Physical Layer Security based Key Management for LoRaWAN

Andreas Weinand[*], Andreu G. de la Fuente[†], Christoph Lipps[+], Michael Karrenbauer[*]
[*]Institute for Wireless Communication and Navigation (WICON), Technische Universität Kaiserslautern (TUK), Germany
[†]Telecommunication School in Barcelona (ETSETB), Universitat Politècnica de Catalunya (UPC), Spain
[+]Intelligent Networks Research Group, German Research Center for Artificial Intelligence, Kaiserslautern, Germany
Email: [*]{weinand, karrenbauer}@eit.uni-kl.de, [†]girones96@gmail.com, [+]christoph.lipps@dfki.de

***Abstract*—Within this the work applicability of Physical Layer Security (PHYSEC) based key management within Long Range Wide Area Network (LoRaWAN) is proposed and evaluated using an experimental testbed. Since Internet of Things (IoT) technologies have been arising in past years, they have as well attracted attention for possible cyber attacks. While LoRaWAN already provides many of the features needed in order to ensure security goals such as data confidentiality and integrity, it lacks in measures such as secure key management and distribution schemes. Since conventional solutions are not feasible here, e.g. due to constraints on payload size and power consumption, we propose the usage of PHYSEC based session key management, which can provide the respective measures in a more lightweight way. The results derived from our testbed show that it can be a promising alternative approach.**

***Index Terms*—IoT, security, LoRaWAN, PHYSEC**

I. Introduction

Since the upcoming of IoT applications, there have been many radio technologies proposed as enablers for the transmission of data from end devices, such as sensor nodes, towards cloud or other central processing entities. These can provide advantages in the sense of a higher deployment flexibility and enable the connection of a huge number of devices at a low cost, compared to wired systems. On the other hand, they bring challenges and risks due to the open nature of the wireless channel. Especially in industrial scenarios, such as e.g. smart metering, agricultural applications or process monitoring, the nondisclosure of intellectual property such as process control parameters, machine configuration data or even simple information such as the production volume have to be ensured. Beside online attacks interfering with such applications and causing damage instantly, other risks such as blackmailing have increased recently as well.

In order to prevent such cyber attacks, e.g. symmetric key cryptography ciphers such as the Advanced Encryption Standard (AES) [1] can be used to ensure data confidentiality and integrity. Both of these requirements are fulfilled by the LoRaWAN [2] protocol, which utilizes the AES-128 cipher suite for data encryption and decryption and AES based Cipher based Message Authentication Code (CMAC) [3] as message integrity code. Since the keys used for the respective AES operation are typically derived manually from device manufacturers, this offers a high possibility for disclosure. Additionally, the root key is typically hard coded on both sides, end device and the LoRaWAN network or application server. This brings the problem, that it can not be refreshed regularly, in order to enable security concepts such as perfect forward secrecy. Conventional key management schemes, such as e.g. Diffie Hellman Key Exchange (DHKE), are not applicable here due to their high requirements towards computational power and transmission overhead. Further, the key management should be realized at a high level of usability, where no manual configuration is required by e.g. a system administrator. This is especially due to scalability reasons, occuring e.g. in massive IoT scenarios. All these requirements can be fulfilled by PHYSEC based key generation, where the idea is to exploit the characteristics of the wireless channel as a random process and derive a secret key from that. There are however some other conditions to be fulfilled, such as channel reciprocity between two parties deriving a secret key. That means, the time and frequency at which both of them sample the channel have to be aligned. Resulting from that, key bits derived from that process might not be identical between two parties and require further processing and communication for information reconciliation. Therefore, it is desired to keep the erroneous bits before that stage as low as possible by applying optimal quantization and reciprocity enhancement schemes. Further, it has to be ensured, that initial trust is set up between involved parties, such as a cryptographic authentication process. A periodic session key refreshment procedure can then be realized by support of PHYSEC based Secret Key Generation (SKG) on top of that trust root.

The remaining work is structured as follows, within section II we present related work considering PHYSEC and especially the concept of SKG. In section III we introduce the LoRaWAN protocol and within section IV, the PHYSEC based key generation procedure is presented. Section V elaborates the results derived from our testbed and section VI concludes our work.

This is a preprint, the full paper is published in Proceedings of 2020 Workshop on Next Generation Networks and Applications (NGNA 2020). Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the authors. A part of this work was funded by the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany (Foerderkennzeichen 16KIS1011, Industrial Radio Lab Germany). The authors alone are responsible for the content of the paper.