Brief Announcement: Providing End-to-End Secure Communication in Low-Power Wide Area Networks

Ioannis Chatzigiannakis[1], Vasiliki Liagkou[2], and Paul G. Spirakis[3,4]

[1] Sapienza University of Rome, Italy
[2] Computer Technology Institute and Press "Diophantus", Patras, Greece
[3] Computer Science Department, University of Liverpool, UK
[4] Computer Engineering and Informatics Department, Patras University, Greece
E-mails: ichatz@dis.uniroma1.it, liagkou@cti.gr, p.spirakis@liverpool.ac.uk

Abstract. Recent technologies for low-rate, long-range transmission in unlicensed sub-GHz frequency bands enables the realization of Long-range Wide Area Network. Despite the rapid uptake of LPWANs, security concerns arising from the open architecture and usage of the unlicensed band are also growing. While the current LPWAN deployments include basic techniques to deal with end-to-end encryption there are specific security issues that arise due to the overall architecture and protocol layer design. In this paper, a new scheme to establish end-to-end secure communication in long-range IoT deployments is introduced. The advantages over the existing approaches and architectural design are presented in the context of typical smart cities application scenarios.

1 Introduction to Security Issues & Vulnerabilities in LPWAN

In the past few years, the approach of exploiting sub-GHz was proposed in order to increase the transmission range of nodes by trading-off data transmission rate while keeping power consumption at low levels [1]. This so-called Low-Power Wide Area Networks (LPWANs) allow IoT devices to connect to Concentrators (also called a *collector*) over distances in the range of several kilometres. Concentrators forward data received from the IoT devices to a Network Server (over for example Ethernet or 3G/4G/5G) that manages all the decoding of the packets and handles redundant transmissions. Overall, LPWANs are considered promising candidates for IoT applications, since they allow *high energy autonomy* of the connected devices, *low device and deployment costs*, *high coverage capabilities* and support *large number of devices* [2].

Recently some technical papers concentrated on the security vulnerabilities in LPWANs providing alternative solutions for the used cryptographic primitives [3], focus on application server vulnerabilities [4] or introduce alternative key management [5].

In LPWANs the encryption of the payload is by default enabled in every transmission. The data frame of an end-node has a 32-bit identifier, a 7-bit network identifier and a 25-bit network address and the maximum payload is 250 Bytes. Since IoT devices are not assigned to a specific concentrator, the data frames do not include any concentrator identifier. In this way, it is possible for anyone to receive the encrypted data packets. In

order to prevent from replaying packets, a frame counter is used both for upstream and downstream messages which will block a transmission from being sent more than once.

Two different 128-bit AES keys are used for a two-step message chain for both upstream and downstream message exchanges. In the first step, an Application Session Key (AppSKey) is used to encrypt the data frame between the IoT device and the application server. In the second step, a Network Session Key (NwkSKey) is used to verify the authenticity of the nodes. The data frame exchanged between the IoT device and the Network server is encrypted with the NwkSKey. Therefore, each message is encrypted by using the XOR operation with the corresponding key.

Currently in LPWAN there are specific security issues that arise due to the overall architecture and protocol layer design:

Keys Storage Keys need to be safely stored by the IoT devices, the Network Server and the Application Server. Moreover in LPWAN network the IoT device is placed to an unprotected external or internal environment for very long time thus its impractical and costly to increase the physical security level of the IoT devices.

Symmetric Encryption Factors AES is operating in counter mode (CTR) and not in electronic codebook (ECB) mode. In this mode of operation, IoT devices generate cyphertexts which are output of the XOR procedure on the string that contains a counter, the AppSkey and the plaintext As a result, encryptions are vulnerable to chosen cyphertext attack since if an attacker changes the payload data she can figure out which bit position in the encrypted payload corresponds to the same bit position in the plaintext. major security flaw.

Authentication The Network Server and the intermediate concentrator (or an attacker on the intermediate network) are in a position to modify the encrypted payload without the Application server being able to notice the change. If an adversary could posses the session key, then he can generate a LoRaWAN message that will pass the signature checking procedure at the network server.

Compromised IoT device LPWANs are suitable for large deployments of battery operated static IoT devices that remain for long periods of times (in many cases spanning several years) in semi-controlled environments or even uncontrolled areas.

Untrusted Concentrators Traffic passing through this point can be easily recorded and even manipulated.

2 An End-to-End Secure Communication Scheme

The LoRa LPWAN architecture is extended by introducing the so-called *Median Server* that complements the functionality of the Network Server and Application Server by taking over the role of the *Registration Authority* of the system both for IoT devices and concentrators. A PKI Credential Authority (CA) is introduced to ensure that only authenticated IoT devices interact with the system and connect only to an authenticated concentrator that issued their certificates.

The overall security is further reinforced by establishing a VPN network for the communication between the concentrators, the median server and the network server. The VPN connections use SSL sessions with bidirectional authentication (i.e., each

side must present its own certificate). A block cypher and fingerprint (hash value) for encrypting/decrypting packets are activated along with the HMAC construction to authenticate them. In this way, passive attacks (packet sniffing, eavesdropping) are eliminated. However, even if packet encryption is unbreakable, it does not prevent active attackers to insert into a communication channel and add, modify or delete packets. Active attacks are thwarted by embedding Device Identifier (DevEUI) (timestamps) on packets and make IoT devices able to keep track of timestamps in order to make sure that they never accept a packet with the same timestamp twice.

Furthermore, the critical data like symmetric keys, private-public keys and IoT device credentials are protected using a *HMAC* before they are stored into the Network server and Application server to further assure their integrity. In particular, the HMAC-MD5 is used within the Application server on IoT device credentials (username, password). In this way, critical data disclosure is prevented in situations like database server thefts or unscrupulous administrators.

In terms of *preventing modifications on payload data*, a MAC is used to authenticate transmitted payload data against any modification. The Application server verifies that the message was received from an authenticated IoT device and subsequently decrypts it and locks it in order to detect possible post-modifications and illicit manipulations.

A fundamental requirement for the proposed model is to strictly link IoT device tasks with system's application data. The proposed architecture is associated with a workflow mechanism that guarantees data transmission thought heterogenous parties whereas supervising user's device interaction. In LPWAN the data rate transitions between the IoT device and LPWAN infrastructure is low and makes the security synchronization interaction mechanisms impractical thus the flow control determines a certain lifecycle for payload application data, from its insertion into the LPWAN till the time that is ready to be stored and utilized by the application server. IoT device payload passes through certain phases introduced by the mechanism. Each phase has its own predefined tasks committed by the user. The mechanism introduces associations between phases (i.e., each phase depends on the successful completion of its previous one) and executes them in a linear fashion (1^{st}, 2^{nd}, ...), making a discrete workflow for each payload.

References

1. M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi. Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios. *IEEE Wireless Communications*, 23, October 2016.
2. Ioannis Chatzigiannakis, Andrea Vitaletti, and Apostolos Pyrgelis. A privacy-preserving smart parking system using an iot elliptic curve based security platform. *Computer Communications*, 89-90:165–177, 2016.
3. Jaehyu Kim and JooSeok Song. A simple and efficient replay attack prevention scheme for lorawan. In *ICCNS*, 2017.
4. Jordy Michorius. Whats mine is not yours: Lora network and privacy of data on publishing devices. 2016.
5. Sarra Naoui, MoMohamed Elhoucine Elhdhili, and Leila Azouz Saidane. Enhancing the security of the iot lorawan architecture. In *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, pages 1–7, Nov 2016.