoT will give high-value in IoT markets. NB-IoT offers low latency and high quality of services. NB-IoT use LTE encryption while other technologies use AES encryption methods. The actual battery life, security and performance of NB-IoT is currently an open question. From the case study of LoRa and its security vulnerabilities it is clear that LoRa devices are prone to various security attacks despite of the security mechanism offered by it.

the image below summarizes the difference between its technologies:

	LoRa	NB-IoT	Sigfox	DASH7
Bandwidth	125 KHz	180 KHz	100 Hz	25 KHz/200KHz
Frequency	Below 1 GHz	Below or above 1GHz	Below 1 GHz	Below 1 GHz
Downlink peak data rate	50 Kbps	250 Kbps	600 bps	55.55 Kbps
Uplink peak data rate	50 Kbps	250 Kbps	100 bps	9.6 Kbps
Module cost	Low	Low	Very low	Low
Data confidentiality	Yes	Yes	No	Yes
Authentication and encryption	Yes(AES 128)	Yes (LTE Encryption)	No	Yes
Bidirectional	Yes/Half-duplex	Yes/Half-duplex	Limited/Half-duplex	Yes/Half-duplex
Standardization	LoRa Alliance	3GPP	Sigfox company	DASH7 Alliance
Range	15-20 km	22 km	30-50 km	2 km
Battery life	10 years	10 years	10 years	10 years

Figure 1. Comparison of LPWAN technologies

3. IoT blockchain approaches

Fundamentally the IoT can utilize blockchains to ensure integrity of the business logic data. The IoT is the key to smarter cities, transportation systems, energy systems, and health care. To deal with the increasing number of IoT devices, it is necessary to standardize the meth-od of communication for IoT gateways and create a common IoT back end. Using blockchains decentralized, trustless nature in combination with DDOS-resistant, fault-tolerant data stor-age, a new type of IoT back end may be created. In this way, all kinds of IoT end devices may be integrated with this in-frastructure based on their computing and storage capabilities. Such an achievement will lead to data-centric business models where application development and data processing can be massively conducted by using smart contracts.

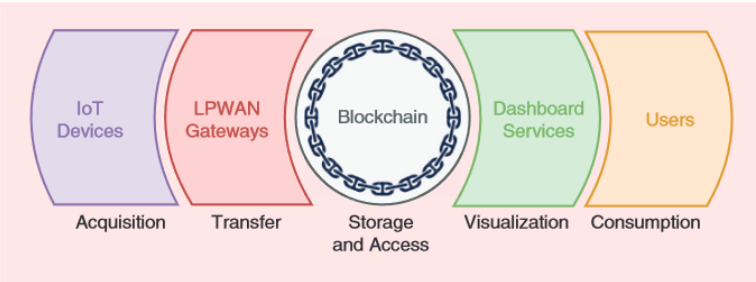

Figure 2. IoT architecture overview

4. LoRa Network and Blockchain Scaling

LoRaWAN has several mechanisms to provide security for the whole network. Data encryption is used in two different layersnetwork and application. Each end-device is configured with one key for the network layer and another key for the application layer. These two keys are referred to as root keys. LoRaWAN uses the Advanced Encryption Standard (AES) encryption algorithm to provide data confidentiality for both the MAC layer and the application layer. AES is also used to ensure frame integrity, by using Message Integrity Codes. There are two types of blockchainpublic and permissioned. They basically differ from each other in terms of performance, consensus algorithm, and read permission. In public blockchains,the elevated amount of participating nodes and validations result in decreased throughput and increased latency. Also, any node in the world can make part of the consensus process in public blockchains and all transactions are visible to anyone else. On the other hand, in permissioned blockchains, the smaller number of validations and the limited amount of nodes participating in the consensus process result in much faster transactions. Moreover, only authenticated nodes can participate in the consensus process of permissioned blockchains and only the organization responsible for maintaining the blockchain network can decide whether the transactions are restricted or visible to the public.

5. Conclusion

This paper presents a secure architecture for the key management mechanism in LoRaWANnetworks based on a permissioned blockchain network. The proposed solution makes use of confidential transactions and takes advantage of the decentralized design of blockchains . In addition, due to the blockchain features, all requests executed in the network are recorded in an verifiable and immutable way by theproposed architecture. Finally, to handle the encryption keys of all end-devices, a smart contract was implemented in the architecture.In order to validate the feasibility of the proposed architecture, a working prototype has been implemented also. The use of multiple ledgers for authenticationand application data in LoRaWAN will also be evaluated. Moreover, performance evaluations of the implemented prototype will be done using real hardware.

Acknowledgements

The work presented in this paper was a synthesis of three scientific papers based on IoT, Security and Blockchain...

References

[1] Usman Raza P.K., Sooriyabandara M.: *Low Power Wide Area Networks: An Overview, IEEE Communications Society on.* IEEE, 16 January 2017.

Affiliations

Mentor: KOBBANE Abdellatif
kobbane@gmail.com, ENSIAS

ETTIACHE Ikrame
Ensias, ikramettiache@gmail.com

EL-FAKIR Mohamed
Ensias, elfakir.med1@gmail.com