



Review

A Comprehensive Analysis of LoRaWAN Key Security Models and Possible Attack Solutions

Koketso Ntshabele ^{1,*}, Bassey Isong ^{1,*} , Naison Gasela ¹ and Adnan M. Abu-Mahfouz ² ¹ Computer Science Department, North-West University, Mafikeng 2745, South Africa² Council for Scientific and Industrial Research (CSIR), Pretoria 0184, South Africa

* Correspondence: bassey.isong@nwu.ac.za

Abstract: Low-Power Wide-Area Network (LPWAN) is a wireless WAN technology that connects low-powered and low-bandwidth devices with low bit rates atop Long Ranges (LoRa). It is characterized by improved scalability, wide area coverage, and low power consumption, which are beneficial to resource-constrained devices on the Internet of Things (IoT) for effective communication and security. Security in Long-Range Wide-Area Networks (LoRaWAN) widely employs Advanced Encryption Standard (AES) 128-bit symmetric encryption as the accepted security standard for a key generation that secures communication and entities. However, designing an efficient key manifestation and management model is still a challenge as different designs are based on different research objectives. To date, there is no global and well-accepted LoRaWAN security model for all applications. Thus, there is a need to continually improve the LoRaWAN security model. This paper, therefore, performed an in-depth analysis of some existing LoRaWAN key security models to identify security challenges affecting these security models and assess the strengths and weaknesses of the proposed solutions. The goal is to improve some of the existing LoRaWAN security models by analysing and bringing together several challenges that affect them. Several relevant studies were collected and analysed; the analysis shows that though there are few research works in this area, several existing LoRaWAN security models are not immune to attacks. Symmetry encryption is found to be the most used approach to manage key security due to its less computational operations. Moreover, it is possible to improve existing key security models in LPWAN with consideration of the resource constrained. Again, trusted third parties for key management were also widely used to defend against possible attacks and minimize operational complexities. We, therefore, recommend the design of lightweight and less complex LPWAN security models to sustain the lifespan of LPWAN devices.



Citation: Ntshabele, K.; Isong, B.; Gasela, N.; Abu-Mahfouz, A.M. A Comprehensive Analysis of LoRaWAN Key Security Models and Possible Attack Solutions. *Mathematics* **2022**, *10*, 3421. <https://doi.org/10.3390/math10193421>

Academic Editors: Jonathan Blackledge and Daniel-Ioan Curia

Received: 29 July 2022

Accepted: 8 September 2022

Published: 21 September 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: IoT; LoRaWAN; LPWAN; key security; attacks**MSC:** 94A60; 94A62

1. Introduction

The emergence of the Internet of Things (IoT) has brought about cross-platform communication over the Internet between different powered devices ranging in energy consumption from low to high [1–5]. A large amount of data is shared autonomously between these devices within widespread application areas such as healthcare, military, agriculture, industrial, and home applications [1,2,5]. To complement the flexibility of the IoT paradigm, various cellular communication networks with low energy consumption were introduced, such as Zigbee, Bluetooth, 2G, 3G, 4G, Z-Wave, etc. [2,6–12]. Although these cellular networks have several characteristics such as short-range communication, the full flexibility of IoT applications could not be fulfilled due to their wide-ranging area communication [2]. However, to deal with the shortfalls of these conventional cellular networks, Low-Power Wide-Area Network (LPWAN) was introduced [1,2,5,13]. LPWAN is considered a low cost-deployment, improved-scalability, wide range of communication,

and low power-consuming protocol [2]. Moreover, several communication protocols based on their technical unique characteristics and properties have been introduced in the realm of LPWAN, such as the Sigfox, Narrow Band-Internet of Things (NB-IoT), and Long Range (LoRa), with LoRa as the commonly applied protocol [2,13].

As shown in Figure 1, these protocols have several benefits for the IoT platform while Table 1 presents the characteristics of some of the LPWAN technologies. Accordingly, LoRa is implemented as a physical layer protocol to permit long-range communication in a wide coverage where less energy is consumed, while LoRaWAN is a medium access control (MAC) layer protocol implemented to define the system operations and structure [2]. Thus, to reduce the severity of high battery consumption and overheads due to synchronization, LoRaWAN adopts asynchronous communication models [2]. In the past, energy efficiency and communication in LPWAN have been a primary research area; however, security issues have recently dominated [2]. Considering the real-life relation to IoT, security and privacy issues are huge threats to the exponential increase of connected devices implemented in the specific geo-location [2]. Since a large amount of data is transmitted between these devices and the servers, there is a need for efficient security models to be put in place. Recently security issues and solutions in IoT have gained research attention, especially key management which ensures the safety and protects devices and data against attacks [2]. Moreover, to implement secure key management models, cryptography has been a favourable technique. Cryptographic techniques include encryption, authentication, message integrity checking, or a hybrid of these forms [2]. However, these techniques are prone to several security attacks due to the nature of the geo-location deployment of the devices where they can be easily accessible to the attackers [2,14]. A possible security breach can occur when communication is engaged between the servers and the end devices [2]. With the specifications implemented in LoRaWAN, the key management model must ensure that the communicating keys for security purposes are uniquely and securely managed [2]. However, current LoRaWAN specifications provide limited security by partially updating the generated keys [2]. Furthermore, in continuous communication, such specification remains infeasible since some of the keys might remain unchanged, and in the event of a key breach, all the information and communication in the network will become prone to attackers' interception [1,2]. To address this challenge, it is important that existing LoRaWAN key models are improved to allow fully automated and periodic key generation and updates [2]. In addition, communication layers such as application and network layers should adopt independent key-level security as each layer operates differently [2].

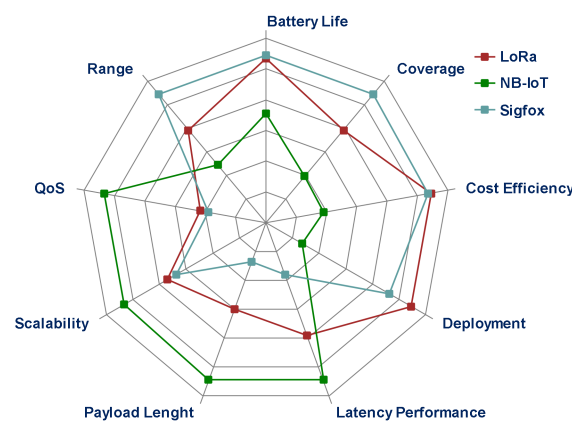


Figure 1. LPWAN protocols benefits in IoT [15].

Table 1. Technical characteristics of LoRa, Sigfox, and NB-IoT [15].

	Sigfox	LoRaWAN	NB-IoT
Modulation	BPSK	CSS	QPSK
Frequency	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Licensed LTE frequency bands
Bandwidth	100 Hz	250 kHz and 125 kHz	200 kHz
Maximum data rate	100 bps	50 kbps	200 kbps
Bidirectional	Limited/Half-duplex	Yes/Half-duplex	Yes/Half-duplex
Maximum payload length	12 bytes (UL), 8 bytes (DL)	243 bytes	1600 bytes
Range	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	1 km (urban), 10 km (rural)
Interface immunity	Very high	Very high	Low
Authentication & encryption	Not supported	Yes (AES 128b)	Yes (LTE encryption)
Adaptive data rate	No	Yes	No
Handover	End devices do not join a single base station	End devices do not join a single base station	End devices join a single base station
Localization	Yes (RSSI)	Yes (TDOA)	No (under specification)
Allow private network	No	Yes	No
Standardization	Sigfox company is collaborating with ETSI on the standardization of the Sigfox-based network	LoRa-Alliance	3GPP

This paper surveyed the existing traditional LoRaWAN security models to comprehend and bring together the security analysis of LoRaWAN traditional security models. The paper carried out a comprehensive analysis of LoRaWAN security under the existing traditional security models, analysed different existing proposed solutions and approaches to addressing several identified attacks that are affecting these security models, and identify open-security challenges considered for future improvement. This analysis will yield a proposal for an improved LoRaWAN security model that curbs the severity of the identified challenges still affecting traditional LoRaWAN security models.

The rest of the paper is organized as follows: Section 2 provides LoRaWAN background, LoRaWAN security architecture, and possible security attacks, Section 3 discusses related works, and Section 4 presents the comprehensive analysis of existing key security models in LPWAN/LoRaWAN, and Section 5 presents a discussion of the analysis. Section 6 discusses the possible research directions and lastly, Section 7 presents the article's conclusions.

2. Background Information

2.1. LoRaWAN

LoRaWAN is a popularly adopted LPWAN technology that is implemented based on the following; low energy consumption, better scalability, wide-area coverage, and low deployment cost [1]. In LoRaWAN architecture, several end devices are battery-powered and communicate with one another through the servers to share information. A single-hop communication is adopted between the end devices and the gateway which relays the shared information across the network [1]. The LoRaWAN model is made up of several entities as shown in Figure 2.

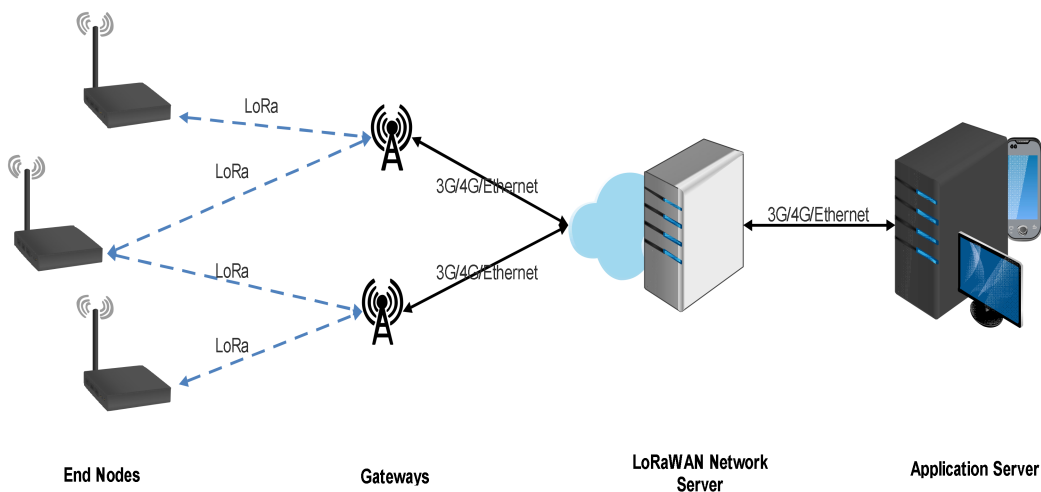


Figure 2. LoRaWAN architecture [4].

As shown in Figure 2, the LoRa protocol is structured into two parts: the front end which is composed of gateways and end devices where the gateway relays data between the servers and the end devices, and the back end which is composed of network servers [16]. The end devices are the LoRa endpoints for communicating with other end devices using shared communication keys. They are remotely located and controlled. The gateways relay communication data between the end devices. Moreover, the network servers are responsible for establishing communication keys that are shared between the application servers and the end devices. It is responsible for managing the whole network by scheduling the acknowledgements in communication, eliminating abnormal packets, and ensuring relevant data rates. Application servers, conversely, are responsible for communication with the end devices by offering the necessary applications to the end devices.

LoRaWAN functions by adopting LoRa capabilities such as its chirp spread spectrum (CSS) modulation, which controls several aspects such as switching through spreading factors (SFs) ranging between SF7 and SF12, modulation optimization for efficient communication range, and shared data requirements [1]. As shown in Figure 3, LoRa is implemented as a physical layer on top of the LoRaWAN, which is referred to as the MAC layer protocol [17]. LoRa uses the SFs to control unwanted interference and multipath fading [16]. Based on the transmission conditions and environment, the end devices are enabled to adjust their transmission power and modulation; the higher the SF increase, the more the signal-to-noise ratio (SNR) improves, the time spent in the air increases, and the bit rate decreases, and vice versa when the SF decreases [16]. Based on the communication specifications, LoRa can be implemented using three classes, A, B, and C as shown in Figure 3; however, as proposed by the LoRa standard, all the modules implemented should follow Class A specifications, whereas B and C are optional [16].

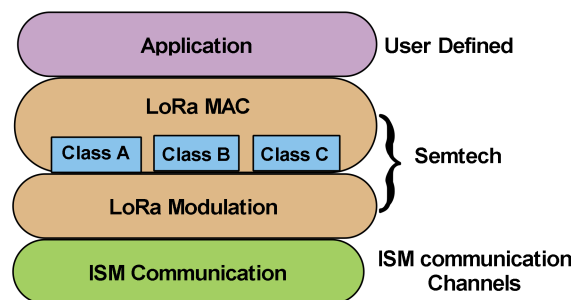


Figure 3. LoRaWAN node system architecture [16].

Class A: This implements bidirectional communication. Three-time slots are used for each transmission; when the Class A devices transmit (uplink) the data, Class A will upon two receiving times for data reception (downlink) transmitted from the gateway. However, the devices in this class can only receive the data once the data is being sent; this qualifies the devices to attain the highest energy efficiency possible which is most suitable for devices that consume less power [16].

Class B: Class B devices adopt bidirectional communication using extra time slots for receiving (downlink) the transmitted (uplink) data. Unlike Class A which adopts random slots for receiving the data, Class B uses a synchronized beacon from the gateway to activate a series of receiving time slots; higher data rates in a downlink can be attained.

Class C: The devices in Class C communicate in a bidirectional manner and use an extra communication time slot for receiving (downlink) unlimited data. However, the Class C devices are restricted to sending the data only during the sending period, but have no restrictions on data reception, which makes them suitable for communication with low latency [4].

2.2. LoRaWAN Security

LoRaWAN offers several benefits to LPWAN; thus, protection against attacks and breaches should be a priority. To effectively apply cryptographic security models in LPWAN IoT-based applications, key manifestation and management are indispensable. To this end, many cryptographic schemes can be implemented in LPWAN IoT-based applications, such as symmetric key encryption for resource-constrained devices, and asymmetric encryption. For symmetric encryption deployment, the participating devices generate and share a symmetric key for communication; however, this is inept for a large scalable network. Symmetric encryption schemes such as Advanced Encryption Standard (AES) 128-bit have been implemented in LoRaWAN to guarantee end-to-end security in the network. Participating entities are structured in star topology and a single or multiple gateway(s) are responsible for relaying the data between the end devices and network server. Generally, AES 128-bit security ensures integrity, authenticity, confidentiality, and bi-directional communication in the network, ensuring that only authenticated end-devices are allowed to communicate as shown in Figure 4. LoRaWAN communication uses a 128-bit Application key (AppKey) generated by the network server, and uses the same AppKey to generate two more keys: the Network Session Key (NwkSKey) and Application Session Key (AppSKey). The AppSKey is shared between the application servers and the network server while the NwkSKey is shared between the network server and the end devices through gateways. All AppKey, NwkSKey, and AppSKey are 128-bit hexadecimal numbers.

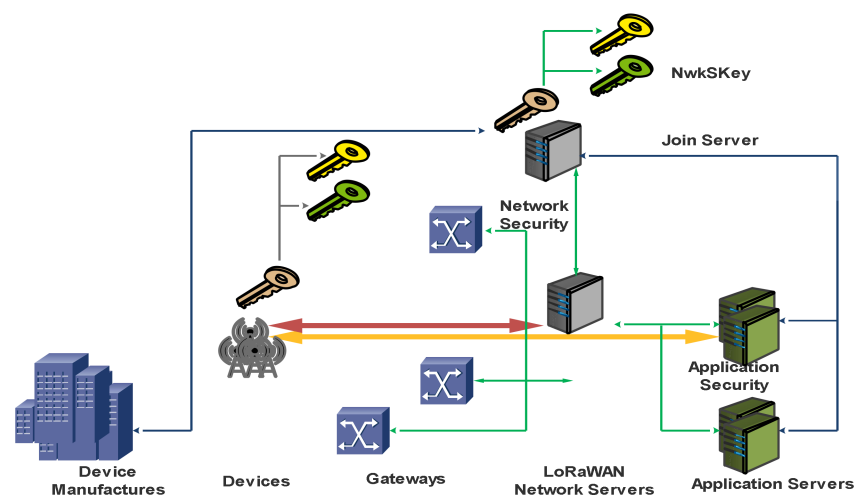


Figure 4. LoRaWAN communication model [1].

However, for the end devices to participate and be recognized in the LoRaWAN, the end devices must be activated. This can be accomplished in two ways: Over The Air Activation (OTAA) and Activation By Personalization (ABP). As presented in Figure 5, with OTAA, the end devices are expected to be pre-personalized and a 64-bit hexadecimal Device EUI (DevEUI) is used to identify the end device’s unique identity based on the network the end device will join, while a 64-bit hexadecimal Application EUI (AppEUI) is used for identifying applications and an AES-128 bit symmetric AppKey [1]. Once pre-personalized, the network and the end device will engage in communication using two messages. *Join Request* (JR) is sent by an end device and transmitted to the network server. The JR message contains the DevEUI, AppEUI and a 2-octet random number called a Device Nonce (DevNonce). An AppKey is used to compute the message integrity code (MIC) for the security of the JR message as the message is not encrypted. Upon the receipt of the JR message at the network server, the server performs integrity checking to verify if the requesting end device is allowed to join the specified network. If an end device is verified, the network sends a “*Join Accept* (JA)” message to the end device. The JA message is consist of a Network Identifier (NetID) which identifies the network assigned to the end devices, a 32-bit hexadecimal Device Address (DevAddr) which identifies the unique address of the end device in the network, and a 3-octet Application Nonce (AppNonce) [1].

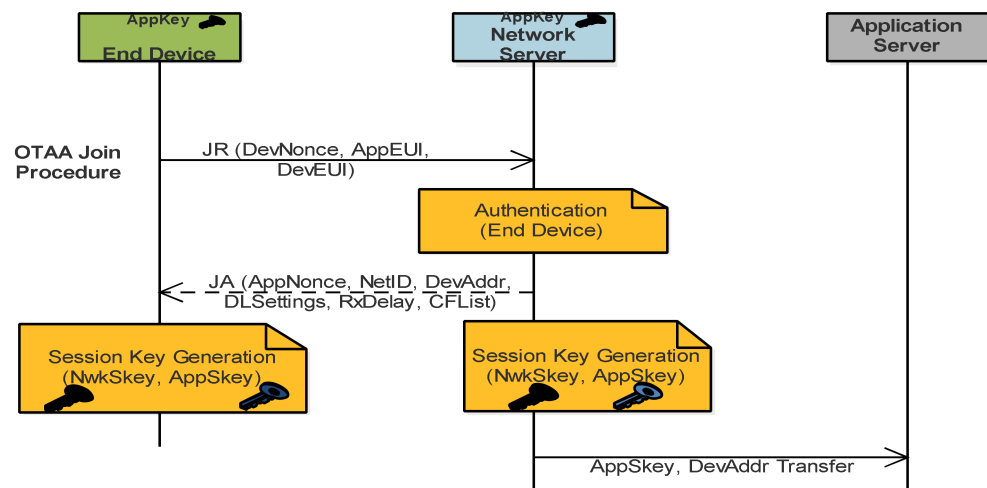


Figure 5. Figure LoRaWAN Over The Air Activation [18].

On the other hand, for ABP, communication can be initiated between the servers and the end devices after the end devices are pre-programmed with AppSKey, NwkSKey, and DevAddr [1]. It uses the nonces as pseudo-random numbers for entity authentication to ensure that previous communication messages cannot be used by the interceptors for replay attacks [3]. For message integrity, the Message Integrity Code (MIC) is generated by an AES-128 bit AppKey, which is appended to the message to be transmitted [3]. Once the MIC is received at any communicating point, if the re-calculated MIC is different from the received appended MIC, it indicates that the message has been tampered with or transmitted by an unauthorized entity [1]. Otherwise, no tampering occurs, the end device then computes a plain-text message and encrypts it with the AES-128 bit AppSKey and the encrypted plain text is sent to the application server, where the encrypted plain text is decrypted with the same AppSKey [1].

2.3. LoRaWAN Possible Attacks

There are several possible security attacks designed to compromise LoR WAN in terms of data confidentiality, integrity, and availability. Thus, LoRaWAN key security models must be regularly enhanced to withstand such adversaries in the network. This subsection discusses some of the existing attacks:

- i. *Denial of Service (DoS) attack*: The attack is associated with denying services to the entities connected to the network, such as denying the communication between the end devices. Due to the static configuration of keys and nonces, during a JR, an attacker can use the Application Key (AppKey) to re-calculate the MIC and the DevNonce for every transmission [1].
- ii. *Replay attack*: The attacker intercepts the transmitted data in the network by repeating or delaying that data in which the attacker can act as one of the participants in the network. In the case of ABP, the frame counters in the end-devices and the network server are re-used with the same keys as static keys are pre-programmed in the entities before joining request and join accept; hence, an attacker can re-use a previous message for replay attacks [1].
- iii. *Known-key attack*: The attacker exploits the AppSKey, and if the attacker discovers it, then the decryption mechanism will be discovered by the attacker [3].
- iv. *Eavesdropping attack*: Here, the attacker captures a large amount of transmitted information and attempts to extract the important information from the captured message, such as by capturing the AppSKey that is used for encryption and decryption [3].
- v. *Side-channel attack*: In the OTAA phase, a single AppKey without being updated is used throughout to compute the session keys; though the session keys can be re-updated for different sessions, the AppKey remains unchanged. If the AppKey can be intercepted during transmission, then the whole network and communication are compromised [2].
- vi. *Physical attack*: The attacker extracts the pre-shared key, such as an AppKey, from the end devices to make it easier to hijack [18].

3. Related Works

This section discusses some of the related works that analyse the security of the existing LoRaWAN security models. Eldefrawy et al. [19] argued that the advancement of LPWAN protocol resulted in a wide deployment across several sectors which brought about several known security vulnerabilities within the traditional LoRaWAN version 1.0 security model. Accordingly, some researchers use security tools such as the Scyther to perform a formal security analysis on the LoRaWAN version 1.0, where several vulnerabilities are not found in version 1.1. The analysis helped in improving LoRaWAN security. Similarly, Butun et al. [20] performed an analysis of security risks on the LoRaWAN 1.1 security model which enhanced the version 1.0 security model. According to several researchers, the analysis was the first to be conducted and discusses a detailed threat catalogue based on the threat scale view, impact, and likelihood. Moreover, practical threats that require immense attention from the organizations and the developers for LoRa network implementations are also discussed. Furthermore, Tomasin et al. [21] carried out a security analysis on the join procedures of LoRaWAN-IoT based on when the end device(s) wishes to initiate a join procedure with the registered network server. The study also discussed the security impacts of random numbers generated in the join procedure, and the abilities of the network server in detecting and preventing replay attacks.

In a similar study, Butun et al.'s [22] analysis of LoRaWAN 1.0 uncovered several security weaknesses that affect the data confidentiality, integrity and overall network availability where LoRaWAN back-end system or/and end devices are likely to be exploited. They found that the severity of these security vulnerabilities was entirely from a physical medium or access, but can be possible within the protocol. They also proposed practical recommendations to curb the severity of these attacks while being compliant with specifications and ensuring interoperability between old and improved equipment. In Butun et al. [23] the authors presented an overview analysis of the security of the traditional LoRaWAN 1.0 with several threats leading to LoRaWAN 1.1. They further discussed LoRaWAN 1.1's implementations of LoRa-based applications and its limitations. In the same vein, Eldefrawy et al. [19] conducted a formal and security analysis of the LoRaWAN protocol. The formal analysis approach was used to uncover several security vulnerabilities

identified in LoRaWAN 1.0's key exchange mechanism, which also resulted in LoRaWAN 1.1. In a similar study, Noura et al. [24] performed a comprehensive review on LoRaWAN architecture, security concerns, and applications, and presented several proposed solutions to address the security shortfalls and counter several identified attacks in the existing LoRaWAN. Finally, Yang [25] performed an analysis on LoRaWAN based on cryptography, key management mechanisms, counter management aspects and message acknowledgement. Several security vulnerabilities and attacks were identified, such as eavesdropping, replay, ACK spoofing, and bit flipping attacks. Consequently, they proposed an improved security and mitigation LoRaWAN models.

As discussed above, several authors [19,22,24] have carried out studies on several key aspects of LoRaWAN such as security analysis, key management architecture, etc. in LoRaWAN. However, these were not comprehensive enough as they do not focus on a particular aspect. Therefore, this paper focus specifically on the key management of traditional LoRaWAN security models to bring together the challenges.

4. Analysis of LoRaWAN Security Models

This section presents the analysis performed on each study considered in the paper from the perspective of LoRaWAN security models. The findings are categorized into key management, security attacks and proposed solutions.

4.1. Key Management

This subsection presents different solutions in each study in terms of the security objectives and the techniques utilized in existing LPWAN and IoT models within LoRaWAN. Tables 2 and 3 summarize the findings.

Table 2. Summary of Security Algorithms and Analysis in LoRaWAN.

Ref.	Security Algorithm	Key Gen. Time	Key Update Time	Execution Time	Memory Usage/Overheads	Energy Consume	Limitations
[2]	AES-128-SE	N/A	N/A	N/A	High	Low	Static key generation and loading, memory flooding due to storing nonces
[3]	AES-128 bit and D-Box	N/A	N/A	N/A	N/A	Low	Unsecure communication layers except for the application layer. No periodic updates for NwSKey in the MAC layer
[26]	Stream Cipher-Based KDF	High	Long	Less	High	N/A	Memory overheads in the end devices due to pre-sharing and distribution of the root keys
[5]	Rabbit Stream Cipher Based-KDF-SE	N/A	N/A	Faster encryption and velocity-time	High	N/A	High memory usage by generating additional 4-byte data of the devices in encryption and decryption.
[27]	Blowfish-SE	N/A	N/A	Faster and less encryption time	High	N/A	Not be suitable for scalable networks, and complex operations due to limited memory in FPGA
[4]	AES-128 SE	N/A	High	N/A	N/A	N/A	Irregular key refreshment periods

SE = Symmetric encryption, AE = Asymmetry encryption.

Table 3. Summary of Security Algorithms and Analysis in LoRaWAN.

Ref.	Security Algorithm	Key Gen. Time	Key Update Time	Execution Time	Memory Usage/Overheads	Energy Consume	Limitations
[28]	AES-128 SE	N/A	N/A	Less	N/A	Low	Limited to validation of three attacks only
[1]	AES-128 SE	N/A	N/A	Less	Low	Low	Unsecured random numbers to compute session keys. Static NwkKey changed in every session
[14]	ECC-Diffie Hellman algorithm (AE)	Faster	Faster	Faster	N/A	High	Limited validation and restriction of analysed attacks
[29]	AES-128 SE	N/A	N/A	Less	Low	Low	Evaluations of attacks are limited
[30]	AES-128 SE	N/A	N/A	N/A	Low	N/A	Forward compatibility should not be examined after backward compatibility
[31]	AES-128 SE	N/A	N/A	N/A	N/A	N/A	Asymmetric encryption is heavy on resources

SE = Symmetric encryption, AE = Asymmetry encryption.

Kim and Song [2] designed a dual key-based activation scheme that allows automatic key generation and updates where each LoRaWAN layer independently generates its keys. This model uses pre-programming and pre-loading techniques to generate session keys shared with the network and application servers for authentication and communication. The phases involved are as follows: the end-node generates the NwkKey and AppKey through pre-programming and preloading before initiating the joining procedure and sends NwkKey to the network server and AppKey to the application server. A JR message is transmitted by the end node containing MIC, AppEUI, DevEUI, and DevNonce to the network server for node authentication and session key generation. Accordingly, if the end-node is recognized by the network server, then the network server generates NwkSKey from NwkKey and forwards its NetID and DevNonce to the application server. Once forwarded, the application server generates the AppSKey from AppKey and transmits an encrypted AppNonce with AppSKey to the network server where it forwards the JA message to the end node. However, if the end node wishes to join the network again, it computes a new NwkSKey and AppSKey with the old NwkSKey and AppSKey.

Tsai et al. [3] proposed an AES-128-based energy-efficient and highly secure communication scheme known as Secure Low-Power Communication (SeLPC) for balancing the security level and the power consumption in the network. This is to ease end devices' high data-encryption power by reducing AES encryption cycles. The SeLPC has two stages: the key generation and the data encryption process [4]. Key generation is applied to minimize the complex operations via encryption keys called AppSKey and D-Box, which are dynamically and automatically updated for every k-days, where k is only known by the network manager. Moreover, data encryption is applied to ensure payloads' security and the MAC layer's integrity using an AppSKey to encrypt the payload at the application layer and the NwkSKey generates the MIC. In addition, the AES-128 deployed at the end-devices employs five encryption cycles to minimize the complex operations that are heavy on power consumption. The cycles are repeated for k-days to update the encryption key and D-Box, to restrict the attackers from exploiting the encryption system.

Han and Wang [26] suggested a LoRaWAN root key update mechanism to strengthen traditional LoRaWAN 1.0 and 1.1 security models. The study implemented a Rabbit Stream Cipher-Based KDF scheme to reduce key derivation time, frequent root key updates, and

non-random key generation. The scheme applies a two-step Rabbit KDF structure with a pseudo-random number generator [3]. The randomness extractor is applied to take a series of non-uniform values of shared contexts c , and a root key K_a . Session keys generated form part of the shared contexts c as these keys are re-generated immediately after the root key has been updated. Moreover, in this phase, the value of c and K_a are generated as pseudorandom values. While the key expander uses another root key and the output from the randomness extractor as input, where a new different root key is the 128 bits output in this phase which is a pseudorandom sequence number close to a uniform distribution. The key management scheme was implemented as the primary core of the root key update mechanism in LoRaWAN due to its ability to lower computing weight for deriving root keys and zero crypto-analysis weaknesses that can be exploited with Rabbit Stream Cipher.

Choi and Kim [5] proposed an improved LEA block chain encryption scheme to optimize processing in resource-constrained IoT systems. In this scheme, instead of using masking by adding an arbitrary value to arithmetic operations for generating the output from the plain text, the arbitrary value is added directly to the plain text to change the value of the data format as a defence against side channels [6]. A 12-byte data format is received as an input, and 16-byte encryption is performed on the data input which consists of a 12-byte of the actual data and a 4-byte of the dummy data. In this case, a 12-byte is used to store the sensitive information and the 4-byte is randomly selected to mutually generate a sequence, where every information that is changed is stored in the 4-byte for decryption. Once the encryption function is applied, the actual data input is restored in a one-operation process by using the 4-byte dummy data to attain lesser decryption processing time as compared to the standard masking-LEA model.

Prasetyo et al. [27] suggested a blowfish symmetric encryption algorithm with minimized Feistel rounds in FPGA to achieve high throughput, improved security, average-to-high avalanche effect, and lesser encryption time. The model involves two processes to safeguard and efficiently encrypt the data. One is the key expansion where the function key is changed by using 18 entries of p-array and 4 of 256 substitution boxes while 4 Feistel rounds are used instead of 8 rounds. The other process is efficient data encryption in resource-limited FPGA, where 16 iterations per round are used in a Feistel network by minimizing the key bit size of the traditional blowfish from 128-bits to 64-bits, 256 bits to 192 bits, and 448 bits to 384 bits.

Ruotsalainen et al. [4] designed a revised LPWAN key manifestation mechanism to deal with the challenge posed by channel probing, large latency, and static spectrum conditions for LoRaWAN class A devices. To achieve this, the key manifestation protocol is organized into seven steps: channel probing where the end devices and the gateway participate in bidirectional communication, where the RSSI, packet counters, and SNR are recorded in uplink and downlink communications; measurement preselection, where a gateway ensures that the measurements collected are correctly selected and matched, which guarantees continuous spectrum probing between the gateway and the end device and for each uplink and downlink to reduce high packet collisions caused by congested ISM bands due to the used CSS modulation; precorrection is where a Discrete Cosine Transform (DCT) is used to correctly synchronize the measurements, a quantization where measurements of the total packet dropped are communicated between the end devices and the gateway for ensured synchronized quantized key bits; reconciliation is where BCH encoding as a suitable low-resource-constrained algorithm is used for correcting up to 23 out of 127 key bits that can be caused by imperfect measurements; privacy amplification is the final key generation phase and is privacy amplified to restrict the attackers' access to the information that can be leaked during the reconciliation phase.

Roselin et al. [28] proposed a security solution for 6LoWPAN WSN known as lightweight authentication protocol (LAUP) based on symmetric encryption without the pre-shared keys. The scheme employed four flights for authentication establishment and session keys sharing and establishment using existing information. For session requests, flight one communication is used for securing communication between the sensor node

and the edge router that transmits the payload contents to the edge router. The identity of the sensor node nonce value is validated by the XOR function on the message encrypted with a flight one key such that the encrypted identifier of the sensor node, the MAC one value, and the request message are transmitted to the edge router as first-flight data. For authentication, the initial authentication and second-level authentication are carried out by the edge router employing the AES-128-bit ECB algorithm for decrypting the received flight one data to validate the new data against the existing data from the flight one data. For second-level authentication, the edge router compares the sensor nodes' nonce value from flight two with the session key from flight two; if a match is found, further generating sessions will be initiated. Flight three key is generated by the XOR function between the sensor node and the edge router upon successful retrieval of the flight two values. The edge router terminates the process if the MAC three value calculated is different from the received MAC three value calculated using the hash function on the encrypted received values. Lastly, for key distribution, the edge router ensures that key distribution is successful for the wireless sensor nodes by communicating all the four-flight data where a session key encrypts recurring communication.

Naoui et al. [1] also proposed a new security model to improve the existing model(s) considered highly susceptible to two attacks. The three phases involved are as follows: (i) the system set-up where two session keys are computed by the trusted third party using asymmetric encryption and shared with one for the network server and one for an application server. These session keys ensure secured communication between the trusted third party and the servers. (ii) The join procedure process is where the end device transmits a JR message to the third party which is forwarded to the network server by the third party. Once in the network server, the JA message is then sent to the third party and is then forwarded to the end device for transmission. The third party will then generate and send two keys for generating their session keys for communication: NwKey for the network server and AppKey for the application server. Finally, (iii) the rekeying process takes place, where the generated session keys are updated provided that a new join procedure is initiated using the same steps. However, the AppKey is meant for a single join procedure; thus, it is updated using a One Time Password (OTP) generator to derive new pre-shared from the previously shared AppKey. This is to guard against replay attacks as this AppKey can be used for generating session keys.

Tsai et al. [14] suggested the TTP-Based High-Efficiency Multi-Key Exchange Protocol (THMEP) model enhances existing models in terms of user and message authentication and securing the data and key exchanges. The overall security objectives of THMEP are based on: (i) Reliability, which assures that the user, the data, and the system are to be protected against several attacks such as forgery, impersonation, replay, and known key attacks. Moreover, it guarantees full mutual authentication between the users and the trusted third party. (ii) Efficiency ensures a high-security level using ECC even at the same key sizes as the RSA algorithm as well as supporting parallel computation to shorten processing times. Thus, TTP's communication and computation costs and complexity are reduced by replicating some of ECC operations with XOR operation and binary addition; this also reduces the energy consumption, which makes it suitable for mobile devices. Finally, (iii) high throughput is ensured by having the capability to generate 40 session keys simultaneously, which allows having 40 channels for communication.

Gao et al. [29] suggested a secure packet transmission (SPT) scheme to strengthen LoRaWAN 1.1 security during joining request processes against attacks if the root key is compromised. Consequently, the JR packets are secured against eavesdropping attacks and replay attacks. SPT employ three approaches to redefine and secure the request to join packets. (i) A re-defined JR payload is used, where the old request is redefined to join packet characteristics to a new request to join packet using a new dynamic coding technique that ensures that the attacker cannot perform any correct coding even though the new request to join the packet is intercepted. (ii) The new OTP approach is used for effective and efficient encryption on the request to join messages. This secures the request

to join messages. (iii) The Adaptive Data Rate (ADR) algorithm is applied to prolong the battery life of the LoRa end devices. In this case, the operational complexities of the ADR are performed by the network server, keeping the LoRa end devices as simple as possible. Moreover, the asynchronous execution of ADR is performed between the end device and the network server, where the end device adjusts its SF for a guaranteed delivery ratio. If the SF is high, the ADR ensures that the energy consumption is kept at a minimum level.

Dönmez and Nigussie [30] performed an analysis to determine other possible attacks such as DoS, replay, and eavesdropping attacks and their countermeasures targeting the join procedure since the current LoRaWAN 1.1 model detects only one attack in backward compatibility. The process involved is as follows: (i) The security session consists of the end device and the network server that maintains the network session by maintaining device addresses, frame counters, and network session keys. Moreover, the application session is also maintained by the end device. (ii) The cryptographic process involving a 128-bit AES algorithm is used with two modes of operation: the ECB, and cypher-based message authentication code (CMAC) to provide authentication, confidentiality, and encryption. (iii) Keys security and derivation where the root key generates the three-session keys FNwkSIntKey, SNwkIntKey, and NwkSEncKey and the other two lifetime keys, JSIntKey and JSEncKey. The root key also ensures message integrity and confidentiality of join procedures. (iv). Counters and nonces are used to derive new network session keys and recommend limiting the periodicity of the increments to avoid any overflow in the lifetime of end devices.

Naoui et al. [18] suggested an enhanced key management model for LoRaWAN architecture. The model is influenced by proxy nodes by minimizing the computation of the constrained nodes. Moreover, the reputation system is implemented for selecting proxy nodes in several phases as follows: (i) Protocol initial where the certification authority (CA) generates the proxy nodes groups and two certification tables and trust tables. The public key of each proxy is shared with the relevant group members to allow every proxy to have the public keys of all other group members. The shared public keys secure the transmitted messages between group members to which the proxy nodes are based to create their trust tables. The trust tables are used by the members for communication with other members and the proxy nodes. (ii) A joining node where a JR is broadcasted to the group members when the gateway wishes to join the proxy node groups to discover the assigned CA. The receiving proxy node will forward the received message composed of the CA identifier and the public key. The CA verifies if the transmitting node possesses a trust value in the trust table, and if not, it will generate it with a value equal to 1. A trust value will then be encrypted with the private key of CA and with the public key of the node and transmitted to the receiving node. The node will be active upon decrypting the received message. (iii) A leaving node where if a node opts to leave, it sends a leaving message to the CA composed of the node identifier. The CA will then remove the node's information within its certification table and decrement the trust by 1 so that it can be updated. The CA will then send a response message to the node that the release process is successful as its certificate has been removed. (iv). Selection of a new CA, where the existing CA updates its trust table and detects a gateway with a better trust value. A new CA is then assumed and is expected to enforce security by updating its group members' certifications.

4.2. Attacks Addressed and Solution Approaches

This subsection presents some of the several solutions proposed in the studies considered in this paper to address the security attacks faced by LoRaWAN. Each of the proposed solutions is employed differently to prevent or detect different attacks based on the researchers' objectives. Table 4 presents a summary of the findings.

Table 4. Summary of Possible Security Attacks and Solutions.

Ref.	DoS Attack	Replay Attack	Known-Key Attack	Eavesdropping Attack	Side-Channel Attacks	Physical Attack	Other Attack(s)	Solutions
[2]	No	Yes	No	No	No	No	No	Dual key based activation system
[3]	No	Yes	Yes	Yes	No	No	No	SeLPC with time key K_{ct} and lookup D-Box
[26]	No	No	No	No	Yes	No	Crypto analysis	Rabbit Stream Cipher-Based KDF
[5]	No	No	No	No	Yes	No	No	Rabbit Stream Cipher-Based KDF with 16-byte and 4-byte dummy data
[27]	No	No	No	No	No	No	No	Blowfish symmetric encryption with minimized feistel rounds in FPGA
[4]	No	Yes	N/A	Yes	No	No	Key-guessing, brute-force, quantum computer	DCT, BCH encoding, True Random Number Generator
[28]	No	Yes	No	No	No	No	Impersonation, man-in-the-middle	Unique flight keys and the AES-128 ECB algorithm
[1]	No	Yes	No	No	No	No	No	One-time password generator for AppKey re-updates
[14]	No	Yes	Yes	Yes	No	No	Forgery, impersonation	Trusted Third party, and ECC with 2D operation binary adder, and logical XOR
[29]	No	Yes	No	Yes	No	No	No	Modified MIC format And DevNoce. OTP
[30]	Yes	Yes	No	Yes	No	No	ACK spoofing, bit flipping	AES 128-bit counter
[31]	No	No	No	No	No	No	Man-in-the-middle	AES 128-bit symmetric encryption and SSL

Kim and Song [2] attempted to eliminate the replay attacks in LoRaWAN by proposing a dual Key-Based activation scheme that implements automatic key generation and updates for LoRaWAN layer independence in generating keys. Tsai et al. [3] proposed SeLPC to deal with replay attacks. The proposed SeLPC uses a time key K_{ct} generated by the network server's time of time key K_{ct} found in them with an encryption key (AppSKey) and lookup D-Box used for updating procedures. This security feature is to differentiate the calculated replay message from the transmitted message. Moreover, to eliminate known-key attacks, the SeLPC uses the improved AES-128 with an encryption key (AppSKey) and lookup D-Box to encrypt the application layer's information, which is updated every k -days. This security feature restricts the attackers from using and deriving the old AppSKey due to not knowing the lookup D-Box table that is updated every k -days. Moreover, to deal with eavesdropping attacks, the SeLPC encrypts the AppSKey and lookup D-Box table sent by

the network using the time key K_{ct} and previously generated AppSKey. This security is then based on varying the time by K_{ct} that restricts the eavesdroppers to extract the lookup D-Box and AppSKey from the transmitted information.

Han and Wang's [26] KDF scheme minimizes key deviation time, frequent root key updates, and key ransom generation. It is made secure against crypto analysis attacks by employing a Rabbit Stream Cipher-Based KDF implemented as the primary core of updating the root key in LoRaWAN based on its ability to lower computing weight for deriving root keys. In [5], the Rabbit Stream Cipher-Based KDF security model is designed to prevent side-channel attacks and improve the standard masking LEA algorithm based on performing 16-byte encryption on 12-byte data input. The model employs the 16-byte for encrypting 12-byte actual data (sensitive information) and 4-byte dummy data (randomly selected to mutually generate a sequence for decryption). Once the encryption function is applied, the actual data input is restored in a one-operation process using the 4-byte dummy data. In Prasetyo et al. [27] a model involving two processes is implemented on FPGA to securely encrypt the data. One process facilitates the key expansion by changing the function key using 18 entries of p-array and 4 of 256 substitution boxes while 4 Feistel rounds are used instead of 8 rounds. The other process is for data encryption where 16 iterations per round are used in a Feistel network by minimizing the key bit size of the traditional blowfish from 128-bits to 64-bits, 256 bits to 192 bits, and 448 bits to 384 bits.

Furthermore, Ruotsalainen et al. [4] mitigated attacks on LoRaWAN based on the use of mechanisms such as DCT to correctly synchronize the measurements, a BCH encoding for key bits that might be due to imperfect corrections and the True Random Number Generator (TRNG) properties for quantized key materials to restrict the attacker's access to exploiting the keys.

In the same vein, in Roselin et al. [28], to ensure the physical security and identity of the sensor node, every communicating node that is within the communication range of the edge router is successfully registered to the edge router. In this case, the edge router should have prior knowledge about the LoWPAN network PAN ID and ensure that all the sensor nodes wishing to communicate are physically secured and connected to the network. To maintain the individual protection of each flight, a unique flight session key is generated and distributed using the common key derivation method. To generate a nonce for each flight, the message generation time for each flight is treated as the nonce; this ensures that unnecessary high memory usage and computational overheads are reduced for resource-constrained sensor nodes. The messages transmitted are protected within all four flights using MAC values for message integrity. All four flights individually and independently have secured unique value(s) for their operations. This offers protection against man-in-the-middle attacks across all four flights where the LAUP model ensures that messages generated with nonces are well encrypted with unique flight keys and the AES-128 ECB algorithm. A non-injective synchronization property is also maintained. Moreover, it also offers protection against impersonation attacks where the LAUP model ensures that the wireless sensor nodes' identity is protected by registering the nodes in the edge router.

The proposed model by Naoui et al. [1] was based on designing and developing an improved model with key management for enhancing security in LoRaWAN and eliminating two attack types due to poor and insecure cryptographic key managing schemes. The attacks include the DevNonce attack that re-uses the same nonce for every transmission, where the old requests are used for launching replay attacks and the AppNonce attack, where the end-devices do not store the AppNonces to validate the AppServers for subsequent transmission, in which a join message is exploited by an attacker and transmitted to the end-devices. These stored nonces are memory consuming for resource-constrained devices. The scheme ensures forward and backward secrecy, key independency, and low computation overhead are maintained in the network. Moreover, to ensure that the AppKey is secured, a one-time password generator is used to compute a new AppKey for each session to restrict the attackers from exploiting the key with replay attacks.

Similarly, the THMEP security model by Tsai et al. [14], as compared to the existing models, does not use CAs that issue digital signatures to its users, but rather deploys a trusted third party to enforce user and message authentication for the safe exchange of important information such as parameters in the network. The trusted third-party system's clock is used to derive a dynamic parameter for encrypting important keys exchanged for communication; this is to restrict eavesdroppers and replay attacks. However, most importantly, the proposed model deploys a 2D operation with a binary adder and logical XOR aimed at reducing the overall number of multiplication operations performed by ECC for important parameter encryption. On the same note, to deal with replay attacks, an SPT scheme by Gao et al. [29] was designed to change the MIC format and the DevNonce. DevNonce is used to store all the important information about the joining time for each end device. Again, an OTP is used for only one accessing and transmission process which guarantees that all the previous data cannot be re-used by the attackers to intercept current processes. Lastly, during OTAA, the SPT guarantees that though the root key may be leaked from the resting devices, the attackers cannot use the leaked root key to copy and intercept the transmitted requests.

The AES 128-bit counter was also suggested by Fonmez and Nigussie [30] to deal with eavesdropping and replay attacks by not re-using the DevNonce and joinNonce_last values to strengthen the security by making exploiting the replay attack insufficient. In addition, to deal with fake sessions on the network server, the joining server does not re-use the joinNonce value where the DevNonce_last value in the improved replay protection protocol is not re-used for configuration. For bit flipping and ACK spoofing attacks, the new message integrity check calculations in the proposed v1.1 are employed and use the frame counters for frame acknowledging. In a similar study, Naoui et al. [31] designed security for LoRaWAN to counter man-in-the-middle attacks. The schemes employed an AES 128-bit symmetric encryption to secure communication between the end devices and the gateways. An SSL protocol is used for authenticity and security in the communication between the gateway and network server. Moreover, for a group of proxy nodes communicating using public keys, the exchanged message is only decrypted by the relevant CA with the relevant private key of the proxy node.

5. Discussions

In this paper, several research works on security models in LPWAN, IoT, and LoRaWAN have been surveyed and presented. The paper brings together a comprehensive analysis of existing key security models, the possible challenges of key security management and their different attacks. For each study considered, we performed an analysis in terms of the techniques for key security models, their correctness to verification and validation, and the performance analysis and evaluations based on the security efficiency and effectiveness. Moreover, possible research opportunities were identified and discussed as well. The summary of the findings is presented in Tables 2–4.

As shown in Tables 2 and 3, several security metrics were used to analyse and assess the security performance and effectiveness of the proposed key security models. We found the urgent need to address the security issues faced in LoRaWAN key security models. Existing less complex and lightweight security models already designed are still in their infancy, hence there is the need to enhance these models or propose novel key security models. Several studies considered focused on improving the existing LoRaWAN key security models considering the LPWAN nature, whereas some researchers improved the LoRaWAN AES-128-bit algorithm. For instance, Kim and Song [1] modified the AES-128 algorithm by simplifying the key and D-Box dynamic update for the dynamic key process. In the work, by Choi and Kim [7], the AES-128 algorithm was improved by implementing AES-128-bit Electron Cipher Block using XOR with Hash function, while others such as Gao et al. [8] and Prasetyo et al. [9] focused on alleviating complex operations on the network servers by implementing a trusted third party to securely and efficiently manage and distribute both the AppKey and session keys, namely AppSKey and NwkSKey.

Moreover, Choi and Kim [7] focused on improving key distribution. In addition, for each proposed solution, experiments were conducted to analyse and assess its performance and effectiveness against several common attacks while preserving the nature of the resource-constrained LPWAN devices.

Furthermore, we also found that several attacks affect the LoRaWAN key security model. Among these attacks, replay attacks have been identified as the commonest attack in the network that compromises the LoRaWAN security. These attacks mainly exploit the AppKey as the main key in the network responsible for generating two session keys, namely, AppSKey used for payload encryption and decryption between the end-device and the application server, and the NwkSKey used for validating message integrity. In some of the proposed security models, the severity of the replay attack on the AppKey is discussed if the AppKey is not updated for every session as this leads to a replay attack intercepting the AppKey to generate the old session keys to discover previously communicated messages [1,3,21,29]. LoRaWAN as an LPWAN technology is prone to security attacks due to the nature of connecting end devices and the base stations in a star topology. As argued by other researchers Naoui et al. [1], and Kim and Song [2] as implemented in some of the existing works, the AppKey should be regenerated and re-updated for every session. This is important to enforce a defence mechanism against any attacks where the previous communication cannot be discovered due to session keys being regularly updated using a new AppKey for every session. However, updating these keys should not be extremely regular as this could impact the energy efficiency of resource-constrained devices. Thus, the resource-constrained nature of the devices should be considered when designing these key models in LPWAN as heavy and complex operations affect critical resources. Moreover, asymmetric encryption is not commonly implemented in LPWAN due to its heavy and complex operations that are less compatible with the nature of LPWAN. Most researchers implement the key security models based on symmetric encryption as it is not complex and heavy on operations [28,31].

6. Possible Research Opportunities

As the LPWAN paradigm is gaining popularity, several studies have been proposed to address several research gaps highlighted in the studies considered in this paper for efficient security models. This section discusses some of the possible research opportunities.

- Kim and Song [2] recommend a dual server mechanism to ease the complexities in layers. One server shall facilitate transmission processes and the other server for facilitate reception processes. Moreover, we recommend an autonomous key generation and update mechanism implemented on the key server; this is to overcome key replay attacks if the old keys are breached by the attacker.
- Similarly, the proposed scheme by Tsai et al. [3] was only evaluated using the formal method. However, the use of security verifying tools such as Scyther and ProVerif should also be considered to check for other security vulnerabilities not proven by mathematical proofs.
- In the same vein, Han and Wang's [26] proposed scheme should further be investigated by using a security verifying tool to analyse the proposed model for other attacks not analysed in this work that are likely to severely affect the proposed model.
- In Choi et al. [5], we recommend further experiments using security verifying tools to be carried out to analyse more attacks that are likely to compromise the network.
- In the scheme proposed in Prasetyo et al. [27], we suggested future work that considers dynamic and autonomous key updates to avoid replay attacks and security implementation at all entities as well as an entity that is scalable to memory to avoid overheads in a resource-limited FPGA due to complex operations.
- In Ruotsalainen et al. [4], the authors suggested performing a system-level analysis and evaluation for large coverage LPWAN with less energy consumption.

- Similarly, Roselin et al. [28] have suggested minimizing strong interferences when establishing communication in the network between the router and the wireless end devices by synchronization amongst these wireless end devices in their study.
- Naoui et al. [1] recommend an energy harvesting model to sustain the lifespan of LoRaWAN end devices to accommodate repetitive processes of accepting and re-computing session keys.
- Likewise, in the work by Tsai et al. [14], we recommend the use of a security analyser tool on their proposed model to verify other attacks not analysed. This is to identify other attacks existent in the LPWAN invisible to the human eye.
- The proposed SPT model by Gao et al. [29] lacks in-depth evaluations and analyses of the attacks. Thus, we recommend that the work can be extended by taking advantage of the flexibility of tools such as Scyther to effectively analyse the proposed model against all other possible LoRaWAN attacks.
- The security verifying tool is also recommended for the work by Donmez et al. [30]. Accordingly, Naoui et al. [31] have suggested the use of a Markov chain model in evaluating the trust values of the proxy nodes following their behavioural history. The chain Markov will be used to change each proxy node's trust state based on the joining, leaving, and packet relaying phases.

7. Conclusions

This paper presented a comprehensive analysis of existing key security models in LPWAN using LoRaWAN as a case study. The study focused on the existing challenges, key security model attacks and the proposed solution approaches implemented for LoRaWAN key security. This paper performed an analysis on several security algorithms, key security models, their correctness, verification, and validations, as well as performance. We found that LoRaWAN is a promising key security protocol for implementation in LPWAN and is affected by its resource-constrained nature. Moreover, the analysis reveals that symmetric encryption dominates the modelling of key security in LoRaWAN based on the AES-128 bits scheme while asymmetric encryption was considered inept due to the involved complex operations and the LPWAN resource-constrained setting. Furthermore, the area is still in its infancy stage and only a little research is available. Therefore, more research attention should be focused on this aspect. When designing reliable, flexible, and efficient key security models in the LPWAN ecosystems, an encryption system that is lightweight such as symmetric encryption should be utilized. This is because as the AppKey is generated and distributed to generate AppSKey and NwksKey, it is important to design a secured key model to secure the AppKey and update it regularly to avoid attacks such as replay attacks. In addition, there is a need to design and develop a LoRaWAN security model that is compatible with LPWAN. Network security tools such as Scyther, ProVerif, AVISPA, etc. should be used to analyse and validate any proposed models against several attacks, especially if such models are to be used in real-life applications.

For our future work, the intention is to design and implement a less complex and lightweight key security model in LoRaWAN with a flexible and efficient key distribution trusted key server that is compatible with LPWAN's nature. This is positioned at improving some of the existing model(s) discussed in this paper as the goal of this paper was to identify and bring together several existing challenges that affect traditional LoRaWAN security models. Furthermore, we recommend that other researchers on LoRaWAN security consider aspects such as security, efficiency, and integrated capability as metrics to analyse their proposed models for an improved analysis; this yields an in-depth analysis of their proposed works based on those aspects rather than analysing the assumption that the proposed existing models satisfy security, efficiency, and integrated capability as metrics.

Author Contributions: Conceptualization, K.N. and B.I.; methodology, B.I.; investigation, K.N.; writing—original draft preparation, K.N.; writing—review and editing, B.I.; supervision, B.I.; project administration, N.G.; funding acquisition, A.M.A.-M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received external funding from the Council for Scientific and Industrial Research (CSIR) via the Smart Networks collaboration initiative and IoT-Factory Program (funded by the Department of Science and Innovation (DSI), South Africa. This research received external funding from the Council for Scientific and Industrial Research (CSIR) via the Smart Networks collaboration initiative and IoT-Factory Program (funded by the Department of Science and Innovation (DSI), South Africa.

Acknowledgments: This was supported by FNAS, UDSC, and the Department of Computer Science at the North-West University, Mafikeng campus as well as the Council for Scientific and Industrial Research (CSIR) via the Smart Networks collaboration initiative and IoT-Factory Program (funded by the Department of Science and Innovation (DSI), South Africa).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Naoui, S.; Elhdhili, M.E.; Saidane, L.A. Trusted third party based key management for enhancing LoRaWAN security. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; pp. 1306–1313.
2. Kim, J.; Song, J. A Dual Key-Based Activation Scheme for Secure LoRaWAN. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 6590713. [CrossRef]
3. Tsai, K.-L.; Huang, Y.-L.; Leu, F.-Y.; You, I.; Huang, Y.-L.; Tsai, C.-H. AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments. *IEEE Access* **2018**, *6*, 45325–45334. [CrossRef]
4. Ruotsalainen, H.; Zhang, J.; Grebeniuk, S. Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks. *IEEE Internet Things J.* **2019**, *7*, 1745–1755. [CrossRef]
5. Choi, J.; Kim, Y. An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system. In Proceedings of the 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Jeju, Korea, 13–16 December 2016; pp. 1–4.
6. Froiz-Míguez, I.; Fraga-Lamas, P.; Fernández-Caramés, T.M. Design, Implementation and Validation of a Bluetooth 5 Real-Time Monitoring System for Large Indoor Environments. *Eng. Proc.* **2021**, *7*, 18. [CrossRef]
7. Bahashwan, A.A.; Anbar, M.; Abdullah, N.; Al-Hadhrami, T.; Hanshi, S.M. Review on Common IoT Communication Technologies for Both Long-Range Network (LPWAN) and Short-Range Network. In *Advances on Smart and Soft Computing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 341–353.
8. Bali, M.S.; Gupta, K.; Bali, K.K.; Singh, P.K. Towards energy efficient NB-IoT: A survey on evaluating its suitability for smart applications. *Mater. Today Proc.* **2022**, *49*, 3227–3234. [CrossRef]
9. Ferreira, C.M.S.; Oliveira, R.A.R.; Silva, J.S. Low-energy smart cities network with LoRa and Bluetooth. In Proceedings of the 2019 7th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Newark, CA, USA, 4–9 April 2019; pp. 24–29.
10. Islam, N.; Ray, B.; Pasandideh, F. IoT Based Smart Farming: Are the LPWAN Technologies Suitable for Remote Communication? In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; pp. 270–276.
11. Qi, X.; Yu, K.; Sato, T.; Shibata, K.; Brigham, E.; Tokutake, T.; Eguchi, R.; Maruyama, Y.; Wen, Z.; Tamesue, K.; et al. Ledger-based Points Transfer System in LPWAN: From Disaster Management Aspect. In Proceedings of the 2021 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Hangzhou, China, 3–5 December 2021; pp. 150–155.
12. Rajab, H.; Cinkler, T.; Bouguera, T. Evaluation of Energy Consumption of LPWAN Technologies. 2021. Available online: <https://www.researchsquare.com/article/rs-343897/latest.pdf> (accessed on 11 June 2022).
13. Ntshabele, K.; Isong, B.; Abu-Mahfouz, A.M. CR-LPWAN: Issues, solutions and research directions. In Proceedings of the 2021 IEEE World AI IoT Congress (AIIoT), Virtual Conference, Seattle, WA, USA, 10–13 May 2021; pp. 0504–0511.
14. Tsai, K.-L.; Huang, Y.-L.; Leu, F.-Y.; You, I. TTP Based High-Efficient Multi-Key Exchange Protocol. *IEEE Access* **2016**, *4*, 6261–6271. [CrossRef]
15. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2019**, *5*, 1–7. [CrossRef]
16. Lavric, A.; Popa, V. Internet of things and LoRa™ low-power wide-area networks: A survey. In Proceedings of the 2017 IEEE International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 13–14 July 2017; pp. 1–5.
17. Wixted, A.J.; Kinnaird, P.; Larijani, H.; Tait, A.; Ahmadinia, A.; Strachan, N. Evaluation of LoRa and LoRaWAN for Wireless Sensor Networks. In Proceedings of the 2016 IEEE SENSORS, Orlando, FL, USA, 30 October–3 November 2016; pp. 1–3.
18. Sanchez-Iborra, R.; Sánchez-Gómez, J.; Pérez, S.; Fernández, P.J.; Santa, J.; Hernández-Ramos, J.L.; Skarmeta, A.F. Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach. *Sensors* **2018**, *18*, 1833. [CrossRef] [PubMed]

19. Eldefrawy, M.; Butun, I.; Pereira, N.; Gidlund, M. Formal security analysis of LoRaWAN. *Comput. Netw.* **2019**, *148*, 328–339. [[CrossRef](#)]
20. Butun, I.; Pereira, N.; Gidlund, M. Security Risk Analysis of LoRaWAN and Future Directions. *Futur. Internet* **2018**, *11*, 3. [[CrossRef](#)]
21. Tomasin, S.; Zulian, S.; Vangelista, L. Security analysis of lorawan join procedure for internet of things networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
22. Avoine, G.; Ferreira, L. Rescuing LoRaWAN 1.0. In Proceedings of the International Conference on Financial Cryptography and Data Security, Nieuwpoort, Curaçao, 26 February 26–2 March 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 253–271.
23. Butun, I.; Pereira, N.; Gidlund, M. Analysis of LoRaWAN v1. 1 security. In Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, Los Angeles, CA, USA, 25 June 2018; pp. 1–6.
24. Noura, H.; Hatoum, T.; Salman, O.; Yaacoub, J.-P.; Chehab, A. LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet Things* **2020**, *12*, 100303. [[CrossRef](#)]
25. Yang, X. LoRaWAN: Vulnerability Analysis and Practical Exploitation. Master’s Thesis, Delft University of Technology, Delft, The Netherlands, 2017.
26. Han, J.; Wang, J. An Enhanced Key Management Scheme for LoRaWAN. *Cryptography* **2018**, *2*, 34. [[CrossRef](#)]
27. Prasetyo, K.N.; Purwanto, Y.; Darlis, D. An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA. In Proceedings of the 2014 2nd International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 28–30 May 2014; pp. 75–79.
28. Roselin, A.G.; Nanda, P.; Nepal, S. Lightweight Authentication Protocol (LAUP) for 6LoWPAN Wireless Sensor Networks. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICSS, Sydney, Australia, 1–4 August 2017; pp. 371–378.
29. Gao, S.-Y.; Li, X.-H.; Ma, M.-D. A Malicious Behavior Awareness and Defense Countermeasure Based on LoRaWAN Protocol. *Sensors* **2019**, *19*, 5122. [[CrossRef](#)]
30. Dönmez, T.C.; Nigussie, E. Security of LoRaWAN v1.1 in Backward Compatibility Scenarios. *Procedia Comput. Sci.* **2018**, *134*, 51–58. [[CrossRef](#)]
31. Naoui, S.; Elhdhili, M.E.; Saidane, L.A. Enhancing the security of the IoT LoraWAN architecture. In Proceedings of the 2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN), Paris, France, 22–25 November 2016; pp. 1–7.