electronics

MDPI

Review

Security in Low Powered Wide Area Networks: Opportunities for Software Defined Network-Supported Solutions

Gaurav Pathak [1,*], Jairo Gutierrez [1] and Saeed Ur Rehman [2]

[1] School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland 1142, New Zealand; jairo.gutierrez@aut.ac.nz

[2] Cybersecurity and Networking College of Science and Engineering, Flinders University, Tonsley, Adelaide 5001, Australia; saeed.rehman@flinders.edu.au

[*] Correspondence: gaurav.pathak@aut.ac.nz

Received: 26 June 2020; Accepted: 17 July 2020; Published: 25 July 2020

check for updates

Abstract: The Internet of things (IoT) has revolutionized the use of connectivity and has given birth to new transmission technologies to satisfy the requirements of diverse IoT applications. Low powered wide area networks (LPWAN) is one of those transmission technologies, and is becoming exceptionally useful for IoT applications. The nodes use energy-efficient mechanisms for long-range data transmission (10–20 km), lasting in hostile environments for years and making them suitable for IoT applications such as environmental monitoring, automated billing systems, smart homes, smart offices, and patient monitoring. However, LPWAN devices have minimal resources, which makes it challenging to provide promising security to devices and data in the network. In this paper, we discuss the security mechanisms used in current LPWAN technologies along with their vulnerabilities and possible attacks on them. A detailed literature review is conducted on existing solutions on the security of constrained IoT networks similar to LPWAN using different networking frameworks. The reviewed literature is then compared based on various network security measures addressed by them. In addition, the emergence of software defined network (SDN) architecture for security in IoT is explained based on literature. Finally, the applicability of SDN in LPWAN security, its opportunities, and challenges in implementation are discussed.

Keywords: LPWAN; network security; SDN security; IoT security; software defined networking; Internet of things

1. Introduction

The smartification of our everyday life has increased the use of Internet of things (IoT) technologies in almost every area. IoT devices provide sensing and transmitting capabilities via the Internet, and can communicate seamlessly irrespective of the underlying technologies [1]. IoT devices are embedded in fridges, microwaves, vehicles, medical devices, and almost every object in our daily use. Thus, providing comfort and ease in our daily life.

New IoT applications are launched daily. The number of sensor devices in IoT networks are expected to grow exponentially and have a revenue of approximately $2 trillion [2,3]. Most sensor devices in IoT networks are battery powered and are expected to last for years. Hence, energy efficiency is a key consideration in the design of IoT devices and associated transmission technologies.

Low powered wide area network (LPWAN) transmission technologies are commonly used in IoT application for long-range communication. They are capable of transferring data up to 10–20 km with minimal energy consumption, enabling the node lifetime of 8 to 10 years while providing data rates of

100 bps–200 kbps [4]. These technologies are suitable for applications with low data rate requirements where the nodes with limited energy are deployed in challenging terrains, and it is burdensome to re-energize the nodes. LPWAN uses a star topology where the low-end sensing devices transmit data to a gateway, from where it is forwarded to application servers.

While LPWAN technologies are getting popular for IoT applications, the security of LPWAN networks remains a significant challenge as the end devices in the network are limited in resources (memory, computation, battery), therefore, deploying state of the art computation-intensive cryptographic algorithm is not possible [5]. LPWAN networks require a mechanism to offload the computation of demanding tasks to a capable unit in the network. In order to fill this gap, software defined networks (SDNs) have been emerging as a solution in providing adequate security to constrained network environments such as LPWAN [6–12]. SDN decouples the control plane from network devices and provides programmability in network control mechanisms. The controller acts as a central entity and can communicate remotely to network devices while performing computations for end nodes using OpenFlow [13] protocol.

In this paper, a detailed review of security mechanisms in LPWAN communication technologies is discussed. The paper discusses the security vulnerabilities and possible attacks and their impacts on various LPWAN technologies. Besides, an extensive literature review is performed for security in IoT communication technologies to identify challenges and solutions for security in the IoT environment. The reviewed literature is compared based on various security parameters addressed, such as authentication, confidentiality, key exchange, and attack detection. The literature review also identifies the possible shortcomings of the solutions discussed in the literature. Most of the literature surveys [1,5,8,14–16] focus on partial solutions based on either traditional or software defined networking (SDN) frameworks. In this paper, we have also discussed the applicability of the SDN framework in IoT security by examining available solutions for different security parameters. How SDN can provide flexible and robust security solutions in IoT, advantages, and challenges in SDN security solutions are also discussed.

The remainder of the paper is organized as follows: Section 2 overviews the security mechanisms of current LPWAN technologies. In contrast, the security vulnerabilities and possible attacks on LPWAN networks are discussed in Section 3. Further, Section 4 discusses various solutions proposed in the direction of strengthening security mechanisms in constrained networks such as LPWAN and those solutions are compared based on the way they address security threats. Section 5 discusses the applicability of SDN in LPWAN security, its challenges, opportunities, and advantages over traditional networking frameworks. Finally, Section 6 concludes the paper.

2. Security in Current Low Powered Wide Area Network (LPWAN) Technologies

As mentioned in the previous section, LPWAN is becoming exceptionally convenient with IoT applications. As the use cases of LPWAN rise, it becomes imperative to assess the security mechanisms of these technologies. Various transmission technologies come under the spectrum of LPWAN, and different LPWAN technologies use different frequencies and transmission mechanisms for communication. Hence, they all have their own set of features and security mechanisms for data authenticity, confidentiality, and integrity. The following subsections discuss the security mechanisms of various LPWAN communication technologies in detail.

2.1. Weightless

Weightless is backed by a UK company, Neul, recently acquired by Huawei. The technology is described in a set of three standards which were developed by a non-profit standard organization “Weightless SIG” [17]. The three standards are Weightless-N, Weightless-W, and Weightless-P. Weightless-N uses ultra-narrow band (UNB) on a sub-GHz spectrum and has a range of several kilometers. Weightless-W operates in television whitespace spectrum for communication. Weightless-P uses a narrow band with TDMA and FDMA. In addition, it uses energy-efficient modulations with an adaptive data rate.

Weightless-P [17,18] has considered data security and integrity by providing AES 128/256 for encryption and node authentication. However, the nodes use the same shared key throughout their lifetime. No session key mechanism is provided in the network; a secret key leak because of a physical attack in the network can lead to a breach of all the data transmitted by a node (no forward secrecy) [19].

2.2. Sigfox

Sigfox is a French network operator established in 2009 and targets wireless connectivity of low powered devices. Sigfox uses a proprietary ultra-narrow band (UNB) with limited uplink connection [20]. Sigfox can achieve maximum data rates of 100 bps with a maximum payload of 12 bytes and up to a range of 10 km. It uses a stored symmetric key to authenticate the node and uses sequence numbers to avoid replay attacks. These sequence number counters are auto-incremented with every message and reset in one month with 140 messages/day. The integrity of sequence number is confirmed by using a message authentication code (MAC) which is sent with the data packet. Sigfox does not provide message encryption by default. However, depending on the application, customers can either use their end to end encryption mechanism or they can use the end to end encryption solution provided by Sigfox. Figure 1 shows the checks performed in Sigfox during message transmission.

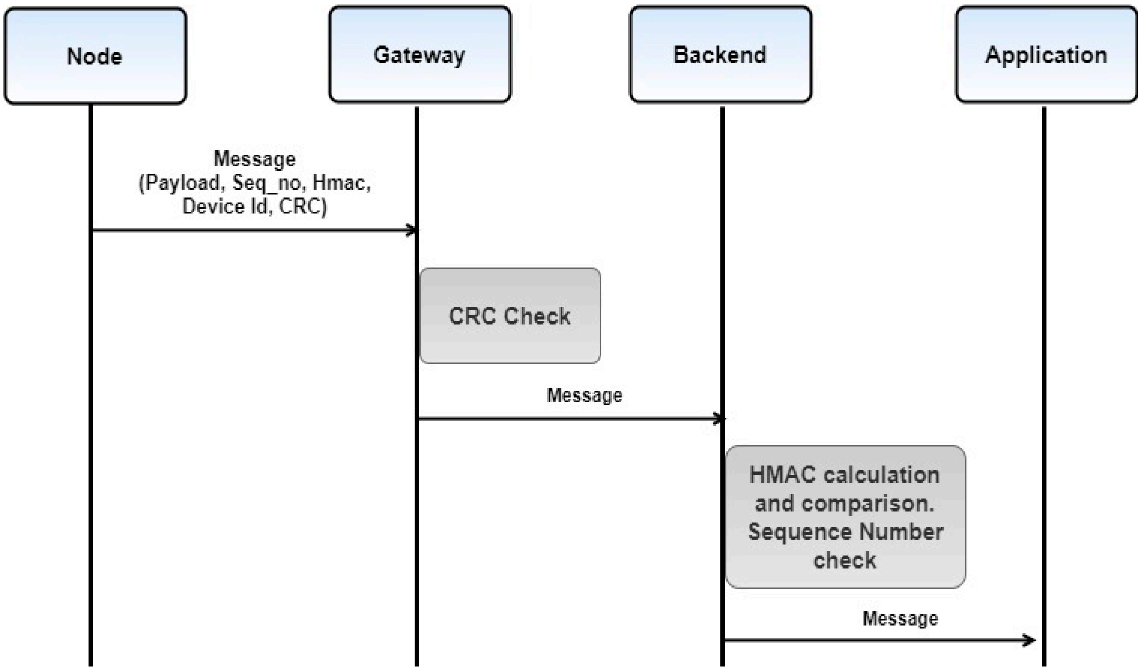

Figure 1. Sigfox message transmission process.

2.3. Narrowband-IoT (NB-IoT)

NB-IoT is standardized by the third-generation partnership project (3GPP). It is a cellular network technology that uses Long Term Evolution (LTE) spectrum for data transmission. The design goal of this technology was to include low-cost devices, long-distance coverage, long battery life, and a huge scale [21]. NB-IoT inherits the security mechanisms for confidentiality and authentication from LTE networks. The perception layers are prone to different kinds of attacks on confidentiality, integrity, and authenticity of data [22]. LTE provides symmetric encryption and signing mechanisms to prevent a data breach, and uses SIM cards to authenticate and identify devices in the network [23].

2.4. DASH7 Alliance Protocol

It is a wireless protocol designed for low power application such as sensors and active RFID networks and operates on sub-GHz ISM band [24]. DASH7 has three device classes: Endpoint Class, Sub controller Class, and Gateway Class. DASH7 uses AES symmetric key cryptography for confidentiality and node authentications in the network. The secret key is stored in the node file system prior to the deployment and remains the same throughout node's lifetime similar to Sigfox. Hence, it is prone to the same attacks as Sigfox.

2.5. LoRaWAN

LoRaWAN [15] is a MAC layer protocol created by the LoRa Alliance for battery-operated wireless devices. It operates on LoRa for physical layer characteristics and aims to provide support for mobility and secure communication [25]. LoRaWAN provides both authentication and data security. Keeping node resources under consideration, symmetric key operations are used for node authentication and data confidentiality. In LoRaWAN, when the node tries to join the network for the first time, a join procedure is initiated. There are two types of activation procedures in LoRaWAN:

1. Over-the-air activation (OTAA): In this method, every node uses its 128-bit Appkey (given to the node at deployment time). The Appkey is used to calculate a four-byte message integrity check (MIC) code to sign the join request [26]. Figure 2 shows the procedure for OTA activation in LoRaWAN. Mac = aes128_cmac (AppKey, MHDR | AppEUI | DevEUI | DevNonce) MIC = mac[0..3] AppEUI is unique to the owner, and DevUI is unique to the device; they act as identifiers for the application and the end device, respectively. DevNonce is a random number sent by the device to avoid the replay of the packet. In the first step, the source node sends a join request to the network server. To minimize computation source node does not encrypt the join request. Upon receiving the join request, the network server checks the MIC for message integrity, and it checks the DevNonce if it has already been used previously. Further, the server responds with join accept which is encrypted with AppKey by using the decrypting module of AES, which can be decrypted using the encrypt module of AES. Using only a decrypt module in the device makes it possible to load only one module in the end node. The MIC for join accept is generated with appkey [26]. Mac = aes128_cmac(AppKey, MHDR | AppNonce | NetID | DevAddr | RFU | RxDelay | CFList) MIC = mac[0..3] AppNonce is a random number generated by the server to produce AppSKey and NwkSKey, i.e., application session key and network session key, respectively [26]. NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16) AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16) When the end node gets the join request from the server, it calculates the session keys with the above-explained procedure. Figure 2 shows the OTAA procedure of LoRaWAN and its message sequence.
2. Activation by personalization (ABP): In ABP, the nodes are deployed with secret keys, and they can directly start transmitting data without any registration procedure. This process saves time and energy; however, it is considered to be less secure as the same key is used for the lifetime of the node [27].

Once the nodes join the network by either of the two procedures, the upcoming messages are encrypted, and MIC is calculated using the combination of network and application key, as shown in Figure 3.

LPWAN communication is one of the most effective communication technologies for long-range transmission. As discussed earlier, there are different technologies from different vendors available in the market which are capable of providing effective long-range communications. As all the LPWAN communication technologies are provided by different vendors, each one has different security measures available for their devices and users. Table 1 shows a summary of the security mechanisms used by various LPWAN technologies.

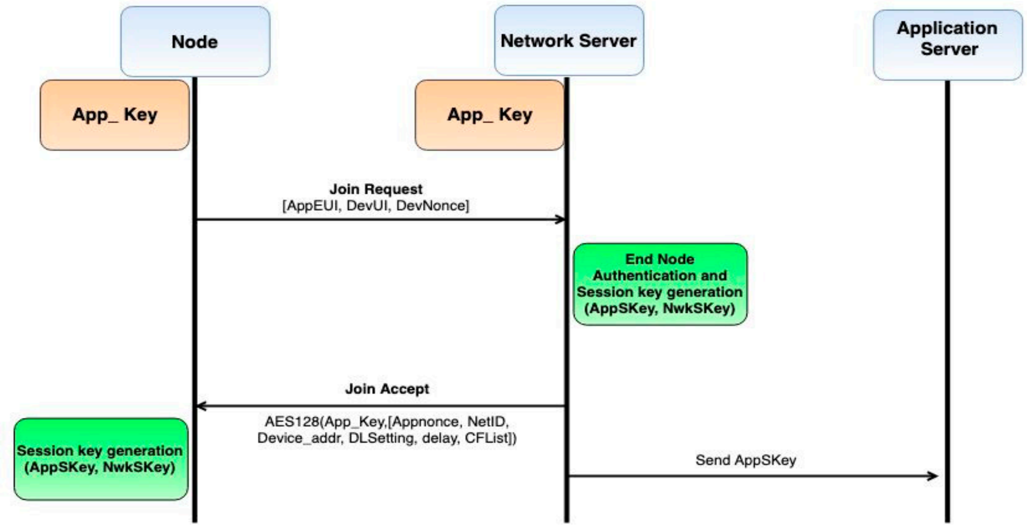
Node
Network Server
Application Server
App_ Key
App_ Key
Join Request
[AppEUI, DevUI, DevNonce]
End Node Authentication and Session key generation (AppSKey, NwkSKey)
Join Accept
AES128(App_Key,[Appnonce, NetID, Device_addr, DLSetting, delay, CFList])
Session key generation (AppSKey, NwkSKey)
Send AppSKey

Figure 2. Over-the-air activation (OTAA) join procedure LoRaWAN.

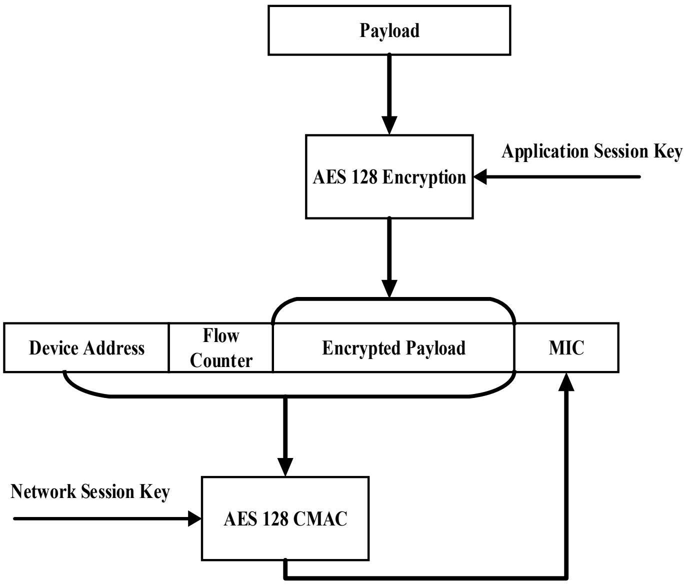

Figure 3. Encryption and message signing in LoRaWAN.

Table 1. Security features and vulnerabilities in low powered wide area network (LPWAN) technologies.

LPWAN Technology	Authentication	Confidentiality	Replay attack Countermeasure	Session Key Mechanism	Vulnerabilities/Possible Attacks
NB-IoT	AES-128 bit MAC	LTE encryption mechanisms	-	Not Available	NB-IoT Sim card misuse in 4G [22]. Jamming, hidden channel communication [28].
LoRaWAN	AES-128 bit MAC	AES-128 bit encryption	Frame Counter	Yes. Session keys can be generated over the air	Eavesdropping, replay attacks [29], wormhole attack, device key compromise [30], packet forging [22]. Jamming, hidden channel communication [28].
Sigfox	AES-128 bit MAC	By default None (Optional: AES-128 bit encryption)	Sequence Number used	Not Available	Replay attacks [22], security mechanisms left optional for users [31].
Weightless	AES-128 bit MAC	AES-128/256 bit encryption	Data Frame counter	Not Available	Jamming, eavesdropping, sniffing attack [32,33]
DASH7	AES-128 bit MAC	AES-128 with counter mode	Not Available	Not Available	Eavesdropping, sniffing attacks, jamming attack [33]

3. Security Vulnerabilities in LPWAN

Sigfox is one of the most popular transmission technologies in LPWAN, in [34] a security assessment of Sigfox is done, and vulnerabilities are discussed. It is highlighted that it lacks end to end security from sensors to users which can cause hindrance in the use of Sigfox in applications with sensitive data. A detailed security analysis of LPWAN technologies is performed in [35]. LoRa, Sigfox, NB-IoT, and DASH7 are discussed and compared considering their applications in IoT. Possibilities of a range of attacks are explained on LPWAN transmission technologies using the example of LoRaWAN. In [36], vulnerabilities of LoRaWAN procedures against DDoS attacks are explained.

It is also argued that LoRa devices are prone to physical attacks which can be used to get the secret keys from the devices, making the device untrustworthy [37]. In addition, in the encryption process, the transceivers of end devices are used, and the microcontroller does not know the keys used in the process, this makes it possible to send fake data from the devices using Universal Asynchronous Receiver/Transmitter (UART) pins of the transceivers [38]. LoRaWAN provides a prevention mechanism against replay attacks of join requests, but there is no mechanism for the prevention for a replay to join accept messages [38]. A replay of a join accept message can cause ambiguity in the network as there is no way for end nodes to find out the legitimate sender. Using fake join accept messages, an attacker can redirect the traffic towards a fake gateway, resulting in a blackhole attack on the network. Table 1 provides an overview of the existing vulnerabilities and possible attacks on a few existing LPWAN technologies along with the existing security mechanisms.

The author in [27] has explained attacks and their impact on both LoRaWAN activation techniques. According to the author, the attack tree shown in Figure 4 explains the possible attacks on LoRaWAN. LoRaWAN's ABP activation has been considered flawed due to the usage of static keys [39]. In ABP activation the keys remain the same even if the device is reset, as unlike OTAA, ABP does not have any join procedure for session key generation. There is also a probability of replay attack on LoRaWAN network. If the attacker captures the packets before the counter resets, moreover, it starts transmitting the captured packets after the sequence number counter resets again. The network server will not be able to identify the replay packets as it is signed by a valid key and has a valid counter. In [27], it has been shown with an experiment that a replay attack is possible in LoRaWAN if the attacker gets the highest counter value of the node. A detailed analysis of possible attacks and their impacts on the communication layer is discussed in [28,33,40] and summarized in Table 2.

Constrained IoT networks such as LPWAN are susceptible to various other attacks as discussed by authors in [41–47]. Figure 4 shows the possible attacks on IoT and LPWAN networks with constrained node environment and studies conducted by various researchers.

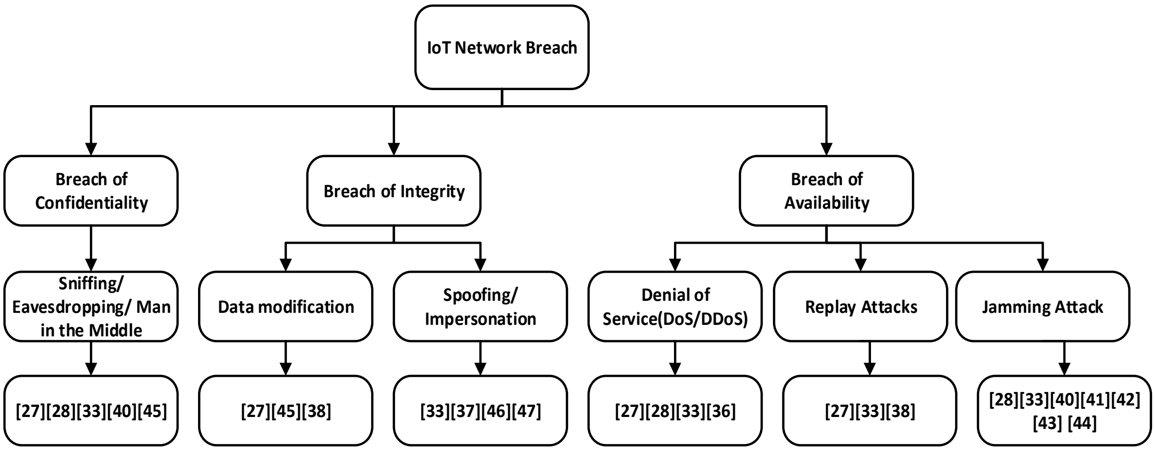

Figure 4. Attack tree for LPWAN and Internet of things (IoT) networks.

Table 2. Possible attacks and impacts on LPWAN communication layer [28,33,40].

Communication Layer attack	Impact on Network	Possibility
Jamming attack	Very High	High
Sinkhole attack	High	Medium
Wormhole attack	High	Medium
Hello Flooding attack	Moderate	Medium
Man in the Middle attack (MITM)	High	High
Sybil attack	High	Medium
Duty Cycle Manipulation	High	-

4. Literature Analysis

4.1. Security with Traditional Networking Architecture

Security in constrained IoT networks has been a challenging task for researchers, and a considerable amount of work is being conducted for security provision to constrained IoT networks. The literature covers multiple security aspects such as the authenticity of data and the sender, integrity, and confidentiality of the data. In this section, we discuss the different approaches and frameworks used by researchers to address various security measures in constrained networks.

In [48], Datagram Transport Layer Security (DTLS) with 6LowPAN, compression for the constrained devices are taken into consideration to reduce the header size of DTLS to fit in 802.15.4's maximum transmission unit (MTU). The compressed DTLS is linked with 6LowPAN's standard mechanism for security. This scheme gives the ability to implement a complicated security mechanism in constrained nodes, as by compressing, we can reduce the size of the header information. The compression of the data will reduce bandwidth consumption. However, the compression is still to be performed by the end nodes. Swapped Huffman tree coding is used in [49] to compress and encode (encrypt) the data with a secret key. This technique is very lightweight but it may not be very resilient against sophisticated attacks on the data, as the encoding patterns can be analyzed and plain text can be deduced by collecting enough data.

In [50], a load relieving scheme for the nodes is proposed, where each node can share the processing burden for encryption with a set of assisting nodes. This scheme can enable the nodes to overcome the problem of limited resources by combining the resources of multiple nodes. However, this scheme can lead to complications with maintaining the integrity of the data that is being shared among the nodes. It can also lead to an increase in the duty-cycles of the nodes in the network, which will lead to high power consumption. In a similar approach, Naoui, S. [51] uses a proxy-based encryption scheme, where the nodes distribute the processing overhead of encryption with the proxy nodes. The nodes select trusted proxy nodes and distribute their encryption load between them to save energy. It is assumed that the proxy node and the end nodes have a secure connection, which is challenging to provide in constrained node networks. However, the process to find trusted nodes to perform the encryption and to maintain the integrity and authenticity of the data is itself a very challenging task to perform at end nodes. Power adaptive encryption is introduced for solar-powered wireless sensor networks in [52]. The technique switches between symmetric and public-key cryptography depending on the urgency of energy saving in the node. The scheme is focused on the solar-powered nodes so public-key cryptography can be used, and it is assumed that power is not a significant concern.

Researchers have also tried to modify the well-known encryption techniques for constrained nodes in IoT by minimizing the processing overhead of well-known cryptographic algorithms. The Blowfish encryption algorithm is implemented in [53] for data encryption in the constrained devices. Blowfish may give adequate data confidentiality and faster calculation of ciphertext. However, it requires hardware capability to perform the data encryption, and there are higher memory requirements for its long key setup [54] proposed attribute-based encryption (ABE) based on elliptic curve cryptography (ECC) rather than bilinear Diffie–Hellman pairing. The recommended encryption is no-pairing ECC-based ABE, suitable for constrained devices and to secure the communication in the network. The authors claim that the proposed encryption has lower overhead than key-policy ABE and ciphertext-policy ABE. In [55], the authors proposed a cypher-policy ABE using some precomputation techniques. The basic idea is to pre-compute and store the data obtained from expensive operations to decrease the computation for ECC. This scheme can save a significant amount of processing costs. However, the precomputation data requires memory to be stored in the node.

In [56], prevention against side-channel attacks in existing LEA (lightweight encryption algorithm) is proposed. LEA was standardized in South Korea in 2013 for IoT devices. LEA is a block encryption algorithm, used to provide confidentiality in a constrained environment. It uses addition, rotation, and XOR operations and does not use S-Box lookup like AES. To prevent the side-channel attack in LEA the bit pattern of the original pattern is changed, and information of the change is kept in the extra four bytes to decipher the data. By doing this, the differential power analysis used for the side-channel attack becomes useless. However, removing the S-Box may lead to a decrease in the strength of encryption. In [57] modification in AES operations are made to make it more dynamic and energy-efficient. The session keys and AES S-Box are updated periodically in LoRaWAN devices. The results of experimentations in the paper show that with proposed AES operation modifications LoRaWAN devices can preserve 26.2% energy for standard LoRaWAN operations.

Symmetric key encryption is relatively lightweight when compared with public key encryption techniques, but there have been attempts to embed crucial public cryptography to constrained IoT networks. The authors in [58] proposed a multi-key exchange using elliptic curve cryptography operations, and an encryption key for the exchange of session keys between the nodes. The proposed protocol is claimed to be capable enough to handle 40 sessions at a time, and the authors argue that the protocol is suitable for IoT operations. However, ECC requires rigorous calculations, and nodes in IoT are not very efficient in doing heavy processing for data encryption.

In addition to data confidentiality, node authenticity is an essential factor in ensuring legitimate data in IoT networks. As the number of nodes can be very high, and the authentication of those nodes is a challenging task. Roselin, A.G. [59] proposed an authentication technique for the end node's verification by using MAC messages. The proposed algorithm uses the symmetric key without a pre-shared key. They have used four flights (stages) for establishing the authentication and session keys. Each flight uses existing information (PAN ID, node ID) to derive a new key. The authors claim that the authentication is practical and lightweight, but it has a long process of registration of the nodes and four tiers of key calculations from the edge routers.

In [60], the authors proposed a scheme for a secure joining of the LoRa nodes in the networks. As there are so many loopholes in the current joining procedure, the authors introduced a dual key-based joining process for the new nodes in the network. They also claim that they can update the shared key in the initial deployment to enhance security. The proposed algorithm will take more energy because two keys are preloaded, and both session keys are calculated separately from different keys, which is a reasonable trade-off for better security. However, this scheme is limited to only LoRa nodes. In [61], a root key update mechanism for LoRaWAN is proposed. A two-step key derivation function using the rabbit stream pseudo-random number generator is used to derive and update the root key. The root key is used to generate session keys for data transmission. According to the authors, the proposed key update mechanism requires fewer resources in comparison to the hash-based key derivation mechanism, which is currently being used by LoRaWAN.

Considering the security vulnerabilities in current LoRaWAN standards, You, I. [62] proposed a six-step joining procedure for LoRaWAN devices. The algorithm has two options: Default option (DO) and security-enhanced option (SEO). In DO, the device follows six steps to register; in the first two steps, network server and end device authenticate each other. In the remaining four steps, application server and end devices get authenticated. The SEO option is used to save the network from the impersonation of a network server. The node communicates with the application server by signing the message with its private key to prevent any modification from an impersonator. The algorithm increases the number of transmissions to twice as many as the original LoRaWAN operations; this can shorten node energy significantly with each join operation.

In [63], a key generation and refreshment mechanism for LoRaWAN communication devices are proposed. The mechanism works in seven stages to generate AES128 keys for devices. (1) Channel probing: The devices communicate with gateway and stores received signal strength (RSSI), signal to noise ratio (SNR), and packet counter value at both parties. (2) Measurement preselection: Gateway analyzes the RSSI and SNR, and the gateway select only the values that match with antenna configuration. (3) Measurement match: The end device performs a measurement calculation based on uplink message information received from the gateway in order to achieve no packet drop. (4) Precorrection: The correction of synchronization measurements are performed in this stage using cosine transformation. (5) Quantization: The received measurements are converted into key bits. (6) Reconciliation: The errors in calculated bits are corrected in this stage. (7) Privacy affiliation: To remove the possibility of key information leak, SHA256 is used for final key generation. The authors state that security keys can be regenerated every three hours by using this scheme. However, no analysis of the energy consumption is performed. As the process requires end nodes to perform several calculations, it most probably will have an adverse effect on the node lifetime. Han, B. [64] follow a similar approach to generate keys for LPWAN devices with a four-step procedure: (1) channel probing; (2) reconciliation; (3) quantization; and (4) privacy affiliation. The authors have used signal strength sequences to quantize into a secret key. A two-step quantization mechanism is used. In the first step, the RSSI sequence is converted into binary bits. In the second step, a level crossing algorithm is used to generate an initial sequence of the secret key. As the key agreement requires the end nodes to probe and collect channel information to generate the keys, there can be probable negative impacts on node lifetime. The authors have not done any analysis of the energy consumption of the scheme.

A key management and update mechanism is proposed in [65] for LoRa devices. Elliptic-curve Deffie–Helman (ECC-DH) is used for key agreements, and a hierarchical deterministic (HD) wallet is used for key management in the system. Server and the devices generate a public and private key pair in their HD wallet using BIP32 algorithm [66]. After the key pair generation, the end devices register themselves to the server by sending their public keys. The server generates a root key pair based on the information received from the device and stores it for communication. The mechanism uses ECC-DH for a key agreement after receiving the public information from devices in the network. The proposed mechanism enables the devices to update the security keys for better security. The key generation mechanism adds communication and procession overhead by using eight-step for key generation. However, the authors argue that it is a reasonable trade-off for the security of the network. LPWAN networks are vulnerable to attacks like identity theft or impersonation of legitimate nodes. These attacks can cause substantial damage to the authenticity of nodes that are transmitting data to users. It becomes essential to have a robust attack detection mechanism.

There are many attempts in constrained network environments to minimize the effect of these attacks by identifying the devices for early detection of an attack and for taking the necessary actions. The authors Rasmussen, B.K. and Xu, Q. in [67,68] discuss the usability of node fingerprinting for security in a sensor network. The approach in [69] uses the time difference between the acknowledgement and authentication packets to create a fingerprint of the nodes, in [16,70] neighbor information is used to create fingerprints and to identify clones in the network. In [71], "GTID" is proposed for device type fingerprinting. It has four components: Feature extraction, signature generation, similarity measure, and enroll. GTID primarily relies on inter-arrival time (IAT) of the packets from devices and generates their fingerprint based on the traffic rate distribution of devices. Once the signatures are generated, they are used to train artificial neural networks and patterns are registered to add the devices to the network.

In [72], the authors introduced the "PARADIS" technique, which uses the defects in hardware to identify the nodes. Differences in individual frames in the modulation domain are analyzed, and machine learning classification tools are used to identify the end nodes. Deviation in the clock skews of transmitting devices to create fingerprints to identify the devices is proposed in [73]. The authors in [74–76] have used radio frequencies to create device prints. In [77], the authors used the preamble of the signal to generate node fingerprints to identify impersonators in the network.

A node identification based on radio signal irregularities is proposed in [78]. Authors have proposed an identification mechanism for nodes based on their signal irregularities of nodes. The receiver fingerprints every node based on attributes like frequency offset, I-Q imbalance, DC offset channel information. On top of these attributes, a neural network is trained to identify the nodes in the network. No secret key is to be stored in the nodes for authentication. All the processing is performed by the gateway. Although no key is required for authentication, the secret key will be needed for secure data transmission. In [79], a machine learning-based node identification mechanism based on physical unclonable functions (PUF) is suggested. PUFs are values that are generated due to the irregularity of the manufacturing of electronic chips. The authors first proposed a cloning mechanism of PUF, and then a machine learning classifier is trained for detection of cloned PUFs with an accuracy of 96%.

4.2. Security with Software Defined Architecture

The constrained nodes restrict the use of advanced cryptographic mechanisms for security in LPWAN. As discussed in the previous subsection, there have been numerous attempts to enhance security in constrained networks. However, to implement state-of-the-art security in LPWAN communication, we need to transfer the computation's extensive tasks to a capable entity in the network while maintaining the efficiency of security mechanisms.

SDN has been an emerging framework in networks security. Its decoupled architecture provides the flexibility of rapid implementation of the dynamic mechanism. The data plane of the network is separated from the control plane and can be managed in a generic manner instead of being vendor-specific [14]. The network programmability [13,14,80–86] provides the opportunity to implement robust security measures that can adapt to the changing network requirement in LPWAN-based IoT networks.

SDN has been applied and tested in multiple attempts and has proven its effectiveness in various aspects of network security. Jun Wu et al. [87] proposed a hierarchy-based framework for the higher security of wireless sensor networks. Detection of attacks is divided into two parts, sensor end and base station end. The sensor nodes perform low-level detection with basic rules that require less computation. The base station performs detection with sophisticated rules with higher computation requirements. Once the detection is done, SDN and network virtualization are used to mitigate the attack on the network. As the involvement of sensor nodes in detection will require the active participation of sensor nodes, they will require to gather data and use decision-making algorithms to detect attacks on the network. Sensor nodes are energy constrained; the more they participate in the detection mechanism, the more energy is consumed. Hence, the node lifetime will be shortened because of the detection mechanism.

An authentication mechanism in a heterogeneous environment is being suggested in [88]. The technique is divided into three phases: (1) Gateway public key certification; (2) thing registration; (3) authentication phase. The gateway is certified by the controller in the first phase; in the second phase, end nodes register their identities to the controller using the controller's public key with ECC. The third phase is for node authentication, where the node's public key is used to send encrypted data to the end node. The controller is powerful enough to perform the complicated operations of ECC. However, it is not very efficient to perform such rigorous calculations at the end nodes with limited resources.

A lightweight security mechanism was proposed for the smart building [89,90]. Mutual authentication between the SDN controller and sensors is proposed. Controller and devices share a secret key before any communications. In the first phase, the device authenticates the controller, where devices generate a nonce and send it to the controller with its ID. The controller calculates Hash Message Authentication Code (HMAC) on receiving the nonce and data using the secret key and sends it to the end node. Finally, the end node again calculates the HMAC on its end to compare and verify the authenticity of the controller. Nodes are verified by the controller, in the same manner, using nonce and secret key.

In [91], attack detection on network nodes is proposed by traffic monitoring. SDN controller continuously monitors traffic patterns from nodes and uses learning modules from stored attack models. An anomaly in traffic pattern is detected using a machine-learning algorithm to identify an attack on the network. The authors in [86] proposed a secure architecture for IoT using the "black" network, an SDN controller, and a key management registry. The black network is used to add privacy, the key registry is used for key management, and SDN controllers are used for secure routing in the network. IoT SENTINEL [92], is proposed as a system that can identify the types of devices connected and enforce the rules to minimize the damage from node compromise. Device fingerprint is created by using previous network traffic. SDN controllers are used to identify the fingerprints of the new devices and enforce security rules on them. Using only traffic data for device fingerprinting can cause errors in the classification and identification of the devices; multiple criteria should be used to identify devices instead.

In [93] an energy efficient blockchain and SDN-based architecture is proposed for security in IoT networks. The architecture uses cluster structure to increase the manageability of the network, each cluster is an SDN domain, and the SDN controller acts as a cluster head. The SDN controller is responsible for activation of end devices and enforcing the policies in the domain. The SDN controllers of all the clusters form a peer-to-peer blockchain-based connection for secure transactions. The computations are transferred towards the SDN controller to avoid energy drain of IoT devices in the network.

In [94], a prevention mechanism against Man in the Middle attack is proposed by using SDN framework. The proposed mechanism uses a proxy as a traffic security upgrader. The proxy converts the HTTP traffic into HTTPS. By using a proxy, the mechanism offloads the processing from end devices to a different entity and avoids energy consumption at the end node. The SDN controller is used as the traffic redirector. It redirects the traffic to proxy if it requires the security upgrade, or lets it pass directly to the routers and further to the servers.

A DDoS attack prevention mechanism is proposed in [95]. The proposed mechanism uses cloud, SDN framework, and machine learning for attack detection. A semi-supervised machine learning algorithm is used for blacklisting of malicious nodes and filters the traffic using OpenFlow switches and SDN controller. Similarly, SeArch, an SDN-based intrusion detection mechanism for cloud-based IoT networks is proposed in. [96].

In another attempt against DDoS attack on IoT networks, Luo, X. [97] uses SDN-based honeypots. The SDN controller is used to mimic IoT nodes in the network to lure the attackers. In addition, moving target defense (MTD) is implemented with the SDN controller. The SDN controller changes the address of the devices while mapping it to their original addresses, making it difficult for the attackers to find the active devices to attack.

In [98], SDN controller is used to enforce security policies in IoT networks. The proposed system profiles the security of various devices based on their attributes. To enforce security profiles in network, features of the SDN framework are used for fine-grained control. Authors in [99] leverage the decoupled architecture of SDN. They suggest potential mechanisms for detection and countermeasures against different attacks on IoT networks.

Table 3 shows the overview and comparison of solutions discussed in this section based on various security measures addressed.

Table 3. Comparative analysis of existing security solutions.

Paper Name	Proposed Solution	Security Aspects Covered				Shortcomings
		Authentication	**Confidentiality**	**Key Exchange**	**Attack Detection**	
Swapped Huffman tree coding application for low-power wide-area network (LPWAN) [49]	Swapped Huffman tree encoding is used for compression and encryption.	-	✔		-	The encryption is weak against sophisticated attacks like pattern analysis.
Cooperative Ciphertext-Policy Attribute-Based Encryption for the Internet of Things [50]	The load distribution between the nodes is done to divide the encryption task amongst the nodes.	-	✔	-	-	Data division and joining can be a complicated scenario, can cause integrity issues with the data.
Implementation of data encryption for the Internet of Things using Blowfish algorithm on FPGA [53]	Blowfish symmetric key algorithm is implemented on a field-programmable gate array (FPGA).	-	✔	-	-	Blowfish is considered faster than AES. However, it takes much memory to store the key setup, giving AES an edge over Blowfish.
A lightweight attribute-based encryption scheme for the Internet of Things [54]	No pairing attribute-based encryption (ABE) using ECC rather than using the Diffie–Hellman pairing.	-	✔	-	-	ECC has complicated operations for encryption that may exhaust the nodes faster.
Lightweight Attribute-Based Encryption for the Internet of Things [55]	Use pre-computed data to perform encryption to save time.	-	✔	-	-	The pre-computed data can occupy lots of space in the node.
Secure and efficient data transmission in the Internet of Things [100]	A public key and identity-based infrastructure interface to make them both work together.	✔	✔	-	-	Public key encryption is considered a computation-intensive algorithm and hence would drain the battery of IoT nodes.
TTP Based High-Efficient Multi-Key Exchange Protocol [58]	Use of ECC for key exchange.	✔	✔	✔	-	ECC is complicated and energy-consuming for IoT devices.

Table 3. *Cont.*

Paper Name	Proposed Solution	Security Aspects Covered				Shortcomings
		Authentication	Confidentiality	Key Exchange	Attack Detection	
An improved LEA block encryption algorithm to prevent a side-channel attack in the IoT system [56]	Prevention mechanism from side-channel attacks on nodes.		✔	-	–	The proposed algorithm removed S-box lookup, which might decrease the cipher strength.
Lightweight Authentication Protocol (LAUP) for 6LoWPAN Wireless Sensor Networks [59]	Proposed a four-step procedure to establish authentication and session key.	✔	✔	✔	-	The process is lengthy and time-consuming, as it takes four stages to calculate the session keys from information from previous stages.
Enhancing the security of the IoT LoRaWAN architecture [51]	Proxy-based encryption scheme for distributing the processing load.	✔	✔	✔	-	It is challenging to find trusted nodes in the network.
A Dual Key-Based Activation Scheme for Secure LoRaWAN [60]	Secure joining procedure for LoRa nodes.	✔	-	✔	-	Different keys are loaded to generate network and application session key. However, this scheme is only limited to LoRa nodes.
Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks [63]	A key generation and key refreshment mechanism for LoRa devices.	✔	-	✔	-	The process requires end nodes to perform several calculations, it most probably will have an adverse effect on the node lifetime
An Improved Secure Key Management Scheme for LoRa System [65]	A key management and update mechanism based on ECC for LoRa devices.	✔	-	✔	-	The key generation mechanism is long and may put overhead on the network nodes.

Table 3. *Cont.*

Paper Name	Proposed Solution	Security Aspects Covered				Shortcomings
		Authentication	Confidentiality	Key Exchange	Attack Detection	
A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities [87]	SDN is used for multi-stage attack detections in the network.	-	-	-	✔	Sensor nodes are also participating in attack detection. This can cause overhead on constrained nodes of the network.
Identity-Based Authentication Scheme for the Internet of Things [88]	Three-stage node authentication using SDN controller.	✔	-	-	-	Constrain nodes have to perform a computationally extensive process of ECC.
Software Defined Intelligent Building [89]	Mutual authentication scheme between SDN controller and sensor nodes.	✔	✔	✔	-	The proposed algorithm can use SDN controller as a central key management authority. However, the number of operations the end node is performing is the same as a LoRaWAN, and the effect of energy consumption due to operations is not analyzed.
S2 Net: A Security Framework for Software Defined Intelligent Building Networks [90]	Mutual authentication scheme between the SDN controller and sensor nodes.	✔	✔	✔	-	The proposed approach is an extension of Xu, R.Y. [89]. However, the number of operations for end nodes remain the same as the previous scheme. Hence the drawback of energy consumption remains the same.
Dynamic Attack Detection and Mitigation in IoT using SDN [91]	The attack on end nodes is detected by continuously analyzing network traffic with the SDN controller.	-	-	-	✔	The experimentation conducted is only focusing on denial of service (DoS) type attacks on the network. Other types of attacks, such as impersonation attack and injection attacks are not tested in experiments.

Table 3. *Cont.*

Paper Name	Proposed Solution	Security Aspects Covered				Shortcomings
		Authentication	Confidentiality	Key Exchange	Attack Detection	
A Secure IoT Architecture for Smart Cities [86]	An amalgamation of traditional and SDN framework is used to provide holistic security with the network providing confidentiality, identity management, and attack detection.	✔	✔	-	✔	The architecture addresses key aspects of security. However, it still lacks mobility support of the nodes in the network.
IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT [92]	Device identification based on data attributes in the network.	-	-	-	✔	Using only traffic data for device fingerprinting can cause errors in the classification and identification of the devices.

As Table 3 illustrates, the SDN architecture has been proven to be effective on various security parameters. Although there are split opinions about SDN to be used in security, SDN brings in novel and effective aspects for security in IoT and other constrained network environments. In light of the findings from the literature about the possibilities of SDN in IoT and constrained network security, the next section explores the opportunities and challenges SDN brings to the table.

5. Challenges and Opportunities for Software Defined Network (SDN)-Based Security in LPWAN

The literature shows various attempts in the direction of enhancements in security for constrained node networks, with and without the use of SDN architectures. There have been numerous attempts to enhance the network architecture for the security of IoT networks such as LPWAN. However, traditional network architectures take a long time to adapt to the changes in the network, and the novel approaches are challenging to implement quickly as the underlying devices are not very open to modifications.

In addition, the literature also shows various attempts of using SDN architecture for security in IoT or constrained networks with similar conditions as LPWAN. SDN has proved to be effective against various attacks such as DoS, DDoS, impersonation attacks [91]. Also, SDN has proven effective with other security challenges like node identification, authentication, node classification, and intrusion detection [86,89,90,92–99]. Table 4 shows an overview of applicability of SDN in various security domains shown in literature.

Table 4. Software defined network (SDN) applicability in various security domains.

Literature	Focused Area for Security
[86,87,91,92,94,95,97,99]	Prevention against various attacks such as DoS, DDoS, MIMT, flooding attacks on network by using SDN controller.
[86,88–90,93,98]	Authentication of nodes in the network by using SDN controller as central entity of key distribution or by using attribute-based node authentications.
[89,90,93]	Key exchange and node activation with SDN controller

Unlike traditional networking architecture, SDN provides flexibility to the network administrators to change the policies on the fly, monitor the dynamics of the network, recognize the attack patterns, self-learn, and self-heal using algorithms. Thus, SDN makes it easy to implement new techniques and develop algorithms on top of the control plane [101].

SDN uses an open architecture for viewing and controlling the network. Applications can be developed on top of the control plane as per the requirement of IoT networks. For example, in smart home IoT or industrial IoT, applications can be developed to provide a higher level of security such as behavioral intrusion detection. SDN has several advantages over the traditional networking paradigm. SDN comes with great opportunities and some trade-offs. We further discuss the pros and cons of SDN-based security mechanisms [102].

5.1. Opportunities with SDN in LPWAN Security

SDN brings some promising factors into the security of nodes in LPWAN networks. SDN features have been used for different areas in networking such as network management, traffic engineering, load balancing, and routing. How these features can be used for security in LPWAN is discussed below:

1. Global-view: SDN provides a complete view of the network to the controller. This property can be used as very effective in defending IoT networks against multiple attacks. The controller can monitor the activities of all the end nodes at the switch level. Various machine learning techniques can be implemented at the controller to perform packet inspection to classify the traffic. Anomaly detections mechanisms can be used at the controller to point out the malicious behavior of nodes in an IoT network.

2. Early stage attack detection: With advanced machine learning techniques at the controller, network attacks can be detected in the early stages. The controller can redirect or block the malicious traffic on the network devices, and prevent IoT application servers from failing to provide services. This property of SDN also puts it forward as a substitute for efficient middleware in IoT networks. In recent advancements, machine learning and artificial intelligence (AI) have been used with SDN for quick and effective intrusion detection in 5G networks [103–106]. The SDN controllers can be utilized to create smart networks with AI techniques for enhanced security and network management [107].
3. Self-healing mechanisms: IoT networks can scale up to thousands and millions of devices connected to the Internet. In such a large network it is crucial to have mechanisms that can minimize the effect of attacks on the network. In [108], a realization of self-aware network using SDN and AI techniques is discussed. The global view facilitates the early detection of various attacks; in addition to that, SDN provides effective preventive measures against attacks. The switches can be programmed to take action against traffic coming from a malicious node in the network. These packets can either be redirected to a specific port for gathering information or can be dropped. SDN switches are capable of taking multiple actions rather than being just a forwarding device, as in a traditional network. Taking actions at switch level can limit the reach of malicious nodes, preventing IoT services from being interrupted. The smart self-healing capability of SDN also makes it possible for it to handle traffic bottleneck because of the dynamic traffic handling of SDN [109].
4. Fine grain control over data flow: The ability of switches to make decisions enables SDN to minimize the effect of attacks on IoT networks. The switches can make decisions because of the fine-grained control provided in SDN, as the switches can perform header analysis of incoming data and understand the control bits. This control also plays a vital role in data routing where switches can prioritize the flows based on their header information. In IoT, where various applications are running on the same network, it is vital to classify the traffic and make decisions based on application requirements. Moreover, the flow level control of SDN also has the capability of managing huge amounts of data with the help of AI techniques [110,111], making it a compatible solution for handling huge amounts of data in IoT.
5. Cost-effective: For IoT to function on such a large scale, the network component must be efficient and cost-effective. Given the scale of IoT applications, vast volumes of information are gathered and processed, and SDN-based mechanisms can be used as middleware for smart data dissemination [112]. SDN can also be used as a firewall and load balancer in a network, minimizing the requirement of additional hardware for network firewalls [113]. Given the potential of SDN as middleware for data management and security, SDN can be seen as a cost-effective alternative to the traditional networking approach [114].

Figure 5 shows an outline of how SDN can be integrated with constrained nodes in IoT networks to provide security solutions. The SDN controller can be used as a key distribution authority and for network monitoring. The SDN enables switches to make it possible for the controller to monitor the traffic at the network layer and change the configuration at switches. In addition to monitoring traffic, the SDN controller can be used to minimize processing overhead from end nodes.

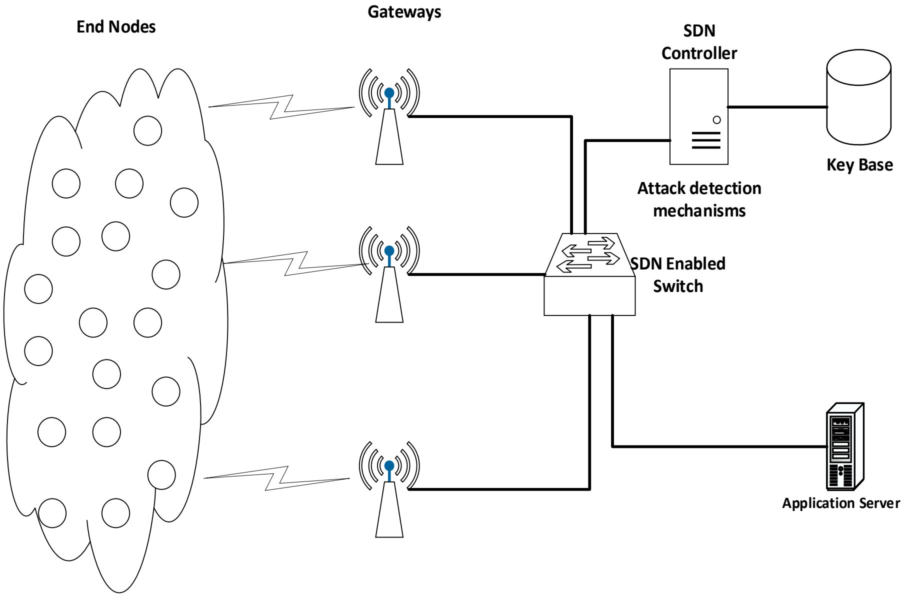

Figure 5. SDN-based architecture for LPWAN.

5.2. Challenges in SDN Based LPWAN Security Implementation

SDN brings promising opportunities for network security and management. However, there are several trade-offs [102,115]. The use of a centralised controller for decision making creates a single point of failure in the network. The attacker can target a single entity to bring the network down. However, the dependency on a single controller can be minimized by using multiple controllers in a hierarchical structure. Use of a hierarchical structure not only minimizes the dependency on a single entity, but it also distributes the load amongst multiple entities and minimizes delays in controller response.

SDN switches are also vulnerable to various kind of attacks like DDoS and false flow entry to switches, and there are various shortcomings in switch authentication mechanisms as well. SDN controllers are prone to DDoS attacks that can cause serious damage to the network, and must be addressed [116]. However, SDN standards are still under development, and these shortcomings are expected to be addressed in later versions of SDN standard protocols such as OpenFlow [117]. For instance, OpenFlow version 1.5.1 proposed a header encryption for better security. However, the security parameters are left optional in the current version and are expected to be addressed in upcoming versions of the protocol [115].

6. Conclusions

IoT has emerged as one of the most prominent areas of research because of its diverse applications. IoT has a number of applications with battery-powered nodes where LPWAN is suitable for data transmission. LPWAN supports low-powered long-range transmission, where nodes are deployed in hostile conditions and are vulnerable to various security threats. This paper discussed current LPWAN technologies, their security mechanisms, and vulnerabilities in detail. A comprehensive literature review of IoT security using different frameworks was carried out, and it showed that LPWAN has multiple vulnerabilities that need to be addressed. Considering the constrained environment, scale, and diversity of IoT networks, it requires flexible frameworks that can reduce computations on end nodes and are quick with applying changes in network policies for network security. SDN brings a framework that provides functionalities and flexibilities required to regulate such network. The literature review revealed that SDN frameworks show significant potential to provide security mechanisms for constrained networks, which can be integrated with current IoT architectures to support security solutions. Although SDN brings some security vulnerabilities, the standardization of the protocols in SDN is still under development, and the vulnerabilities are expected to be resolved in upcoming versions. The review of the literature revealed that SDN has the capability of providing robust security mechanisms. The network programmability capabilities provide quick adaptability to network changes. Because of its dynamic and flexible nature, SDN shows potential not only for security but also as an efficient and cost-effective middleware for networks, making it a total package for a complete suite of network security.

Further, future studies should be conducted on implementation of robust and scalable SDN-based security solutions for LPWAN IoT networks. The highlighted vulnerabilities in LPWAN communication technologies must be address for secure and effective IoT networks.

Author Contributions: Conceptualization, G.P., J.G., and S.U.R.; methodology, G.P.; Validation, J.G., and S.U.R.; formal analysis, G.P.; data curation, G.P.; writing—original draft preparation, G.P.; writing—review and editing, J.G., and S.U.R.; supervision, J.G., and S.U.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research has not received any external funding.

Conflicts of Interest: The authors declare no conflict of interest in this manuscript.

References

1. Alaba, F.A.; Othman, M.; Hashem, I.A.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
2. Raza, U.; Kulkarni, P.; Sooriyabandara, M. Low Power Wide Area Networks: An Overview. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 855–873. [CrossRef]
3. Mehmood, Y.; Ahmad, F.; Yaqoob, I.; Adnane, A.; Imran, M.; Guizani, S. Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Commun. Mag.* **2017**, *55*, 16–24. [CrossRef]
4. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2018**, *5*, 1–7. [CrossRef]
5. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805.
6. Wang, J.; Miao, Y.; Zhou, P.; Hossain, M.S.; Rahman, S.M. A software defined network routing in wireless multihop network. *J. Netw. Comput. Appl.* **2017**, *85*, 76–83. [CrossRef]
7. Liu, K.; Cao, Y.; Liu, Y.; Xie, G.; Wu, C. A Novel Min-Cost Qos Routing Algorithm for Sdn-Based Wireless Mesh Network. In Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 14–17 October 2016.
8. Modieginyane, K.M.; Letswamotse, B.B.; Malekian, R.; Abu-Mahfouz, A.M. Software defined wireless sensor networks application opportunities for efficient network management: A survey. *Comput. Electr. Eng.* **2017**, *66*, 274–287. [CrossRef]
9. Manisekaran, S.; Venkatesan, R. An analysis of software-defined routing approach for wireless sensor networks. *Comput. Electr. Eng.* **2016**, *56*, 456–467. [CrossRef]
10. Brito, S.I.V.; Figueiredo, G.B. Improving QoS and QoE through seamless handoff in Software-Defined IEEE 802.11 Mesh Networks. *IEEE Commun. Lett.* **2017**, *21*, 2484–2487. [CrossRef]
11. Labraoui, M.; Boc, M.; Fladenmuller, A. Self-configuration mechanisms for SDN deployment in Wireless Mesh Networks. In Proceedings of the 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Macau, China, 12–15 June 2017.
12. Abujoda, A.; Dietrich, D.; Papadimitriou, P.; Sathiaseelan, A. Software-defined wireless mesh networks for internet access sharing. *Comput. Netw.* **2015**, *93*, 359–372. [CrossRef]
13. McKeown, N.; Anderson, T.; Balakrishnan, H.; Parulkar, G.; Peterson, L.; Rexford, J.; Shenker, S.; Turner, J. OpenFlow: Enabling innovation in campus networks. *ACM SIGCOMM Comput. Commun. Rev.* **2008**, *38*, 69–74. [CrossRef]
14. Nunes, B.A.; Mendonca, M.; Nguyen, X.N.; Obraczka, K.; Turletti, T. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1617–1634. [CrossRef]
15. Sain, M.; Kang, Y.J.; Lee, H.J. Survey on security in Internet of Things: State of the art and challenges. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 19–22 February 2017.

16. Zhu, W.T.; Zhou, J.; Deng, R.H.; Bao, F. Detecting node replication attacks in wireless sensor networks: A survey. *J. Netw. Comput. Appl.* **2012**, *35*, 1022–1034. [CrossRef]
17. Vangelista, L.; Zanella, A.; Zorzi, M. *Long-Range IoT Technologies: The Dawn of LoRa™ 2015*; Springer International Publishing: Cham, Switzerland, 2015.
18. Knyazev, S.N.; Chechetkin, V.A.; Letavin, D.A. Comparative analysis of standards for Low-power Wide-area Network. In Proceedings of the 2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO), Kazan, Russia, 3–4 July 2017.
19. SIG, W. Weightless Specification. 2017. Available online: http://www.weightless.org/about/weightless-specification (accessed on 12 January 2020).
20. Sanchez-Iborra, R.; Cano, M.-D. State of the Art in LP-WAN Solutions for Industrial IoT Services. *Sensors* **2016**, *16*, 708. [CrossRef] [PubMed]
21. Mangalvedhe, N.; Ratasuk, R.; Ghosh, A. NB-IoT Deployment Study for Low Power Wide Area Cellular IoT. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–7 September 2016.
22. Coman, F.L.; Malarski, K.M.; Petersen, M.N.; Ruepp, S. Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019.
23. GSMA. Security Features of LTE-M and NB-IoT Networks. 2019. Available online: https://www.gsma.com/iot/resources/security-features-of-ltem-nbiot (accessed on 12 January 2020).
24. DASH7 Alliance Wireless Sensor and Actuator Network Protocol, version 1.2. 2018. DASH7 Alliance. Available online: https://dash7-alliance.org/product/dash7-alliance-protocol-specification-v1-2/ (accessed on 17 July 2019).
25. Bor, M.; Vidler, J.; Roedig, U. LoRa for the Internet of Things. In Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, Graz, Austria, 15–17 February 2016; Junction Publishing: Graz, Austria, 2016; pp. 361–366.
26. Miller, R. LoRa Security: Building a secure LoRa solution. *MWR Labs White Paper*, March 2016.
27. Yang, X. LoRaWAN: Vulnerability Analysis and Practical Exploitation. Master's Thesis, Delft University of Technology, Delft, The Netherlands, 2017.
28. Nguyen, V.-L.; Lin, P.-C.; Hwang, R.-H. Energy Depletion Attacks in Low Power Wireless Networks. *IEEE Access* **2019**, *7*, 51915–51932. [CrossRef]
29. Yang, X.; Karampatzakis, E.; Doerr, C.; Kuipers, F. Security Vulnerabilities in LoRaWAN. In Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017.
30. Aras, E.; Ramachandran, G.S.; Lawrence, P.; Hughes, D. Exploring the security vulnerabilities of LoRa. In Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, UK, 21–23 June 2017.
31. Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wirel. Commun.* **2016**, *23*, 60–67. [CrossRef]
32. Kail, E.; Banati, A.; Lászlo, E.; Kozlovszky, M. Security Survey of Dedicated IoT Networks in the Unlicensed ISM Bands. In Proceedings of the 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 17–19 May 2018.
33. Siddiqui, S.T.; Alam, S.; Ahmad, R.; Shuaib, M. Security Threats, Attacks, and Possible Countermeasures in Internet of Things. In *Advances in Data and Information Sciences*; Springer: Singapore, 2020.
34. Fujdiak, R.; Blazek, P.; Mikhaylov, K.; Malina, L.; Mlynek, P.; Misurec, J.; Blazek, V. On Track of Sigfox Confidentiality with End-to-End Encryption. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; ACM: Hamburg, Germany, 2018; pp. 1–6.
35. Chacko, S.; Job, M.D. Security mechanisms and Vulnerabilities in LPWAN. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *396*. [CrossRef]
36. Van Es, E.; Vranken, H.; Hommersom, A. Denial-of-Service Attacks on LoRaWAN. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; ACM: Hamburg, Germany, 2018; pp. 1–6.

37. 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]
38. Zulian, S. Security Threat Analysis and Countermeasures for Lorawan Join Procedure. Master's Thesis, University of Padova, Padua, Italy, 2016.
39. Gresak, E.; Voznak, M. Protecting gateway from abp replay attack on lorawan. In *International Conference on Advanced Engineering Theory and Applications*; Springer: Cham, Switzerland, 2018; pp. 400–408.
40. Grammatikis, P.I.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, threats and solutions. *Internet Things* **2019**, *5*, 41–70. [CrossRef]
41. Danish, S.M.; Nasir, A.; Qureshi, H.K.; Ashfaq, A.B.; Mumtaz, S.; Rodriguez, J. Network intrusion detection system for jamming attack in lorawan join procedure. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018.
42. Hamza, T.; Kaddoum, G.; Meddeb, A.; Matar, G. A survey on intelligent MAC layer jamming attacks and countermeasures in WSNs. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016.
43. Wei, X.; Wang, T.; Tang, C.; Fan, J. Collaborative mobile jammer tracking in multi-hop wireless network. *Future Gener. Comput. Syst.* **2018**, *78*, 1027–1039. [CrossRef]
44. Tang, X.; Ren, P.; Han, Z. Jamming mitigation via hierarchical security game for IoT communications. *IEEE Access* **2018**, *6*, 5766–5779. [CrossRef]
45. Zillner, T.; Strobl, S. ZigBee Exploited: The Good, the Bad and the Ugly. Black Hat–2015. Available online: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf (accessed on 21 March 2018).
46. Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 184–208. [CrossRef]
47. Aminanto, M.E.; Tanuwidjaja, H.C.; Yoo, P.D.; Kim, K. Weighted feature selection techniques for detecting impersonation attack in Wi-Fi networks. In Proceedings of the SCIS 2017 - Symposium on Cryptography and Information Security, Naha, Japan, 24–27 January 2017.
48. Raza, S.; Trabalza, D.; Voigt, T. 6LoWPAN Compressed DTLS for CoAP. In Proceedings of the 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, Hangzhou, China, 16–18 May 2012.
49. Jang, Y.S.; Usman, M.R.; Usman, M.A.; Shin, S.Y. Swapped Huffman tree coding application for low-power wide-area network (LPWAN). In Proceedings of the 2016 International Conference on Smart Green Technology in Electrical and Information Systems (ICSGTEIS), Bali, Indonesia, 6–8 October 2016.
50. Touati, L.; Challal, Y.; Bouabdallah, A. C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things. In Proceedings of the 2014 International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, Algeria, 17–19 June 2014.
51. 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, 22–24 November 2016.
52. Kim, J.M.; Lee, H.S.; Yi, J.; Park, M. Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks. *J. Sens.* **2016**, *2016*, 2678269. [CrossRef]
53. Prasetyo, N.K.; 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.
54. Yao, X.; Chen, Z.; Tian, Y. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Gener. Comput. Syst.* **2015**, *49*, 104–112. [CrossRef]
55. Oualha, N.; Nguyen, K.T. Lightweight Attribute-Based Encryption for the Internet of Things. In Proceedings of the 2016 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA, 1–4 August 2016.
56. 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, 13–15 December 2016.
57. 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]

58. 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]
59. Roselin, A.G.; Nanda, P.; Nepal, S. Lightweight Authentication Protocol (LAUP) for 6LoWPAN Wireless Sensor Networks. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 1–4 August 2017.
60. Kim, J.; Song, J. A Dual Key-Based Activation Scheme for Secure LoRaWAN. *Wirel. Commun. Mobile Comput.* **2017**, *2017*, 6590713. [CrossRef]
61. Han, J.; Wang, J. *An Enhanced Key Management Scheme for LoRaWAN.*; Springer International Publishing: Cham, Switzerland, 2018.
62. You, I.; Kwon, S.; Choudhary, G.; Sharma, V.; Seo, J.T. An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system. *Sensors* **2018**, *18*, 1888. [CrossRef]
63. Ruotsalainen, H.; Zhang, J.; Grebeniuk, S. Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks. *IEEE Internet Things J.* **2020**, *7*, 1745–1755. [CrossRef]
64. Han, B.; Peng, S.; Wang, X.; Wang, B. Distributed Physical Layer Key Generation for Secure LPWAN Communication. In Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, 4–6 December 2019.
65. Xing, J.; Hou, L.; Zhang, K.; Zheng, K. An Improved Secure Key Management Scheme for LoRa System. In Proceedings of the 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 16–19 October 2019.
66. Wuille, P. Bip32: Hierarchical Deterministic Wallets. 2012. Available online: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki (accessed on 27 April 2020).
67. Rasmussen, B.K.; Capkun, S. Implications of radio fingerprinting on the security of sensor networks. In Proceedings of the 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007, Nice, France, 17–21 September 2007.
68. Xu, Q.; Zheng, R.; Saad, W.; Han, Z. Device fingerprinting in wireless networks: Challenges and opportunities. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 94–104. [CrossRef]
69. Sieka, B. Active fingerprinting of 802. 11 devices by timing analysis. In Proceedings of the CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 8–10 January 2006.
70. Xing, K.; Liu, F.; Cheng, X.; Du, D.H. Real-time detection of clone attacks in wireless sensor networks. In Proceedings of the 2008 The 28th International Conference on Distributed Computing Systems, Beijing, China, 17–20 June 2008.
71. Radhakrishnan, V.S.; Uluagac, A.S.; Beyah, R. GTID: A technique for physical device and device type fingerprinting. *IEEE Trans. Dependable Secure Comput.* **2015**, *12*, 519–532. [CrossRef]
72. Brik, V.; Banerjee, S.; Gruteser, M.; Oh, S. Wireless Device Identification With Radiometric Signatures. In Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco, CA, USA, 14–19 September 2008.
73. Kohno, T.; Broido, A.; Claffy, K.C. Remote physical device fingerprinting. *IEEE Trans. Dependable Secure Comput.* **2005**, *2*, 93–108. [CrossRef]
74. Faria, B.D.; Cheriton, D.R. Detecting identity-based attacks in wireless networks using signalprints. In Proceedings of the 5th ACM workshop on Wireless security, Francisco, CA, USA, 29 September 2006.
75. Gerdes, R.M.; Daniels, T.E.; Mina, M.; Russell, S. Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach. In Proceedings of the Network and Distributed System Security Symposium, NDSS 2006, San Diego, CA, USA, 2006.
76. Patwari, N.; Kasera, S.K. Robust Location Distinction Using Temporal Link Signatures. In Proceedings of the 13th annual ACM international conference on Mobile computing and networking, Montreal, QC, Canada, 9–14 September 2007.
77. Rehman, S.U.; Sowerby, K.W.; Chong, P.H.; Alam, S. Robustness of Radiometric Fingerprinting in The Presence of An Impersonator. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017.
78. Chatterjee, B.; Das, D.; Maity, S.; Sen, S. RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning. *IEEE Internet Things J.* **2019**, *6*, 388–398. [CrossRef]

79. Laguduva, V.; Islam, S.A.; Aakur, S.; Katkoori, S.; Karam, R. Machine learning based iot edge node security attack and countermeasures. In Proceedings of the 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Miami, FL, USA, 15–17 July 2019.
80. Campbell, A.T.; Katzela, I.; Miki, K.; Vicente, J. Open signaling for ATM. internet and mobile networks (OPENSIG'98). *ACM SIGCOMM Comput. Commun. Rev.* **1999**, *29*, 97–108. [CrossRef]
81. Bhattacharjee, S.; Calvert, K.L.; Zegura, E.W. An architecture for active networking. In *High Performance Networking VII*; Springer: Boston, MA, USA, 1997; pp. 265–279.
82. van der Merwe, J.E.; Leslie, I.M. Switchlets and dynamic virtual ATM networks. In *Integrated Network Management V*; Springer: Boston, MA, USA, 1997.
83. Enns, R. Rfc4741: Netconf Configuration Protocol. Std. Track. 2006. Available online: http://www.ietf.org/rfc/rfc4741 (accessed on 25 March 2019).
84. Casado, M.; Freedman, M.J.; Pettit, J.; Luo, J.; McKeown, N.; Shenker, S. Ethane: Taking control of the enterprise. *ACM SIGCOMM Comput. Commun. Rev.* **2007**, *37*, 1–2. [CrossRef]
85. Haleplidis, E.; Salim, J.H.; Halpern, J.M.; Hares, S.; Pentikousis, K.; Ogawa, K.; Wang, W.; Denazis, S.; Koufopavlou, O. Network programmability with ForCES. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1423–1440. [CrossRef]
86. Chakrabarty, S.; Engels, D.W. A secure IoT architecture for Smart Cities. In Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016.
87. Wu, J.; Ota, K.; Dong, M.; Li, C. A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities. *IEEE Access* **2016**, *4*, 416–424. [CrossRef]
88. Salman, O.; Abdallah, S.; Elhajj, I.H.; Chehab, A.; Kayssi, A. Identity-based authentication scheme for the Internet of Things. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016.
89. Xu, R.Y.; Huang, X.; Zhang, J.; Lu, Y.; Wu, G.; Yan, Z. Software Defined Intelligent Building. *Int. J. Inf. Sec. Priv.* **2015**, *9*, 84–99. [CrossRef]
90. Xue, N.; Huang, X.; Zhang, J. S2Net: A Security Framework for Software Defined Intelligent Building Networks. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016.
91. Bhunia, S.S.; Gurusamy, M. Dynamic Attack Detection and Mitigation in IoT Using SDN. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, Australia, 22–24 November 2017.
92. Miettinen, M.; Marchal, S.; Hafeez, I.; Asokan, N.; Sadeghi, A.R.; Tarkoma, S. IoT Sentinel: Automated device-type identification for security enforcement in IoT. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017.
93. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.K. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**. [CrossRef]
94. Al-Hayajneh, A.; Bhuiyan, Z.A.; McAndrew, I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers* **2020**, *9*, 8. [CrossRef]
95. Ravi, N.; Shalinie, S.M. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet Things J.* **2020**, *7*, 3559–3570. [CrossRef]
96. Nguyen, T.G.; Phan, T.V.; Nguyen, B.T.; So-In, C.; Baig, Z.A.; Sanguanpong, S. Search: A collaborative and intelligent nids architecture for sdn-based cloud iot networks. *IEEE Access* **2019**, *7*, 107678–107694. [CrossRef]
97. Luo, X.; Yan, Q.; Wang, M.; Huang, W. Using MTD and SDN-based Honeypots to Defend DDoS Attacks in IoT. In Proceedings of the 2019 Computing, Communications and IoT Applications (ComComAp), Shenzhen, China, 26–28 October 2019.
98. Matheu, S.N.; Robles Enciso, A.; Molina Zarca, A.; Garcia-Carrillo, D.; Hernández-Ramos, J.L.; Bernal Bernabe, J.; Skarmeta, A.F. Security architecture for defining and enforcing security profiles in dlt/sdn-based iot systems. *Sensors* **2020**, *20*, 1882. [CrossRef]
99. Zarca, A.M.; Bernabe, J.B.; Trapero, R.; Rivera, D.; Villalobos, J.; Skarmeta, A.; Bianchi, S.; Zafeiropoulos, A.; Gouvas, P. Security management architecture for NFV/SDN-aware IoT systems. *IEEE Internet Things J.* **2019**, *6*, 8005–8020. [CrossRef]
100. Li, F.; Zheng, Z.; Jin, C. Secure and efficient data transmission in the Internet of Things. *Telecommun. Syst.* **2016**, *62*, 111–122. [CrossRef]

101. Kim, H.; Feamster, N. Improving network management with software defined networking. *IEEE Commun. Mag.* **2013**, *51*, 114–119. [CrossRef]
102. Dacier, M.C.; Dietrich, S.; Kargl, F.; König, H. Network Attack Detection and Defense: Security Challenges and Opportunities of Software-Defined Networking. *Dagstuhl Rep.* **2016**, *6*, 1–28.
103. Abdulqadder, I.H.; Zhou, S.; Zou, D.; Aziz, I.T.; Akber, S.M. Multi-layered Intrusion Detection and Prevention in the SDN/NFV Enabled Cloud of 5G Networks using AI-based Defense Mechanisms. *Comput. Netw.* **2020**, *179*, 107364. [CrossRef]
104. Ashraf, J.; Latif, S. Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques. In Proceedings of the 2014 National Software Engineering Conference, Rawalpindi, Pakistan, 11–12 November 2014.
105. Holik, F.; Dolezel, P. Industrial Network Protection by SDN-Based IPS with AI. In *Intelligent Information and Database Systems*; Springer: Singapore, 2020.
106. Hande, Y.; Muddana, A. A survey on intrusion detection system for software defined networks (SDN). *Int. J. Bus. Data Commun. Netw.* **2020**, *16*, 28–47. [CrossRef]
107. Matlou, O.G.; Abu-Mahfouz, A.M. Utilising Artificial Intelligence in Software Defined Wireless Sensor Network. In Proceedings of the IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, 29 October–1 November 2017.
108. Gelenbe, E.; Domanska, J.; Fröhlich, P.; Nowak, M.P.; Nowak, S. Self-Aware Networks That Optimize Security. QoS, and Energy. *Proc. IEEE* **2020**, *108*, 1150–1167. [CrossRef]
109. Wang, L.; Delaney, D.T. QoE Oriented Cognitive Network Based on Machine Learning and SDN. In Proceedings of the 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, 12–15 June 2019.
110. Guo, A.; Yuan, C.; He, G.; Xu, L. Research on SDN/NFV Network Traffic Management and Optimization Based on Big Data And Artificial Intelligence. In Proceedings of the 2018 18th International Symposium on Communications and Information Technologies (ISCIT), Bangkok, Thailand, 26–28 September 2018.
111. Gebremariam, A.A.; Usman, M.; Qaraqe, M. Applications of Artificial Intelligence and Machine Learning in the Area of SDN and NFV: A Survey. In Proceedings of the 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD), Istanbul, Turkey, 21–24 March 2019.
112. Tortonesi, M.; Michaelis, J.; Morelli, A.; Suri, N.; Baker, M.A. SPF: An SDN-Based Middleware Solution to Mitigate the IoT Information Explosion. In Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016.
113. Zope, N.; Pawar, S.; Saquib, Z. Firewall and load balancing as an application of SDN. In Proceedings of the 2016 Conference on advances in signal processing (CASP), Pune, India, 9–11 June 2016.
114. Karakus, M.; Durresi, A. Service Cost in Software Defined Networking (SDN). In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017.
115. Dabbagh, M.; Hamdaoui, B.; Guizani, M.; Rayes, A. Software-defined networking security: Pros and cons. *IEEE Commun. Mag.* **2015**, *53*, 73–79. [CrossRef]
116. Gkountis, C.; Taha, M.; Lloret, J.; Kambourakis, G. Lightweight algorithm for protecting SDN controller against DDoS attacks. In Proceedings of the 2017 10th IFIP Wireless and Mobile Networking Conference (WMNC), Valencia, Spain, 25–27 September 2017.
117. Tourrilhes, J.; Sharma, P.; Banerjee, S.; Pettit, J. Sdn and openflow evolution: A standards perspective. *Computer* **2014**, *47*, 22–29. [CrossRef]