IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 29 July 2022, accepted 25 August 2022, date of publication 1 September 2022, date of current version 12 September 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3203387*

RESEARCH ARTICLE

# Network Architecture and Authentication Scheme for LoRa 2.4 GHz Smart Homes

**LUKE KANE[1,2], VICKY LIU[1], MATTHEW MCKAGUE[1], AND GEOFFREY R. WALKER[3], (Senior Member, IEEE)**

[1]Faculty of Science, Queensland University of Technology (QUT), Brisbane, QLD 4000, Australia
[2]Cyber Security Cooperative Research Centre, Queensland University of Technology (QUT), Brisbane, QLD 4000, Australia
[3]Faculty of Engineering, Queensland University of Technology (QUT), Brisbane, QLD 4000, Australia

Corresponding author: Luke Kane (le.kane@qut.edu.au)

This work was supported in part by the Cyber Security Research Centre Ltd., through the Australian Government's Cooperative Research Centres Programme.

**ABSTRACT** The IoT-based smart grid provides many benefits to both energy consumers and energy producers, such as advanced metering functions, improved reliability, and management. Increasingly with the rise of smart homes and smart cities, security is a concern, as data networks increasingly run parallel to power networks. Ensuring good security practices are implemented in the smart home is critical. This study proposes a Home Area Network architecture design, and secure ChaCha20-Poly1305 Authenticated Encryption with Associated Data (AEAD) based authentication scheme, based on the recent LoRa 2.4 GHz technology; a robust and highly tunable transmission technology. This results in a network that balances performance considerations, whilst providing confidentiality, integrity and authenticity through the use of symmetric key-based authentication and encryption scheme. A performance analysis is conducted using a practical test bench to determine the impact that the proposed security mechanisms have on the LoRa network. The secure architecture proposed by this study has a minimal impact on the transmission time of a packet compared to a network with no security measures. This additional latency does not negatively impact on the smart home user in terms of network performance.

**INDEX TERMS** IoT, ChaCha20, Poly1350, authentication, key management, home area network, smart home, smart grid, network performance, symmetric key encryption, LoRa 2.4 GHz.

## I. INTRODUCTION

The electricity grid has evolved from the traditional grid used to distribute electricity from large generators to customers, to the smart grid (SG); a complex combination of energy systems and IT systems allowing the two-way flow of both data and power [1], [2]. More recently, the benefits of the Internet of Things (IoT) based SG have been realised. IoT-based smart grids can enable many benefits such as Advanced Metering Infrastructure, improved reliability and management, and demand response functions based on dynamic pricing [3]. With more households having energy generation and storage capabilities through distributed energy resources (DERs) such as photovoltaic (PV) systems and battery storage, there exists exciting possibilities such as a decreased reliance on traditional generators with energy-independent neighbourhoods [4].

With all these benefits come risks and challenges. There are numerous recent examples of attacks on critical infrastructure. In May 2021 the IT systems of Colonial Pipeline; a system that is responsible for fuel distribution in the United States were attacked, which resulted in the entire system being taken offline [5]. This resulted in an outage lasting several days, which caused significant fuel shortages and panic buying across the United States [6]. In November 2021, a ransomware attack was launched on CS Energy, a Government-owned energy generator in Queensland, Australia [7]. Fortunately, in this case, CS Energy was able to contain this incident by segregating parts of the network to prevent it from spreading into the power stations [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.


This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

When dealing with any system or systems related to or connected to critical infrastructure, networking solutions need to be robust and secure; they must provide an acceptable level of performance, while also reducing the likelihood of a potentially devastating cyber-attack. Networking and security solutions are vital to the stable operation of the SG with multiple traditional and IoT-based technologies used across the SG. The SG is a widespread interconnection of many systems, ranging from power generation to home appliances [9]. The SG has many more attack surfaces than the traditional power grid; the potential exists for an attacker to gain access to SG systems via homes and businesses [9].

### A. RESEARCH SCOPE

The communication networks that underpin the smart grid can be divided into three broad categories; the home area network (HAN), the neighbourhood area network (NAN), and the wide-area network (WAN) [10]. The roles of these networks are discussed in Section II. The scope of this paper is to study and propose cost-effective Internet of Things (IoT) based networking technology and authentication solutions in the Home Area Network (HAN).

The IoT technology that will be focused on in this study is LoRa 2.4 GHz, a recently released version of the popular LoRa sub-GHz technology, based upon the Semtech SX1280 transceiver [11]. This research focuses on ensuring confidentiality and integrity can be maintained between participants on the HAN; through the proposal and evaluation of network architecture, network protocols, and authentication mechanisms. These solutions must offer acceptable security protections, with minimal impact on network latency. When looking at the well-understood OSI model [12], the scope of our work is within the first three layers, the architecture and infrastructure of the network. Specific application layer uses are not in the scope of this study.

### B. RESEARCH QUESTIONS AND OBJECTIVES

This research will address the following questions:

- How can LoRa 2.4 GHz be used to design and implement a lightweight and secure Home Area Network with sufficient network performance?
- How can security mechanisms and protocols be implemented to support the operation of smart home appliances in the Home Area Network?

To assist in addressing the research questions, this study proposes network architecture designs and secure protocols suitable for use in the HAN. This study also provides insightful network performance evaluations which show the impact of network performance tuning, highlighting the optimal combination of LoRa parameters. It does this by realising the following objectives:

1) Propose a secure LoRa 2.4 GHz based network architecture design suitable for use in the HAN by defining the components of the network, including their roles and functions.
2) Create network protocols and algorithms that define packet structures, commands, and processes for data transmission and key management.
3) Evaluate the network performance in terms of latency and packet delivery rate in a typical home environment and provide recommendations on optimal network tuning parameters.

### C. OUR CONTRIBUTION

The contribution of our work is the creation of a secure and efficient network communication and authentication scheme for the LoRa 2.4 GHz based smart home, verified with a practical implementation approach, rather than simulations. As LoRa 2.4 GHz is a more recent addition to the LoRa sub-GHz offering, minimal studies are currently available that focus on its capability, particular in a smart home environment. Further, at the time of writing, there are no other studies that have created a HAN protocol based on LoRa 2.4 GHz. This study may be of interest to IoT network designers, security professionals, and others with an interest in implementing secure, lightweight, and efficient IoT-based networks. While this study focuses on the HAN, it could easily apply to other domains.

### D. PAPER STRUCTURE

This paper will first provide some background information on key topics such as the smart grid, the HAN, LoRa and LoRaWAN and a brief overview of encryption and authentication mechanisms. Previous related work will then be discussed, with the research gaps highlighted. The network architecture design will then be presented. The proposed session key establishment mechanisms and algorithms will then be covered. An evaluation of the security effectiveness, as well as a performance analysis, will then occur. A discussion will then be presented that will cover interesting findings, difficulties that were encountered, and recommendations on the optimal LoRa tuning parameters. The paper will then conclude and highlight future work.

## II. BACKGROUND

### A. SMART GRID

As technology has evolved, we now have SGs that are capable of bidirectional flows of both data and power [1]. This has provided many improvements for both customers and suppliers such as smart metering, advanced monitoring, automated fault detection and self-healing abilities [1]. One of the key technologies that underpin the SG is IoT through the use of smart metering and other components of the Advanced Metering Infrastructure [13].

There are multiple layers in the SG. There is the electric power system layer, the communication layer and the SG application layer [14], [15]. Our study will be mainly concerned with the communication and security aspects.

There are three different data network domains within the smart grid; the HAN, the NAN, and the WAN [10].

The HAN and similar related networks exist on the premises of the customer [16]. These networks are commonly used for home automation and control, as well as to obtain energy usage information from appliances [16]. They can also facilitate control and monitoring of the home appliances by the consumer and by the utility provider, in either a ''utility managed architecture'' or a combination of ''utility and consumer managed architecture'' [17]. These networks would typically be implemented with short-range transmission technologies, as they are located within a home or building.

The NAN is the infrastructure that enables the HANs to communicate with the WAN (wide area network) and vice-versa [16]. It is also a critical part of the network in supporting Advanced Metering Infrastructure [16]. The NAN could also enable the HANs to communicate with each other in the context of sharing DERs to decrease reliance on power generators, through peer-to-peer arrangements [18].

The WAN is the wider network that sits above the neighbourhood level. It facilitates the connection to the utility provider [16]. It provides services to the entire power network, such as stability monitoring [16]. The term WAN could refer to any networks above the neighbourhood level.

### B. HAN AND HOME ENERGY MANAGEMENT SYSTEMS

This research is focused on the HAN, and as such, some further background information about the purpose and function of the HAN is necessary. As a society, we need to devise more efficient ways of consuming less energy to reduce carbon usage to improve our future environmental outlook. An important area that cannot be overlooked is the home. Giving residential users the tools to monitor and positively impact their energy usage will promote personal accountability through behavioural change [19]. The systems that are implemented within the smart home/HAN to allow home users to monitor and control their energy usage are typically called Smart Home Energy Management Systems (SHEMS) and/or Home Energy Management Systems (HEMS) [19], [20], [21]. Mendes *et al.* [19] define four general areas of the smart home; energy efficiency and management, entertainment, health care and physical security.

HEMS can allow home users to manage, monitor, and act on energy usage within the home. With the increasing prevalence of renewable energy sources within the home such as PV modules and battery storage of energy, these systems can also work together collaboratively in smart neighbourhoods to share energy resources to decrease reliance on the grid and energy suppliers [4]. According to Zhou *et al.* [22], the main functions that should be provided by the HEMS are monitoring, logging, control, alarm, and management. The HEMS infrastructure consists of components including networking, smart meters, a HEMS management centre, and appliances [22]. The HEMS can enable energy reduction through demand response price-based incentives by modifying the usage patterns of schedulable appliances [22], [23].

**TABLE 1. Summary of the valid LoRa modem parameters used for the SX1280 devices for the parameters of SF, BW, and CR.**

| | |
|---|---|
| **Spreading Factor (SF)** | 5, 6, 7, 8, 9, 10, 11, 12 |
| **Bandwidth (BW) KHz** | 203 (200), 406 (400), 812 (800), 1625 (1600) |
| **Code Rate (CR)** | 4/5, 4/6, 4/7, 4/8 |

### C. LoRa AND LoRaWAN

LoRa is an unlicensed band, sub-GHz proprietary Low Power Wide Area Network (LPWAN) technology developed by Semtech [24]. LoRa communicates using a Semtech proprietary physical layer implementation based on a modulation technique known as Chirp Spread Spectrum (CSS) [25]. Developers are free to implement their own media access control mechanisms on top of this Physical layer. A common media access control protocol implementation is LoRaWAN [24]. LoRa contains tunable parameters that have a direct impact on network performance [26]. LoRa's maximum communication range can exceed 10 km [27], [28], [29]. LoRa implementations can reach a maximum data rate of around 27 Kbps [30]. In certain regions and nations, the amount of transmissions allowed per hour is limited by a duty cycle [30]. Not only does LoRa have a substantial range, it is also a robust technology that is resilient to noise [31].

Recently, Semtech released LoRa chipsets that can operate on the 2.4 GHz band through the release of their SX1280 chipset [32], [33]. Like its sub GHz predecessor, it uses a CSS-based modulation and forward error correction to protect from noise, and interference and to generally improve its resilience and robustness [11]. Unlike its sub GHz predecessor, it is not subject to duty cycle limitations and can provide faster data throughput, up to 250 Kbps [34]. It provides tunable parameters such as Spreading Factor (SF), Bandwidth (BW), Forward Error Correction Coding Rate (CR) and transmission power [11].

Increasing the BW will increase the transmission rate while decreasing the communication range [35]. As LoRa is based on CSS, the SF defines the chirp rate [36]. A lower SF increases the chirp rate; this causes a faster transmission rate with a lower communication range [35], [36]. With each increase in SF the chirp rate is halved [36]. Increasing the CR will introduce redundancy into the transmission, improving the resilience while increasing the transmission time [35]. CR is expressed as $k/n$ where $k$ represents the bits of useful data and $n$ represents the bits to be transmitted [37]. $n-k$ will provide the number of redundant bits in a transmission. A summary of the valid parameters for SF, BW, and CR can be seen in Table 1. There is no security implementation built into LoRa. This is entirely up to the network designer.

LoRaWAN is a protocol maintained by the LoRa Alliance; it is designed to run on top of LoRa providing an architecture and media access control functions. The architecture is a star-of-stars topology that uses multiple gateways that bridge the LoRa traffic to a central network server, which in turn

converts the traffic into IP-based traffic [38]. This traffic is then processed by multiple servers such as network servers, join servers, and application servers [38]. LoRaWAN offers three classes of end devices; Class A, Class B, and Class C. Class A devices mostly sleep and can only receive downlink transmissions directly following an uplink transmission, thus using minimal power [38]. Class B uses a schedule to wake and receive downlink messages [38]. Class C is always awake and ready to receive downlink transmissions [38]. Security in LoRaWAN is provided by a symmetric multi-key design with keys protecting network communication, and separate keys protecting application-specific data [39]. Whilst the LoRaWAN protocol is widely used, as the name suggests, it is geared toward WAN communication. Given the architecture design of multiple gateways and backend servers, implementation into the HAN may not be practical. In contrast with LoRaWAN, our research proposes a lightweight LoRa protocol and architecture.

### D. ENCRYPTION AND AUTHENTICATION

Our work makes use of Authenticated Encryption with Associated Data (AEAD) to provide confidentiality, integrity, and authenticity. Not only is the encrypted data protected by such a scheme, the associated unencrypted data such as packet header information that is sent with a given message can be checked for integrity to ensure it has not been modified or tampered with [40]. There are numerous options of AEAD algorithms available, with many being based on AES (Advanced Encryption Standard) [40]. The AEAD algorithm that is used in this study is ChaCha20-Poly1305 [41]. ChaCha20-Poly1305 was chosen due to its proven security [42] and its favourable performance in resource-constrained devices [43].

### E. SECURITY THREATS IN IoT NETWORKS

Our research proposes an authentication scheme for an IoT-based network. It is important to provide some background context into the types of security threats faced by IoT networks. A common and well-established IoT architecture model used to describe and define the components of an IoT network is the Three Layer Architecture [44], [45]. The layers are defined as:

- Perception/Physical Layer - This layer defines the physical capabilities of the IoT network. Sensors are a common component of the perception layer.
- Network Layer - This layer enables device connectivity. The network layer also provides the functionality to enable transmission and processing capabilities.
- Application Layer - The application layer is where the specific application is defined. This layer enables services to be supplied to an end-user.

In Liang and Kim's work [46], security risks were categorised based on the three-layer IoT architecture model. Given that our research is concerned with network architecture design and authentication schemes, we will just focus on attacks classified as ''network layer'' by Liang and Kim. Kominos *et al.* [47] also classified security threats, however, they specifically examined threats related to the HAN. Some noteworthy attacks discussed in these studies [46], [47] are:

1) Man-in-the-middle attack: An attack that allows a third party to eavesdrop and intercept the traffic between two nodes. The attack could be passive or active. An attacker either seeks to change the data in transit (active) or simply capture the data (passive).
2) Spoofing: In a spoofing attack, a message is sent from an attacker to a node with its source address disguised to appear as though it is from a legitimate network participant. This allows an attacker to impersonate a user or another device.
3) Replay attack: This is the act of recording a legitimate message in transit, and then simply retransmitting the message at a later time. This could cause an unwanted or unauthorised action to occur on the destination device.
4) DoS/DDoS (Denial of Service/Distributed Denial of Service) attack: Large amounts of traffic are directed at a particular device with the express purpose of overwhelming the destination. When the destination device is overwhelmed, it is unable to respond to legitimate requests. This malicious traffic can either come from one (DoS) or many (DDoS) nodes. An example of a relevant DoS attack in the HAN would be a jamming attack. This type of attack works by an attacker interrupting wireless transmissions with the introduction of noise at the same frequency that the legitimate devices are communicating.

In Section V, our proposed architecture and authentication scheme will be evaluated against these attacks.

## III. RELATED WORK

In our previous work [48], we evaluated the performance and energy cost of numerous encryption algorithms, running on various microcontrollers to benchmark power consumption, time cost, and energy cost. It was found that the ChaCha family of encryption algorithms performed faster whilst using less energy when compared with AES running in all tested modes. This has influenced the design decision in this study to use ChaCha20-Poly1305 as the AEAD algorithm of choice.

Javed *et al.* [49] outlined important security challenges and design considerations that should be closely examined when designing any IoT network. In their work, they highlighted the importance of authentication mechanisms, key distribution techniques, and device pairing processes. Our work will address these three areas in our proposed LoRa 2.4 GHz based home area network (HAN) network authentication scheme.

Luo *et al.* [50] conducted a study to evaluate the impact of SF and BW on the energy consumption of LoRa 2.4 GHz networks using simulations. The LoRa evaluation conducted in our research does not measure energy consumption. It instead focuses on latency using a practical based experimental approach. They do not consider security in their research.

**TABLE 2. A comparative table showing the security and/or performance focus of the related work against this research.**

| | Luo et al. [50] | Kaur et al. [51] | Schappacher et al. [52] | Our Work |
|---|---|---|---|---|
| Performance | ✓ | ✓ | ✓ | ✓ |
| Security | ✗ | ✗ | ✗ | ✓ |

Kaur *et al.* [51] performed some experimental measurements of LoRa in an indoor environment. Like our work, experiments were conducted to measure reliability through packet delivery. Unlike our research, Kaur *et al.* [51] conduct experiments using the original sub-GHz LoRa. They do not examine security in their work.

Schappacher *et al.* [52] implemented a LoRa 2.4 GHz based network using a combination of LoRaWAN and time-slotted channel hopping. Performance tests were carried out indoors in a university campus environment. Being LoRaWAN based, the study uses several gateways and backend servers. As the focus is solely on performance, there is no mention of security. Our study differs in that we seek to design a system that can be implemented into a HAN environment without the overhead of LoRaWAN. We also are focusing on both security and performance.

Due to the relatively short time since the release of these chipsets and availability in the market, there is a research gap, with only limited studies evaluating the technology, and none in the specific use case of the HAN. Further to this, security is not considered in any of these studies. The main advantage of our research is to address this gap by examining the LoRa 2.4 GHz technology and by proposing a network architecture design and secure authentication scheme, backed by a security and performance evaluation. Through our work, we are providing an innovative and lightweight protocol that is suitable for the HAN. As LoRaWAN is targeted at wide area networks, 2.4 GHz support is not in the specification [53]. While several studies focus on the performance of LoRa, our work focuses on both the security, and the performance aspects, and the relationship between them. This is further highlighted through a comparison of the previous work in Table 2.

## IV. NETWORK ARCHITECTURE DESIGN

The presented architecture design and authentication scheme can be seen in Figure 1. At the time of writing, no such authentication schemes or architecture designs currently exist for LoRa 2.4 GHz networks, and there is no research on the use of LoRa 2.4 GHz in a HAN environment. In our architecture, there is an authenticator application on a smartphone or tablet, one HAN Controller and $n$ appliances. There are two networks, the Home Wi-Fi network, and the LoRa 2.4 GHz based HAN (LoRaHAN). The Wi-Fi network is used by both the HAN Controller, and the authenticator application for:

1) Pairing a new appliance to the HAN. In this case, the device ID ($A$) along with the device's initial key (IK) must be communicated to the HAN Controller ($H$) via our proposed LoRaAuth protocol (discussed in greater detail in Section IV-C). Each appliance must be pre-configured with an IK.
2) Updating an appliance's long-term key ($K$). In this case, $A_n$ must be communicated to $H$.

The HAN Controller and the appliances operate on a LoRa 2.4 GHz based network. All communications in the HAN are secured and authenticated using a symmetric key-based ChaCha-Poly1305 AEAD scheme. Initially, before pairing has occurred between a given appliance ($A$) and the HAN Controller ($H$), $A$ only has an Initial Key (IK). Using a pairing process which will be covered in detail later in this paper, the Authenticator Application communicates the device ID $A$ and the IK to the HAN Controller. For example, in the case of appliance $A_1$, the following occurs:

1) $H$ sends a pairing request to $A_1$ encrypted and tagged using $\text{IK}_1$.
2) $H$ generates a long-term key $K_1$ and communicates it to $A_1$ encrypted and tagged using $\text{IK}_1$.
3) $A_1$ responds with a message encrypted and tagged using $K_1$ to confirm the successful pairing.
4) $H$ can now discard $\text{IK}_1$ as this key will no longer be used. $A_1$ will continue to store $\text{IK}_1$ to be used in the case of future un-pairing and re-pairing.
5) A session key establishment process then takes place between $H$ and $A_1$ to negotiate $\text{SK}_1$.
6) $\text{SK}_1$ can now be used to encrypt and tag communications between $H$ and $A_1$ for the duration of the session. In this paper, a session is defined as 24 hours. If this architecture was applied to a scenario with greater security requirements, this period could be shortened.
7) Once the session has ended, $A_1$ and $H$ can re-negotiate the session key using the long-term key $K_1$ to secure and tag messages that are exchanged during the process.

In the case of an already paired appliance $A_1$, a user may want to update $K_1$. As $K_1$ is already known to both $H$ and $A_1$, there is no need to communicate $\text{IK}_1$ to the HAN Controller. The rest of this process can continue in the same fashion as the initial pairing process discussed above. Appliances in this design do not share any keys, long-term or otherwise. This prevents them from directly communicating. In the case an appliance needs to send a message to another appliance, this can be forwarded by the HAN Controller. The communication between any appliance $A$ and $H$ is in a request-response style, which can be initiated from either $A$ or $H$.

Many components come together to enable the HAN to function. Our proposed architecture design is mainly focused on components from the physical layer (layer 1), the data-link layer (layer 2) and the network layer (layer 3) of the commonly understood 7 layers OSI (Open Systems Interconnection) model [12]. The application layer (layer 7) is only discussed in the context of the Authenticator Application. This allows our proposed architecture design to manage the lower layers of communication for many potential applications. The remainder of this section will discuss the physical components required for the architecture, the Authenticator Application, the structure of packets, the proposed network protocols, and key management.

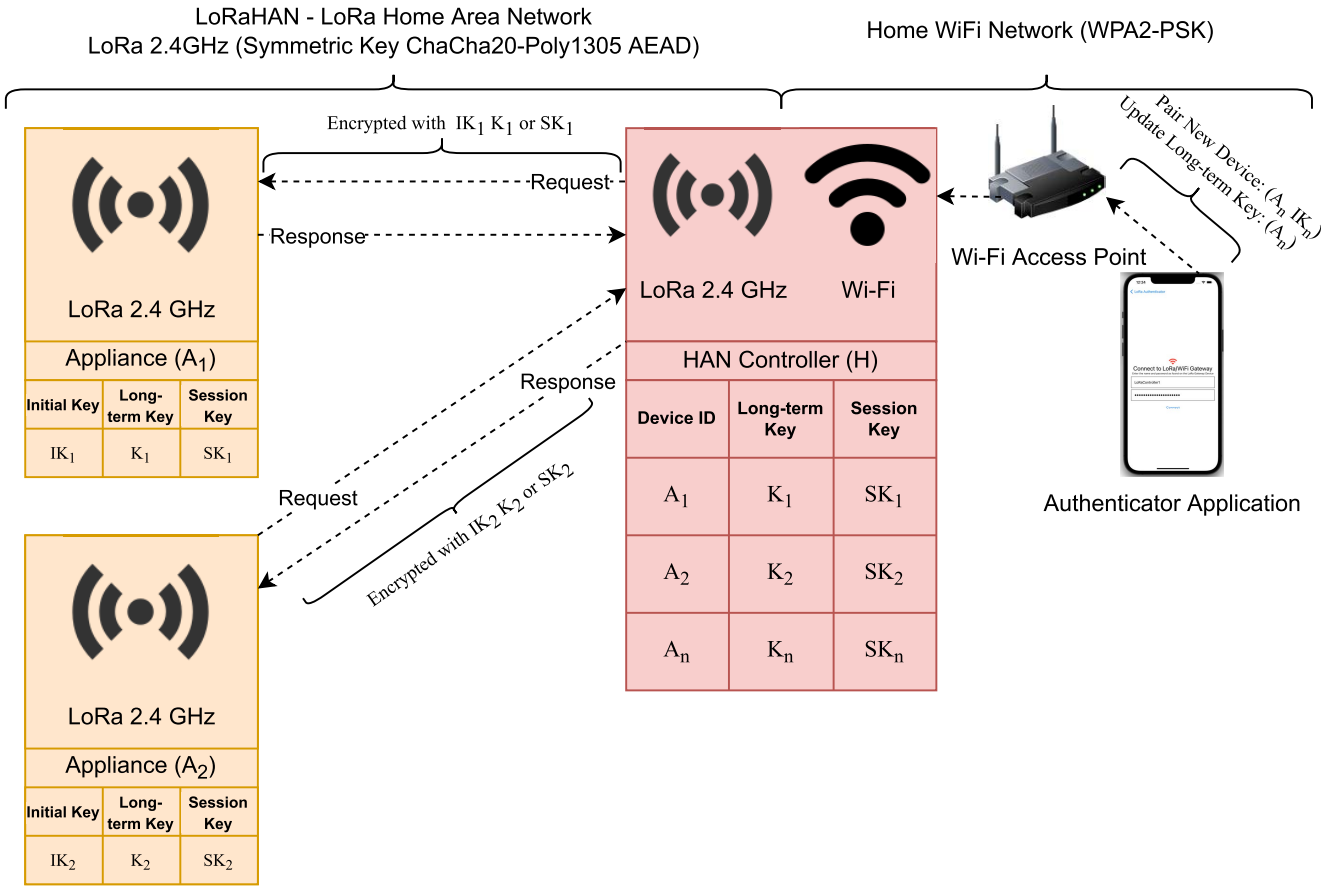


**FIGURE 1.** Network architecture design of the LoRa HAN showing the participants, and certain aspects of the key management process.

### A. HARDWARE

Our architecture design is based upon several physical hardware components. These components form the foundation of the design, upon which all other aspects are based upon. The required physical components are:

1) A HAN Controller. This controller connects to the LoRa 2.4 GHz appliances and the Home Wi-Fi access point. This device can be a lost-cost, low-powered microcontroller with an appropriate power supply. It is required to have both a LoRa 2.4 GHz SX1280 transceiver and a Wi-Fi transceiver.
2) Appliances are required and must contain a microcontroller. The microcontroller can be simple and low-powered. A LoRa 2.4 GHz SX1280 transceiver is required to be connected to the microcontroller to enable network access.
3) A home Wi-Fi access point is required to facilitate communications from the user to the HAN, and key management functions. This device should support, at a minimum, the WPA2 standard.
4) A smartphone or tablet device. This device will run the Authenticator Application, providing the user with an interface to the HAN. This function could also be achieved by hosting a web application on the HAN Controller and accessing it from a web browser on any PC. The implementation of this is left up to the network designer, depending on the individual requirements.

### B. SOFTWARE

The three main software components include the HAN Controller software, the Authenticator Application, and the appliance software. This section will cover the requirements that should be implemented into the software of each of these three components. This is not an exhaustive list of requirements, and a network designer may implement additional application-specific requirements.

The HAN Controller software is responsible for all operations of the HAN Controller. It functions as the central point to facilitate communication between the appliances and the Authenticator Application. The HAN Controller is a bridge between the Home Wi-Fi network and the LoRaHAN network. It communicates directly to each appliance in a one-to-one manner via the LoRaHAN protocol. The HAN Controller, at a minimum, has the following main functions that must be implemented in the software:

1) An implementation of the LoRaHAN protocol.
2) An implementation of the LoRaAuth protocol.

3) The ability to receive and send communication to the appliances on the LoRaHAN network.
4) The ability to receive and reply to communications sent from the Authenticator Application via the Wi-Fi network.
5) A mapping scheme to associate the appliance identifier $A$ with its corresponding keys $K$ and SK.

The Appliance software is responsible for the operation of each appliance. Each appliance can communicate with its paired HAN Controller only via the LoRaHAN network. As each appliance can only maintain one IK, $K$, and SK, the appliance can't communicate with other non-paired controllers or any other device or appliance. At a minimum, the appliance software should support the following features and functions:

1) An implementation of the LoRaHAN protocol.
2) The ability to receive commands and requests from the HAN Controller and send an appropriate response.

The Authenticator Application provides an interface to allow a user to securely pair an appliance with the controller. It can be run on a smartphone or tablet device. It works by connecting via Wi-Fi to the HAN Controller. Once connected, the user can utilise authentication-related functions such as pairing a new appliance to the network, and changing the key $K$ of an existing appliance. There should be some authentication mechanism between the user, the application, and the HAN controller, such as a username and password. There are many well-understood ways to accomplish this. Security across a Wi-Fi network is not the focus of this study, and the implementation of such a scheme is left up to the network designer according to their specific requirements.

### C. PROTOCOLS

There are two separate networks in this architecture design. There is the main network that allows the HAN Controller and the appliances to communicate using LoRa 2.4 GHz, and there is also a Wi-Fi network that allows the Authenticator Application to provide security services and functions to the controller. Both of these networks must follow protocols to ensure they are functioning as required, and can securely authenticate. These networks also must work together to facilitate the initial key distribution between a HAN Controller and an appliance, and provide a way to update long-term keys. In our work, we propose two new protocols. The LoRa 2.4 GHz section of the architecture will be subject to the LoRaHAN protocol, while the network between the HAN Controller and the Authenticator Application will be subject to the LoRaAuth protocol. There are some requirements that the devices need to comply with to participate in this architecture:

1) An appliance must be configured with an initial 256-bit key IK. This key will be used in the initial device pairing process.
2) Appliances must be configured with a device ID $A$. This ID is used as an address to uniquely identify a device operating in the Home Area Network. As the LoRaHAN network is not IP based, this ID will serve as its unique identifier. In our proposal, we have defined a device ID to be represented by a 5-byte string. This could be customised if required by a network designer.

The Authenticator Application and HAN Controller communicate with IP-based communication that utilises the UDP protocol at the transport layer. Encapsulated inside this UDP datagram's payload is a lightweight data structure containing two fields, which form the LoRaAuth packet ($P$); a Control Code field ($C$) and a payload field ($Y$). These fields are the underlying packet data structure for the LoRaAuth protocol. The control code field is used to indicate the type of action the recipient device is to perform or to define the contents of the data in the payload. The payload is used to carry any additional or supporting data, such as encryption keys or device IDs. The structure can be seen in Figure 2. The general format of a LoRaAuth packet is represented in Equation (1). For example, to pair a new device $A_n$, its initial key ($\mathrm{IK}_n$) must be sent to the HAN Controller. The payload will appear as in Equation (2). A summary of the accepted control codes, as well as their payload requirements, and formatting requirements can be seen in Table 3.

$$P = C||Y \tag{1}$$

$$Y = A_n||\mathrm{IK}_n \tag{2}$$

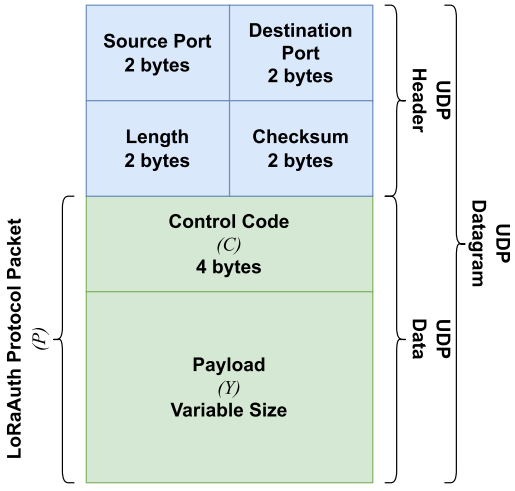


**FIGURE 2.** LoRaAuth protocol packet structure.

LoRa only provides the physical layer implementation and modulation. Network designers are free to implement higher-layer protocols that can be built on top of LoRa. At the time of writing, LoRa 2.4 GHz networks are relatively new, and as such, minimal higher layer implementations currently exist. The LoRaHAN protocol is designed to fill this gap by providing a secure communications protocol, specifically aimed at the HAN. As is seen in the previously presented network architecture design in Figure 1, the LoRaHAN network is used between the HAN Controller and the appliances.

The LoRaHAN protocol uses authenticated encryption with associated data (AEAD) to provide confidentiality

**TABLE 3. Summary of the accepted LoRaAuth control codes $C$, their purpose, and their associated payload requirements.**

| ($C$) | Control Code Purpose | Payload ($Y$) |
|---|---|---|
| NEWK | Transmit a new encryption key, for pairing a previously unpaired appliance to the HAN Controller. | The payload $Y$ is required to contain the device ID $A$ of the new appliance to be paired, as well as the 256-bit symmetric encryption key IK that will be used to pair the HAN Controller and the appliance. For example, to pair a new device D1234 with the key 5v8yxBxEfH1Mb-QeShVmYq3t6w9zECzFz the LoRaAuth packet sent from the Authenticator Application to the HAN Controller would be: NEWKD12345v8yxBxEfH1Mb-QeShVmYq3t6w9zECzFz |
| UPDK | Generate a new encryption key for an appliance that is currently paired with the HAN Controller. | The payload is required to contain the device ID $A$ of the previously paired appliance. For example, to update the key of an appliance with the device ID of D4576, the LoRaAuth packet sent from the Authenticator Application to the HAN Controller would be: UPDKD4576 |
| CONF | Confirms if an action was successful or not. | No payload. |
| FAIL | Confirms that an action was unsuccessful. | No payload. |

through encryption and message integrity. Specifically, it uses ChaCha20-Poly1305 in a combined mode to provide this, as defined in RFC 8439 [41]. Unique to each appliance/controller pair, is a shared long-term key $K$. The long-term key is used to encrypt and decrypt messages between the pair to provide confidentiality and message integrity during the session key negotiation process. Session keys are then used for all ongoing communications for the remainder of the session.

LoRaHAN packets must be structured following the packet structure diagram as seen in Figure 3. The fields that are present in the packet include source and destination addresses, nonce, command, and optionally, additional data. The authentication tag is then appended to the end of the packet before transmission.

The addressing, as seen in the blue layer in Figure3 is used to ensure that the transmission's source and destination can be identified. This ensures a functional network and provides the ability for devices to be able to communicate effectively. It is important to note that the address fields do not undergo encryption, to ensure other nodes that may receive this traffic do not consume resources trying to decrypt traffic that is not addressed to them. The addresses form part of the associated data, which is authenticated by the tag. Any attempt to alter the addresses will result in the authentication tag being invalid once it is verified at the receiving end. The nonce must be unique for each transmission that is encrypted with a given key. In LoRaHAN the nonce increments on each message doubling as a counter. If on the receiving end, a repeated nonce is seen, this packet will be discarded. This assists in the mitigation of replay attacks.

In the purple layer of the packet structure is the command field. This field defines the type of transmission that the packet contains, and the action that is expected from the receiving device. The commands that were used in this work, along with their meanings, are:

- PAIRK - The HAN Controller sends this message to pair a new appliance with the HAN Controller.
- ACKNW - Acknowledge the receipt of a message.
- READY - The appliance is ready to receive an encryption key from the HAN controller.
- NEWKY - The HAN Controller is supplying a new key long-term key to an appliance.
- SKEY1 - Sent from the HAN Controller to an appliance to initiate a new session key agreement process
- SKEY2 - The second stage of the session key agreement process. Sent from an appliance to the HAN Controller in response to a SKEY1 message.
- SKEY3 - This is the final message sent in the key agreement process. It is sent from the HAN Controller to an appliance in response to a SKEY2 message.

We will look at the specific key management processes and algorithms later in this section; this will put these commands into context. The additional data field is used to supply any additional data that needs to accompany the transmission, such as encryption keys and device IDs.

In the orange layer is the authentication tag. This tag is used to provide message integrity. Any attempt to alter the command, additional data, or the addresses will result in the tag being invalid when validation is performed by the receiver. If this occurs, the packet is discarded.

Devices that participate in the LoRaHAN protocol must comply with the following:

1) Session keys should be used to encrypt messages. The long-term key should only be used to encrypt and decrypt messages during the session key negotiation process. The initial key should only be used to encrypt and decrypt messages during an initial appliance pairing.
2) Appliances can not communicate in a peer-to-peer manner. All communication in LoRaHAN occurs between the appliance and the controller.
3) There must be a unique long-term key used between the controller and each appliance. A key must not be shared between appliances.

### D. KEY MANAGEMENT

In our discussion of the architecture and the protocols so far, we have described the roles of the various keys among the numerous participants of the architecture. This section

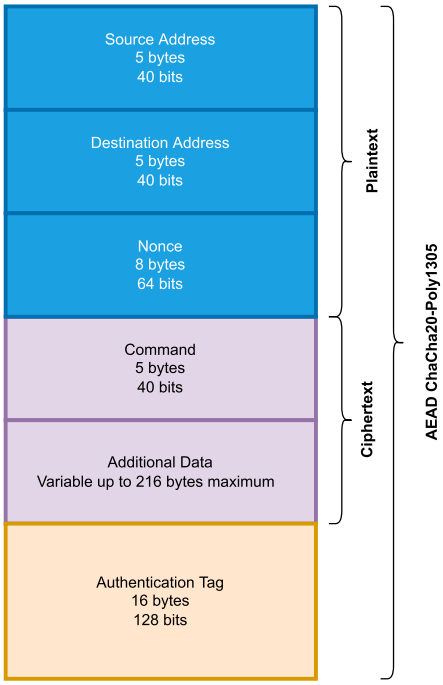


**FIGURE 3.** Structure of the LoRaHAN protocol packet.

provides more specific details on relevant key management processes. Topics that are covered include key generation, distribution, rollover, and revocation. This section presents important processes that are essential to the key management of the network. These processes are presented via several sequence diagrams. These diagrams show the core participants, as well as the flow of messages that are core to the key management processes. The algorithms that drive the session key agreement process are then presented. To prevent the risk of any of the keys being extracted from any of the participating devices, it is recommended that the keys be stored inside a tamper-resistant element.

#### 1) AUTHENTICATOR APPLICATION LOGIN

Before any key management processes can occur, the user must log in to the Authenticator Application. This process authenticates the user, the Authenticator Application, and then HAN Controller. The user opens the Authenticator Application and provides a preconfigured username and password. This is then sent from the application to the HAN Controller via the LoRaAuth protocol for authentication. Once authenticated, further actions such as device pairing and other key management tasks can occur. A sequence diagram for this process can be seen in Figure 4. As previously mentioned, the specific security mechanisms for encryption between devices participating in the Wi-Fi network are not defined by this study and are left up to developer implementation.

#### 2) DEVICE PAIRING, INITIAL KEY DISTRIBUTION, AND LONG-TERM KEY ESTABLISHMENT

The device pairing process is an important component of the HAN network design. As mentioned earlier in this section, each appliance must be preconfigured with IK and $A$. The pairing process authenticates the appliance with the HAN Controller by establishing a common long-term symmetric key. This key can then be used for secure authentication, as well as the basis for establishing an agreed session key. This pairing process is aided by the Authenticator Application.

Once the user has made an initial connection to the controller using the application, several steps must take place to successfully pair an appliance with the HAN Controller:

- The user first needs to activate the device pairing mode and provide the device ID and the Initial Key of the appliance that will be paired with the HAN Controller.
- The Authenticator Application sends the Device ID and the Initial Key to the HAN Controller.
- The HAN Controller sends a pairing request to the appliance, encrypted with the Initial Key.
- The appliance then acknowledges the pairing request.
- The HAN Controller will then generate a new long-term key to be used for future communications.
- The HAN Controller then sends the new key through to the device, encrypted with the Initial key.
- The appliance will then save the long-term key, and send an acknowledgement message back to the HAN Controller.

After the process, a long-term key is established that only the two participating devices are aware of. A sequence diagram of the device pairing process can be seen in Figure 5. Once this process has been completed, the session key agreement must then occur. This process will be discussed later in this section.

#### 3) LONG-TERM KEY ROLLOVER AND REVOCATION

The long-term key can be updated by the user through the use of the Authenticator Application if required. The user needs only provide the application with the ID of the appliance that requires a new key to be issued. This process shares similarities with the initial pairing process, however, it does not require the transmission of the existing/initial key as is the case in the pairing process.

The full process for updating an appliance's key can be seen in Figure 6. The new long-term key replaces the existing long-term key that was stored by the appliance and the controller. As the previous key has not been retained by either party, it is hence revoked. Following the long-term key update, a new session key must then be established.

#### 4) SESSION KEY ESTABLISHMENT

Once a long-term key has been established between the HAN Controller and an appliance, a session key should be established for ongoing communication. The key establishment mechanism that we have integrated into the LoRaHAN protocol is based on the ISO/IEC 11770-2 Key Establishment Mechanism 6 [54], which in turn is based on the ISO/IEC 9798-2 three-pass mutual authentication mechanism [55]. This mechanism includes a three-way exchange of various

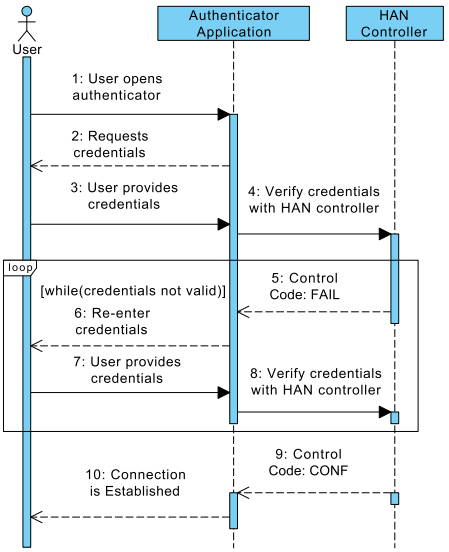


**FIGURE 4.** A sequence diagram showing the process for establishing a connection between the user, the Authenticator Application, and HAN Controller.

nonces between the two participating nodes, as seen in Figure 7. These three messages: SKEY1, SKEY2, and SKEY3 should be encrypted with the long-term key that the HAN Controller and the appliance share. This section will explain each step of the figure in detail, and define the algorithms used in the key agreement process.

The first message sent in the three-way exchange is from the HAN Controller to the appliance. Each field of the LoRaHAN packet should be populated as follows:

1) **Source Address:** The 5-byte address of the HAN Controller.
2) **Destination Address:** The 5-byte address of the appliance.
3) **Nonce:** An 8-byte number that has never been used before with the long-term key.
4) **Authentication Tag:** A 16 byte tag generated by ChaCha20-Poly1305 AEAD. The authenticated data used in the tag generation should be the "Source Address" and "Destination Address" fields. The data that will be encrypted by the algorithm will be the "Command" and "Additional Data" fields.
5) **Command:** The command that is sent should be "SKEY1".
6) **Additional Data:** $R_B$ should be contained in this field. $R_B$ is simply a random 32-byte number generated by the HAN Controller. Refer to Algorithm 1 for details on how the additional data field is generated.

Once the first message is received from the HAN Controller by the appliance, it must be processed and a response message sent. Refer to Algorithm 2 for further details on the SKEY1 validation process, as well as the SKEY2 Additional Data field generation. The second message in the three-way exchange is sent from the appliance to the HAN Controller.

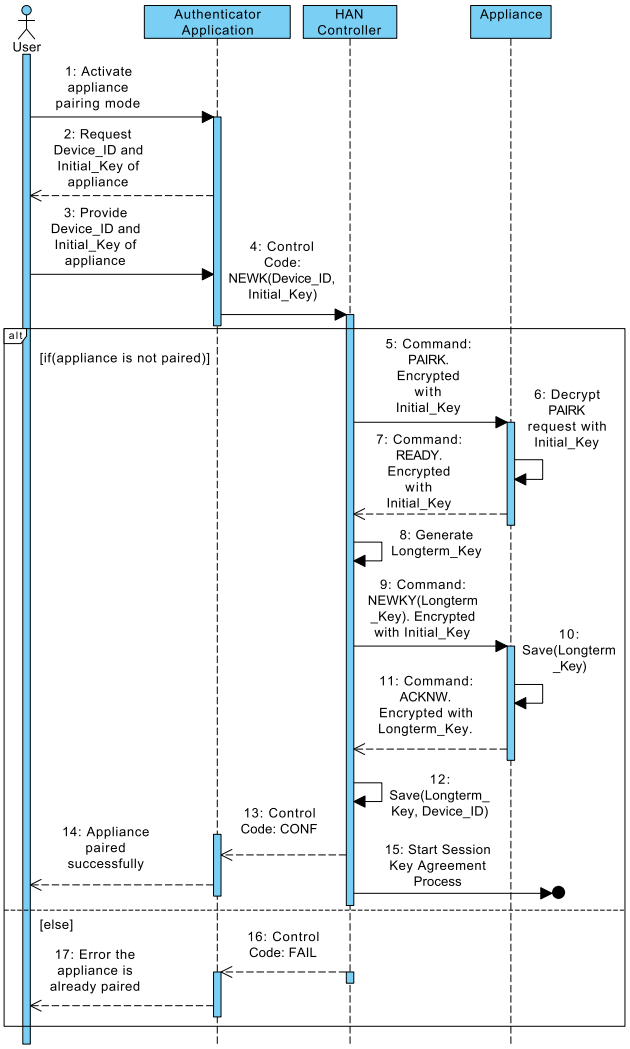


**FIGURE 5.** A sequence diagram showing the process for pairing a new appliance with the HAN Controller.

**Algorithm 1** SKEY1 Message Generation

1: $R_B \leftarrow \{0,1\}^{256}$ {randomly generated 32 byte number}
2: $\text{Stored}_{\text{RB}} \leftarrow R_B$ {saved for later use}
3: $\text{Message}_{\text{TX}} \leftarrow$ "SKEY1"$||R_B$
4: **return** $\text{Message}_{\text{TX}}$ {ready for encryption, tagging, and transmission}

The fields of the LoRaHAN packet should be populated as follows:

1) **Source Address:** The 5-byte address of the appliance.
2) **Destination Address:** The 5-byte address of the HAN Controller.
3) **Nonce:** An 8-byte number that has never been used before with the long-term key.
4) **Authentication Tag:** A 16 byte tag generated by ChaCha20-Poly1305 AEAD. The authenticated data used in the tag generation should be the "Source Address" and "Destination Address" fields. The data

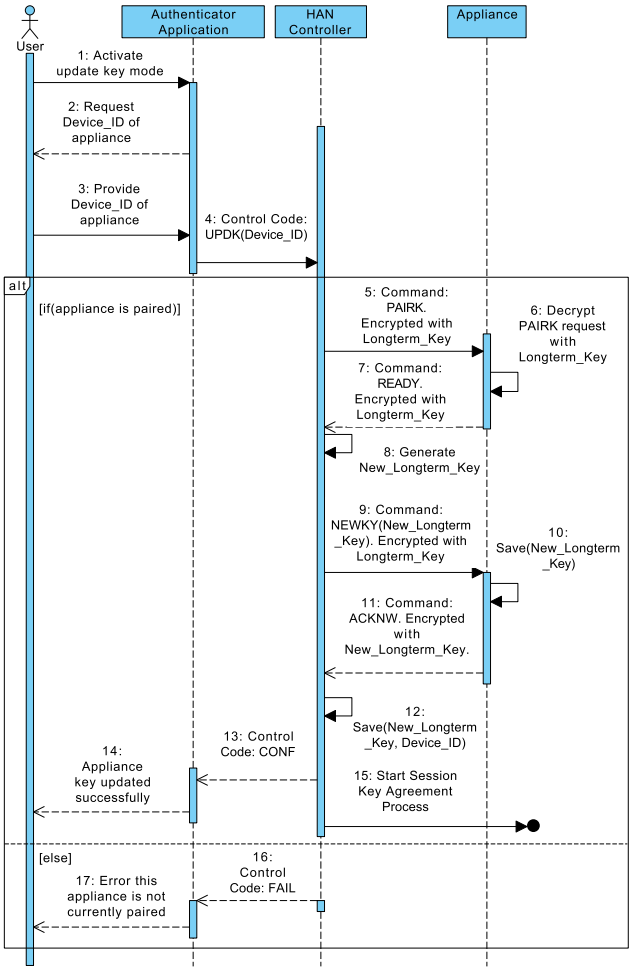


**FIGURE 6.** A sequence diagram showing the process for updating an appliance key with the HAN Controller.

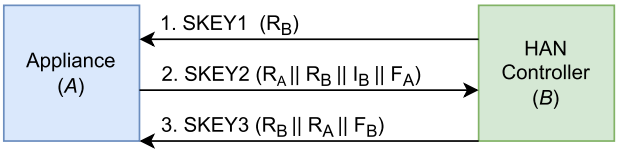


**FIGURE 7.** The three-way nonce exchange process for session key establishment between two nodes. The diagram is a customised version based on key establishment mechanism 6 from ISO/IEC 11770-2 [54].

that will be encrypted by the algorithm will be the "Command" and "Additional Data" fields.

5) **Command:** The command that is sent should be "SKEY2".
6) **Additional Data:** Four values are to be included in the additional data, appended together. The first value is $R_A$ which is a random 32-byte number generated by the appliance. Appended to this is $R_B$, which was the 32-byte number received by the appliance in the first message. Then follows $I_B$, which is the source address of message 1 (the HAN Controller). $F_A$ should then be appended; it is another 32-byte random number generated by the appliance.

**Algorithm 2** SKEY1 Message Validation and SKEY2 Response

**Require:**
$\text{Message}_{\text{RX}} =$ "SKEY1"$||R_B$ {$\text{Message}_{\text{TX}}$ from Alg. 1}
$I_B$ {the device ID of the HAN Controller}

$\text{Stored}_{\text{RB}} \leftarrow R_B$
$\text{Stored}_{\text{IB}} \leftarrow I_B$
$R_A \leftarrow \{0,1\}^{256}$
$F_A \leftarrow \{0,1\}^{256}$
$\text{Stored}_{\text{RA}} \leftarrow R_A$
$\text{Stored}_{\text{FA}} \leftarrow F_A$
$\text{Message}_{\text{TX}} \leftarrow$ "SKEY2"$||R_A||R_B||I_B||F_A$
**return** $\text{Message}_{\text{TX}}$

Once the SKEY2 message is received and validated by the HAN Controller, The final message in the three-way exchange is sent from the HAN Controller to the appliance. For further details on the SKEY2 validation, and the SKEY3 generation process, please refer to Algorithm 3. The LoRaHAN packet should be populated as follows:

1) **Source Address:** The 5-byte address of the HAN Controller.
2) **Destination Address:** The 5-byte address of the appliance.
3) **Nonce:** An 8-byte number that has never been used before with the long-term key.
4) **Authentication Tag:** A 16 byte tag generated by ChaCha20-Poly1305 AEAD. The authenticated data used in the tag generation should be the "Source Address" and "Destination Address" fields. The data that will be encrypted by the algorithm will be the "Command" and "Additional Data" fields.
5) **Command:** The command that is sent should be "SKEY3".
6) **Additional Data:** $R_B$ followed by $R_A$, and a new 32 byte random number generated by the HAN Controller $F_B$.

Lastly, the SKEY3 message must be validated by the appliance. For further details on the validation process, please refer to Algorithm 4.

Once the final validation process has succeeded, two final processes must occur to generate the session key so that encrypted and authenticated communication can occur between the HAN Controller and the appliance. First, a key extraction function (KTF) must be applied, followed by a key expansion function (KPF). The requirements in the ISO/IEC 11770-2 standard [54] state that a two-step key derivation function should be used from the ISO/IEC 11770-6:2016 standard [56].

For the KTF, the 'key extraction function 1' (KTF1) from ISO/IEC 11770-6:2016 [56] standard has been used in this design. The design can be seen in Algorithm 5. To remain compliant with the standard, the following requirements have been met by this protocol:

**Algorithm 3** SKEY2 Message Validation and SKEY3 Response

**Require:**
Message$_{RX}$ = "SKEY2"$||R_A||R_B||I_B||F_A$
{Message$_{TX}$ from Alg. 2}
Stored$_{RB}$ {from Alg. 1}
DeviceID {The address of this HAN Controller}

**if** ($I_B$ = DeviceID) **and** ($R_B$ = Stored$_{RB}$) **then**
  $F_B \leftarrow \{0,1\}^{256}$
  Stored$_{FB} \leftarrow F_B$
  Stored$_{RA} \leftarrow R_A$
  Stored$_{IB} \leftarrow I_B$
  Stored$_{FA} \leftarrow F_A$
  Message$_{TX}$ ← "SKEY3"$||R_B||R_A||F_B$
  **return** Message$_{TX}$
**else**
  **return** ERROR {terminate session key establishment process}
**end if**

**Algorithm 4** SKEY3 Message Validation

**Require:**
Message$_{RX}$ = "SKEY3"$||R_B||R_A||F_B$ {Message$_{TX}$ from Alg. 3}
Stored$_{RB}$ {from Alg. 2}
Stored$_{RA}$ {from Alg. 2}

**if** ($R_B$ = Stored$_{RB}$) **and** ($R_A$ = Stored$_{RA}$) **then**
  Stored$_{FB} \leftarrow F_B$
  **return** SUCCESS
**else**
  **return** ERROR {terminate session key establishment process}
**end if**

1) The HAN Controller and the appliance will both use KTF1.
2) The target key length on both devices is 256 bits.
3) The Message Authentication Code (MAC) function that is used by both devices to implement KTF1 is HMAC-SHA3-256 and is compliant with ISO/IEC 9797-2:2021 [57].
4) Both of the devices are using the same salt value ($t$) in this design. The value is a constant known by both devices. This salt value is used as the key to the KTF.
5) Both devices already have $F_A$ and $F_B$ from the three-way nonce exchange process as seen in Figure 7. These values will be used as the secret input to the KTF, which fulfils the requirement in ISO/IEC 11770-2:2016 [54].

Once the KTF has been executed, the output data must be passed to the KPF. The KPF that has been used in this design is the 'key expansion function 1' (KPF1) from ISO/IEC 11770-6:2016 [56]. To remain compliant with the standard, the following requirements have been met by this protocol:

**Algorithm 5** Key Extraction Function

**Require:**
KTF {a SHA3-256 object}
$t$ {a 32-byte constant value known by both parties that does not need to be secret}
$F_A$
$F_B$

KTF.key ← $t$
KTF.data ← $F_A||F_B$
KTFOuptut ← KTF.execute() {execute the HMAC algorithm with the key and data}

1) The HAN Controller and the appliance will both use KPF1.
2) The MAC function that is used by both devices to implement KPF1 is HMAC-SHA3-256 and is compliant with ISO/IEC 9797-2:2021 [57].
3) The requirement for another counter to be included in the encoding is unnecessary, as only one key will be derived from this process. If an implementation requires multiple keys to be generated at once, then this should be implemented.
4) The target key length on both devices is 256 bits.
5) The salt value ($t$) that will be used as the data in the function should be known to both devices. In compliance with ISO/IEC 11770-2:2018 [54], this should be $t = R_A||R_B||I_B$.

**Algorithm 6** Key Expansion Function

**Require:**
KPF {a SHA3-256 object}
$t = R_A||R_B||I_B$
KTFOutput {the output from the key extraction process}

KPF.key ← KTFOutput
KPF.data ← $t$
KPFOutput ← KPF.execute() {execute the HMAC algorithm with the key and data}
SessionKey ← KPFOutput

## V. EVALUATION

This section will first discuss how the authentication scheme proposed in our research addresses the attacks that were previously discussed in Section II. Following this, the method and results of experiments that were conducted to measure the impact of our proposed security mechanisms on the IoT network performance will then be discussed.

### A. SECURITY EVALUATION

In Section II, relevant security threats and attacks were identified from the literature, listed, and briefly defined. In this section, we will discuss how the proposed authentication scheme addresses them.

#### 1) MAN IN THE MIDDLE ATTACK

Our proposed authentication scheme protects against man-in-the-middle attacks. Each appliance shares a unique long-term key with the HAN controller. This long-term key is used to negotiate temporary session keys that are used to secure communications between them for a session. As long as the long-term key remains secret, the risk of a man-in-the-middle style attack remains extremely unlikely. It is important to ensure the initial key exchange process remains secure. As discussed in Section IV, it is left up to the network designer to ensure that the communication between the HAN controller and the Authenticator Application is encrypted in any implementation.

#### 2) SPOOFING

A device is unable to impersonate another device in our proposed authentication scheme. During the initial pairing process, the HAN controller records the device ID, the long-term key, and the session key of any given device. When a communication is sent between the HAN Controller and an appliance, the communication is encrypted, so it is unreadable to a third party without the appropriate key. In addition to this fact, the unencrypted fields of the packet header are authenticated using ChaCha20-Poly1305 AEAD as discussed in Section IV. If any change were to occur in any part of the transmission, including the source address, the tag would not be validated by the receiver. The malicious packet would be detected and discarded.

#### 3) REPLAY ATTACK

A message can not be replayed by an attacker, as the nonce present in the packet also acts as a counter. The nonce increments with each message and is unique for a given key. If an attempted replay attack were to occur, the receiver would see the repeated nonce, and discard the packet. If an attacker captures a packet, increments the nonce and attempts retransmission, the tag would be invalid. This is because the nonce forms part of the associated data in the AEAD scheme. The malicious packet would be detected and discarded.

#### 4) DDoS/DoS/JAMMING ATTACK

Our work does not specifically address DDoS/DoS/Jamming attacks. LoRa operates across a wide variety of SFs and BWs. Parity data can also be included with a message via the CR. A frequency hopping mechanism could be implemented to counteract these attacks. This was out of the scope of this research.

### B. NETWORK PERFORMANCE EVALUATION

A prototype network was constructed to design and test the key distribution and key agreement systems, as well as to conduct performance measurements to determine the impact that our proposed security mechanisms would have on network performance. The prototype network consists of two LoRa 2.4 GHz devices which contain the SX1280 LoRa transceiver manufactured by Semtech [11] and are powered by an ESP32 microcontroller [58]. Device one acts as a controller, whilst device two acts as an appliance. The ESP32 microcontroller has a built-in Wi-Fi radio, which is only used on the controller device. The device acting as the home Wi-Fi router was a Linksys EA8500 running OpenWrt 21.02.0 custom firmware. The LoRaAuth application was running on an iPhone 13 Pro smartphone running iOS 15.1. Each of the LoRa devices was programmed with the Visual Studio Code software with the PlatformIO extension installed on a Mac computer. External libraries were used to implement the LoRa communications [59] and the cryptographic functions [60]. An implementation of the Authenticator Application was created For the iPhone. It was programmed using the same computer running Xcode 13.3.1. The library that was used to provide the network services was the Network Framework [61].

The first set of performance measurement tests was designed to capture the average time taken to send LoRa packets from the HAN Controller to the appliance. All possible combinations of SFs, BWs, and CRs were measured. The test bench was set up as seen in Figure 8 with the HAN Controller and the appliance both connected to an Arduino Uno device. When the HAN Controller device started the communication process, it set a pin to HIGH. When the appliance device received and processed the packet, it set a pin to HIGH. The Arduino device was used to measure the time between these two events, which was then output to the serial monitor on the PC. The algorithm that was implemented on the Arduino device to conduct this testing can be seen in Algorithm 7.

**Algorithm 7** Measurement of LoRa Transmission Time Between Two Devices

```
startPin ← 2
endPin ← 3
pinMode(startPin, INPUT)
pinMode(endPin, INPUT)
while 1 do
    while digitalRead(startPin) ≠ 1 do
        {do nothing and wait for the start pin to pull up high}
    end while
    startTime ← micros()
    while digitalRead(endPin) ≠ 1 do
        {do nothing and wait for the end pin to pull up high}
    end while
    endTime ← micros()
    totalTime ← endTime − startTime
    Serial.println(totalTime)
    while digitalRead(startPin) = 1 or digitalRead(endPin) = 1 do
        {do nothing and wait until both pins are reset to the low state}
    end while
end while
```

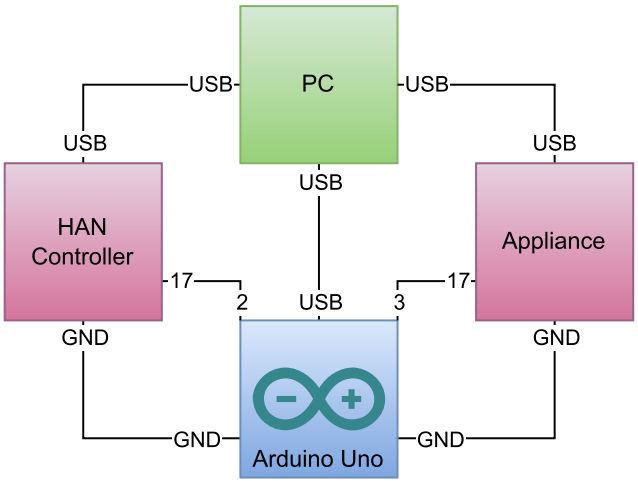


**FIGURE 8.** The test bench was used to measure the total processing and transmission time between the HAN Controller and the appliance devices. The numbers indicate the relevant pins on each of the devices.

**TABLE 4.** The total average processing and transmission time (ms) required to send a 39-byte LoRaHAN packet with no encryption or tagging from the HAN Controller to an appliance device for all BWs, SFs, and CRs.

| BW (kHz) | CR | SF5 | SF6 | SF7 | SF8 | SF9 | SF10 | SF11 | SF12 |
|---|---|---|---|---|---|---|---|---|---|
| 200 | 4/8 | 26.31 | 44.43 | 76.90 | 143.00 | 245.31 | 449.85 | 980.06 | 1799.32 |
| | 4/7 | 23.62 | 40.01 | 69.33 | 129.13 | 222.61 | 409.49 | 889.29 | 1637.96 |
| | 4/6 | 20.94 | 35.59 | 61.75 | 115.26 | 199.90 | 369.13 | 798.52 | 1476.60 |
| | 4/5 | 18.25 | 31.17 | 54.18 | 101.40 | 177.19 | 328.77 | 707.75 | 1315.24 |
| 400 | 4/8 | 13.46 | 22.52 | 38.76 | 71.81 | 122.97 | 225.23 | 490.34 | 899.97 |
| | 4/7 | 12.12 | 20.31 | 34.97 | 64.87 | 111.61 | 205.05 | 444.95 | 819.29 |
| | 4/6 | 10.78 | 18.10 | 31.18 | 57.94 | 100.26 | 184.87 | 399.57 | 738.61 |
| | 4/5 | 9.44 | 15.89 | 27.40 | 51.01 | 88.90 | 164.70 | 354.18 | 657.93 |
| 800 | 4/8 | 7.04 | 11.57 | 19.69 | 36.21 | 61.79 | 112.92 | 245.48 | 450.29 |
| | 4/7 | 6.37 | 10.46 | 17.79 | 32.74 | 56.11 | 102.84 | 222.78 | 409.95 |
| | 4/6 | 5.70 | 9.36 | 15.90 | 29.28 | 50.43 | 92.74 | 200.09 | 369.61 |
| | 4/5 | 5.02 | 8.25 | 14.01 | 25.81 | 44.76 | 82.66 | 177.40 | 329.27 |
| 1600 | 4/8 | 3.82 | 6.09 | 10.15 | 18.41 | 31.20 | 56.77 | 123.04 | 225.45 |
| | 4/7 | 3.49 | 5.54 | 9.20 | 16.68 | 28.36 | 51.72 | 111.70 | 205.28 |
| | 4/6 | 3.15 | 4.98 | 8.25 | 14.94 | 25.52 | 46.68 | 100.35 | 185.11 |
| | 4/5 | 2.82 | 4.43 | 7.31 | 13.21 | 22.69 | 41.63 | 89.00 | 164.94 |

The first test that was conducted was to construct LoRaHAN packets and send them from the HAN Controller to the appliance device. The total packet size was set to the minimum allowable by the packet structure of the LoRaHAN packet, as seen in Figure 3 which is 39 bytes (5 bytes for the source address, 5 bytes for the destination address, 8 bytes for the nonce, 16 bytes for the authentication tag, 5 bytes for the command, and no additional data). The packets were sent in plaintext with no encryption/decryption or tag verification process. The total processing and transmission time of 200 packets were captured for every combination of SF, BW, and CR. The results can be seen in Table 4.

The second test that was conducted was to construct LoRaHAN packets and send them from the HAN Controller to the appliance device. The total packet size was set to the maximum allowable by the packet structure of the LoRaHAN packet, as seen in Figure 3 which is 255 bytes (5 bytes for the source address, 5 bytes for the destination address, 8 bytes for the nonce, 16 bytes for the authentication tag, 5 bytes for the command, and 216 bytes of additional data). The packets were sent in plaintext with no encryption/decryption or tag verification process. The total processing and transmission time of 200 packets were captured for every combination of SF, BW, and CR. The results can be seen in Table 5.

**TABLE 5.** The total average processing and transmission time (ms) required to send a 255-byte LoRaHAN packet with no encryption or tagging from the HAN Controller to an appliance device for all BWs, SFs, and CRs.

| BW (kHz) | CR | SF5 | SF6 | SF7 | SF8 | SF9 | SF10 | SF11 | SF12 |
|---|---|---|---|---|---|---|---|---|---|
| 200 | 4/8 | 135.62 | 226.81 | 390.34 | 688.40 | 1214.24 | 2225.33 | 4853.15 | 8737.95 |
| | 4/7 | 119.38 | 199.70 | 343.69 | 606.47 | 1070.53 | 1963.15 | 4278.36 | 7709.38 |
| | 4/6 | 103.15 | 172.60 | 297.05 | 524.54 | 926.81 | 1700.96 | 3703.56 | 6680.79 |
| | 4/5 | 86.91 | 145.49 | 250.40 | 442.60 | 783.10 | 1438.78 | 3128.76 | 5652.21 |
| 400 | 4/8 | 68.56 | 114.15 | 195.91 | 344.95 | 607.87 | 1113.41 | 2427.32 | 4369.72 |
| | 4/7 | 60.43 | 100.60 | 172.59 | 303.98 | 536.01 | 982.32 | 2139.92 | 3855.43 |
| | 4/6 | 52.32 | 87.04 | 149.27 | 263.01 | 464.15 | 851.23 | 1852.53 | 3341.14 |
| | 4/5 | 44.20 | 73.49 | 125.94 | 222.05 | 392.29 | 720.14 | 1565.13 | 2826.85 |
| 800 | 4/8 | 35.02 | 57.82 | 98.70 | 173.22 | 304.68 | 557.45 | 1214.41 | 2185.61 |
| | 4/7 | 30.96 | 51.04 | 87.04 | 152.73 | 268.75 | 491.90 | 1070.71 | 1928.46 |
| | 4/6 | 26.91 | 44.27 | 75.38 | 132.25 | 232.82 | 426.36 | 927.01 | 1671.32 |
| | 4/5 | 22.84 | 37.49 | 63.72 | 111.77 | 196.89 | 360.81 | 783.31 | 1414.17 |
| 1600 | 4/8 | 18.26 | 29.65 | 50.10 | 87.35 | 153.08 | 279.47 | 607.95 | 1093.55 |
| | 4/7 | 16.23 | 26.27 | 44.26 | 77.11 | 135.12 | 246.70 | 536.10 | 973.29 |
| | 4/6 | 14.20 | 22.88 | 38.43 | 66.87 | 117.16 | 213.92 | 464.25 | 836.40 |
| | 4/5 | 12.17 | 19.49 | 32.60 | 56.63 | 99.19 | 181.15 | 392.40 | 707.83 |

The third test that was conducted was to construct LoRaHAN packets and send them from the HAN Controller to the appliance device. The total packet size was set to the minimum allowable by the packet structure of the LoRaHAN packet, as seen in Figure 3 which is 39 bytes (5 bytes for the source address, 5 bytes for the destination address, 8 bytes for the nonce, 16 bytes for the authentication tag, 5 bytes for the command, and no additional data). The packets were first encrypted and tagged using ChaCha20-Poly1305 AEAD, sent across the network, received, decrypted and validated. The total processing and transmission time of 200 packets were captured for every combination of SF, BW, and CR. The results can be seen in Table 6.

**TABLE 6.** The total average processing and transmission time (ms) required to send a 39-byte encrypted and tagged LoRaHAN packet from the HAN Controller to an appliance device for all BWs, SFs, and CRs.

| BW (kHz) | CR | SF5 | SF6 | SF7 | SF8 | SF9 | SF10 | SF11 | SF12 |
|---|---|---|---|---|---|---|---|---|---|
| 200 | 4/8 | 26.38 | 44.50 | 76.98 | 143.08 | 245.39 | 449.93 | 980.14 | 1799.40 |
| | 4/7 | 23.70 | 40.08 | 69.40 | 129.21 | 222.68 | 409.57 | 889.37 | 1638.04 |
| | 4/6 | 21.01 | 35.66 | 61.83 | 115.34 | 199.97 | 369.21 | 798.60 | 1476.68 |
| | 4/5 | 18.33 | 31.24 | 54.25 | 101.47 | 177.27 | 328.85 | 707.83 | 1315.32 |
| 400 | 4/8 | 13.54 | 22.59 | 38.83 | 71.88 | 123.04 | 225.31 | 490.41 | 900.04 |
| | 4/7 | 12.19 | 20.39 | 35.05 | 64.95 | 111.69 | 205.13 | 445.03 | 819.36 |
| | 4/6 | 10.85 | 18.18 | 31.26 | 58.01 | 100.33 | 184.95 | 399.64 | 738.68 |
| | 4/5 | 9.51 | 15.97 | 27.47 | 51.08 | 88.98 | 164.77 | 354.26 | 658.00 |
| 800 | 4/8 | 7.11 | 11.64 | 19.76 | 36.29 | 61.87 | 113.00 | 245.55 | 450.37 |
| | 4/7 | 6.44 | 10.54 | 17.87 | 32.82 | 56.19 | 102.91 | 222.86 | 410.03 |
| | 4/6 | 5.77 | 9.43 | 15.98 | 29.35 | 50.51 | 92.82 | 200.17 | 369.69 |
| | 4/5 | 5.10 | 8.33 | 14.08 | 25.89 | 44.83 | 82.73 | 177.47 | 329.35 |
| 1600 | 4/8 | 3.90 | 6.17 | 10.23 | 18.49 | 31.28 | 56.84 | 123.12 | 225.53 |
| | 4/7 | 3.57 | 5.61 | 9.28 | 16.75 | 28.44 | 51.80 | 111.77 | 205.36 |
| | 4/6 | 3.23 | 5.06 | 8.33 | 15.02 | 25.60 | 46.76 | 100.43 | 185.19 |
| | 4/5 | 2.90 | 4.51 | 7.39 | 13.29 | 22.76 | 41.71 | 89.08 | 165.02 |

The fourth test that was conducted was to construct LoRaHAN packets and send them from the HAN Controller to the appliance device. The total packet size was set to the maximum allowable by the packet structure of the LoRaHAN packet, as seen in Figure 3 which is 255 bytes (5 bytes for the source address, 5 bytes for the destination address, 8 bytes for the nonce, 16 bytes for the authentication tag, 5 bytes for the command, and 216 bytes of additional data). The packets were first encrypted and tagged using ChaCha20-Poly1305 AEAD, sent across the network, received, decrypted and validated. The total processing and transmission time of 200 packets were captured for every combination of SF, BW, and CR. The results can be seen in Figure 9 and Table 7. As the results from all the latency tests followed similar trends, this is the only latency test that is graphed.

**TABLE 7. The total average processing and transmission time (ms) required to send a 255-byte encrypted and tagged LoRaHAN packet from the HAN Controller to an appliance device for all BWs, SFs, and CRs.**

| BW (kHz) | CR | SF5 | SF6 | SF7 | SF8 | SF9 | SF10 | SF11 | SF12 |
|---|---|---|---|---|---|---|---|---|---|
| 200 | 4/8 | 135.89 | 227.08 | 390.61 | 688.67 | 1214.52 | 2225.61 | 4853.42 | 8738.22 |
| | 4/7 | 119.66 | 199.98 | 343.97 | 606.74 | 1070.80 | 1963.43 | 4278.62 | 7709.64 |
| | 4/6 | 103.41 | 172.86 | 297.32 | 524.81 | 927.08 | 1701.24 | 3703.83 | 6681.06 |
| | 4/5 | 87.18 | 145.76 | 250.67 | 442.87 | 783.37 | 1439.06 | 3129.03 | 5652.48 |
| 400 | 4/8 | 68.83 | 114.42 | 196.18 | 345.22 | 608.14 | 1113.68 | 2427.59 | 4369.99 |
| | 4/7 | 60.71 | 100.87 | 172.86 | 304.25 | 536.28 | 982.59 | 2140.19 | 3855.70 |
| | 4/6 | 52.59 | 87.31 | 149.54 | 263.28 | 464.42 | 851.50 | 1852.79 | 3341.41 |
| | 4/5 | 44.47 | 73.76 | 126.22 | 222.32 | 392.56 | 720.41 | 1565.40 | 2827.12 |
| 800 | 4/8 | 35.29 | 58.09 | 98.97 | 173.49 | 304.95 | 557.72 | 1214.68 | 2185.88 |
| | 4/7 | 31.23 | 51.31 | 87.31 | 153.00 | 269.02 | 492.17 | 1070.98 | 1928.73 |
| | 4/6 | 27.17 | 44.54 | 75.65 | 132.52 | 233.09 | 426.63 | 927.28 | 1671.59 |
| | 4/5 | 23.11 | 37.76 | 63.99 | 112.04 | 197.16 | 361.08 | 783.58 | 1414.44 |
| 1600 | 4/8 | 18.53 | 29.93 | 50.37 | 87.62 | 153.35 | 279.74 | 608.22 | 1093.82 |
| | 4/7 | 16.50 | 26.54 | 44.53 | 77.38 | 135.39 | 246.97 | 536.37 | 973.56 |
| | 4/6 | 14.47 | 23.15 | 38.70 | 67.14 | 117.43 | 214.19 | 464.52 | 836.67 |
| | 4/5 | 12.44 | 19.76 | 32.87 | 56.90 | 99.46 | 181.42 | 392.67 | 708.10 |

After the latency tests for standard LoRa 2.4 GHz transmissions were conducted, data was then collected to determine the average time taken to establish a session key between the HAN Controller and the appliance device. The same test bed setup was used as the first set of tests, which can be seen in Figure 8, as well as the same algorithm for the Arduino Uno as seen in Algorithm 7. The HAN Controller initiated the session key establishment process as seen in Figure 7. At the beginning of the establishment process, the HAN Controller would set a pin to HIGH. The nonce exchanges then occurred. After these exchanges, and after the appliance has generated the session key, a pin on the appliance was then set to HIGH. The Arduino Uno measured the time between these two events. 200 session key establishment events were captured for every combination of SF, BW, and CR. The average of these results can be seen in Table 8.

The last set of tests that were conducted measured the packet delivery rate. These tests required a modification to the test bench setup. The Arduino was not used in these tests. These tests were conducted in a typical suburban Australian home setting. The HAN Controller and the appliance were placed at opposite ends of the home, each connected to a laptop. 200 encrypted and tagged packets, each of 255 bytes in size, were sent from the HAN Controller to the appliance, for each combination of BW, SF, and CR. When the appliance received a packet that was successfully validated, a "1" was output to the serial monitor. These 1's were then counted, with the results being expressed as a percentage of successfully received packets. These results can be seen in Table 9. Only the combinations that demonstrated a latency under 200 ms as per Table 7 were evaluated. The reason for this decision is discussed in Section VI.

**TABLE 8. The total average time (ms) required to perform the three-way nonce exchange process and establish a session key for all BWs, SFs, and CRs.**

| BW (kHz) | CR | SF5 | SF6 | SF7 | SF8 | SF9 | SF10 | SF11 | SF12 |
|---|---|---|---|---|---|---|---|---|---|
| 200 | 4/8 | 196.62 | 330.25 | 566.33 | 1006.76 | 1787.41 | 3313.46 | 7057.30 | 12822.55 |
| | 4/7 | 174.22 | 292.74 | 502.02 | 893.30 | 1588.22 | 2925.11 | 6270.72 | 11410.76 |
| | 4/6 | 151.82 | 255.22 | 437.71 | 779.84 | 1389.03 | 2562.08 | 5484.14 | 9998.97 |
| | 4/5 | 129.43 | 217.71 | 373.40 | 666.39 | 1189.84 | 2199.05 | 4697.55 | 8587.19 |
| 400 | 4/8 | 100.70 | 167.51 | 285.56 | 505.77 | 896.10 | 1646.47 | 3531.05 | 6413.68 |
| | 4/7 | 89.50 | 148.76 | 253.40 | 449.04 | 796.50 | 1464.95 | 3137.76 | 5707.78 |
| | 4/6 | 78.30 | 130.00 | 221.24 | 392.31 | 696.90 | 1283.43 | 2744.46 | 5001.89 |
| | 4/5 | 67.11 | 111.25 | 189.09 | 335.58 | 597.31 | 1101.92 | 2351.17 | 4296.00 |
| 800 | 4/8 | 52.74 | 86.14 | 145.17 | 255.27 | 450.44 | 825.62 | 1767.91 | 3209.23 |
| | 4/7 | 47.15 | 76.77 | 129.09 | 226.91 | 400.64 | 734.86 | 1571.27 | 2856.28 |
| | 4/6 | 41.55 | 67.40 | 113.02 | 198.55 | 350.85 | 644.12 | 1374.63 | 2503.35 |
| | 4/5 | 35.95 | 58.02 | 96.94 | 170.19 | 301.05 | 553.36 | 1177.99 | 2150.40 |
| 1600 | 4/8 | 28.77 | 45.47 | 74.98 | 130.04 | 227.62 | 415.21 | 886.36 | 1607.01 |
| | 4/7 | 25.96 | 40.77 | 66.93 | 115.84 | 202.71 | 369.82 | 788.02 | 1430.54 |
| | 4/6 | 23.17 | 36.08 | 58.89 | 101.66 | 177.81 | 324.44 | 689.70 | 1254.06 |
| | 4/5 | 20.36 | 31.40 | 50.86 | 87.48 | 152.91 | 279.06 | 591.38 | 1077.58 |

**TABLE 9. The percentage of successfully delivered packets measured between the HAN Controller and the appliance device, colour graded from green being the best, to red being the worst performing. "X" indicates combinations that were not tested.**

| BW (kHz) | CR | SF5 | SF6 | SF7 | SF8 | SF9 | SF10 | SF11 | SF12 |
|---|---|---|---|---|---|---|---|---|---|
| 200 | 4/8 | 100.00 | X | X | X | X | X | X | X |
| | 4/7 | 100.00 | 100.00 | X | X | X | X | X | X |
| | 4/6 | 100.00 | 99.50 | X | X | X | X | X | X |
| | 4/5 | 99.50 | 99.50 | X | X | X | X | X | X |
| 400 | 4/8 | 100.00 | 100.00 | 100.00 | X | X | X | X | X |
| | 4/7 | 100.00 | 98.50 | 100.00 | X | X | X | X | X |
| | 4/6 | 100.00 | 100.00 | 100.00 | X | X | X | X | X |
| | 4/5 | 99.50 | 100.00 | 100.00 | X | X | X | X | X |
| 800 | 4/8 | 100.00 | 100.00 | 100.00 | 100.00 | X | X | X | X |
| | 4/7 | 100.00 | 100.00 | 100.00 | 99.50 | X | X | X | X |
| | 4/6 | 100.00 | 100.00 | 100.00 | 99.50 | X | X | X | X |
| | 4/5 | 100.00 | 100.00 | 100.00 | 100.00 | 98.50 | X | X | X |
| 1600 | 4/8 | 100.00 | 100.00 | 100.00 | 100.00 | 100.00 | X | X | X |
| | 4/7 | 98.50 | 100.00 | 100.00 | 100.00 | 100.00 | X | X | X |
| | 4/6 | 98.50 | 100.00 | 100.00 | 100.00 | 100.00 | X | X | X |
| | 4/5 | 95.50 | 98.00 | 100.00 | 100.00 | 100.00 | 100.00 | X | X |

## VI. DISCUSSION

In terms of latency from a user perspective, smart home devices running on a HAN should exhibit minimal latency to ensure a quality user experience. According to Attig *et al.* [62], there is no definitive latency guideline. There have been various studies by numerous authors, with some more recent guidelines suggesting an action that provides some kind of feedback to the user should not exceed 1000 ms with up to 200 ms being preferred in some situations [63]. Accordingly, as seen in Figure 10 are our recommendations on the optimal combination of LoRa parameters for the HAN,

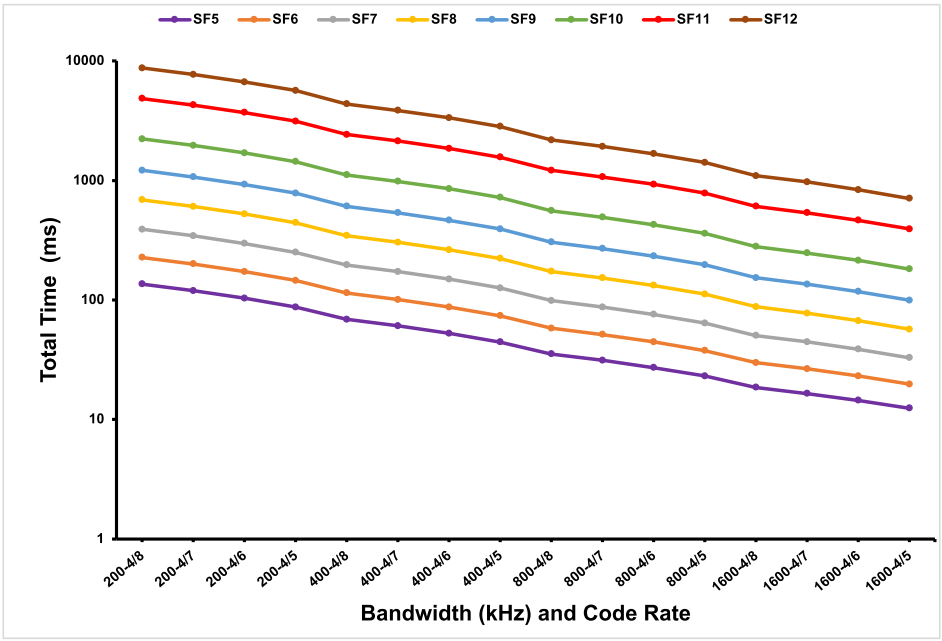


**FIGURE 9.** The total average processing and transmission time (ms) required to send a 255-byte encrypted and tagged LoRaHAN packet from the HAN Controller to an appliance device for all BWs, SFs, and CRs displayed with a logarithmic scale of 10 for improved visibility.

that offer latency under 200 ms when sending the maximum packet size of 255 bytes. While the study did briefly examine transmission range in terms of these faster performing SF, BW, and CR combinations, this was not the focus of this study and as such detailed ranging was not conducted.

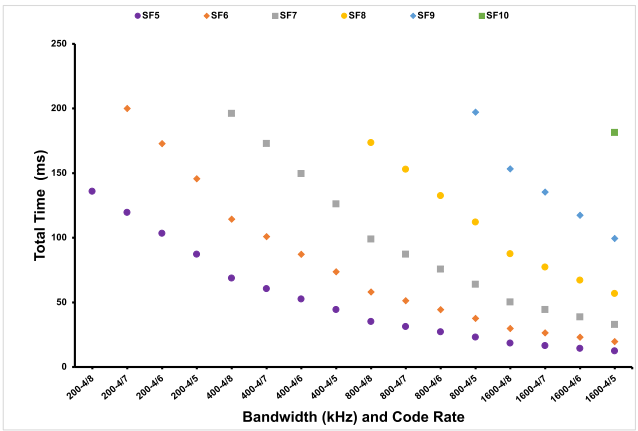


**FIGURE 10.** The combinations of the optimal LoRa performance parameters that offer under 200 ms latency with a 255-byte total packet size.

On analysis of the results from the tests conducted in this study, it is evident that implementing an effective encryption and authentication scheme on a LoRa 2.4 GHz network has minimal impact on latency. The tests that were performed in the evaluation were designed to look at both the best case (39 bytes) and the worst case (255 bytes) scenarios. This is important as it provides clarity on the range of expected performance. In a real-world scenario, it is reasonable to expect that the performance could fall somewhere in between these values, depending on the amount of data being transmitted. An average impact of 76.27 $\mu$s was observed with the minimum packet size of 39 bytes and an average of 270.11 $\mu$s was observed when increasing the packet size to 255 bytes. If you take SF 7 as an example, across all combinations of BW and CR, the time spent on encryption, decryption, and authentication averages to just 0.43% of the time.

The biggest negative impact that occurs on network performance is realised by decreasing the BW; this is closely followed by increasing the SF. When looking at the three tunable parameters, the CR has the lowest impact on the network performance.

With such a large amount of possible LoRa configurations, and examining both encrypted and plaintext as well as session key establishment, it can be difficult to make a comparison. The trends seen are consistent across the multiple spreading factors, and as such, Table 10 provides a comparison of all combinations of BW and CR with SF set to 7. The table shows figures for plaintext and encrypted transmission times, as well as session key agreement times. All values are presented in ms.

ChaCha20-Poly1305 was our choice of AEAD algorithm in this study and was informed by our previous research [48], as previously mentioned in Section III. This algorithm could be substituted for another AEAD scheme with little modification to suit individual implementation requirements. If this were to occur, the encrypted and tagged processing and transmission time measurements could not be relied upon, with further measurements being necessary.

**TABLE 10. A comparison table showing the total time (ms) for plaintext and encrypted transmissions at both 39 and 255 bytes, as well as the total time (ms) for the key agreement process. Only SF 7 is shown for all combinations of BW and CR.**

| BW-CR | Transmission | | | | Key Agreement |
|---|---|---|---|---|---|
| | Plaintext | | Encrypted | | |
| | Min | Max | Min | Max | |
| 200-4/8 | 76.90 | 390.34 | 76.98 | 390.61 | 566.33 |
| 200-4/7 | 69.33 | 343.69 | 69.40 | 343.97 | 502.02 |
| 200-4/6 | 61.75 | 297.05 | 61.83 | 297.32 | 437.71 |
| 200-4/5 | 54.18 | 250.40 | 54.25 | 250.67 | 373.40 |
| 400-4/8 | 38.76 | 195.91 | 38.83 | 196.18 | 285.56 |
| 400-4/7 | 34.97 | 172.59 | 35.05 | 172.86 | 253.40 |
| 400-4/6 | 31.18 | 149.27 | 31.26 | 149.54 | 221.24 |
| 400-4/5 | 27.40 | 125.94 | 27.47 | 126.22 | 189.09 |
| 800-4/8 | 19.69 | 98.70 | 19.76 | 98.97 | 145.17 |
| 800-4/7 | 17.79 | 87.04 | 17.87 | 87.31 | 129.09 |
| 800-4/6 | 15.90 | 75.38 | 15.98 | 75.65 | 113.02 |
| 800-4/5 | 14.01 | 63.72 | 14.08 | 63.99 | 96.94 |
| 1600-4/8 | 10.15 | 50.10 | 10.23 | 50.37 | 74.98 |
| 1600-4/7 | 9.20 | 44.26 | 9.28 | 44.53 | 66.93 |
| 1600-4/6 | 8.25 | 38.43 | 8.33 | 38.70 | 58.89 |
| 1600-4/5 | 7.31 | 32.60 | 7.39 | 32.87 | 50.86 |

The session key establishment processes and algorithms discussed in our work rely heavily on random number generation. It is assumed that any implementation would use a suitable function that will not return predictable numbers. In our evaluation, we used the ESP32 hardware random number generator [64]. An interesting fact to note is that either Bluetooth or Wi-Fi should be enabled at the time of the number generation to produce truly random numbers. If the requirements in the manual are not adhered to, the numbers are pseudo-random only.

When conducting the latency testing for encrypted transmissions using SF10, BW 200 kHz at all CRs, data integrity proved to be an issue with the bytes being received on the appliance not matching what was sent from the HAN Controller, causing the authentication tag to be invalid. We would not recommend using this combination until further investigation is conducted. Given that this combination far exceeds 200 ms, this particular combination of tuning parameters may not be suitable for the HAN. This could be improved with a higher quality antenna, as in this evaluation, only the built-in antenna on the SX1280 was used.

Using a single SX1280-based device as a HAN Controller could be problematic, particularly in a large home environment. Each SX1280 device can only be configured to communicate at a single BW and SF at any one time. This means that each device would have to be configured with a single BW and SF that would cater for the device operating in the worst-case scenario (i.e. the device that is furthest away). To mitigate this, a HAN controller could consist of several SX1280 transceivers operating at different BWs and SFs.

## VII. CONCLUSION

This study proposed a secure architecture and protocol suite for LoRa 2.4 GHz based HANs. It introduced mechanisms that focus on secure data transmission, initial key distribution, and ongoing key management through a standards-based session key agreement protocol. We then discussed the proposed authentication scheme's effectiveness against some common relevant security risks and attacks.

Next, a network performance study was conducted, which showed that the proposed security mechanisms in this research have minimal impact on the network performance compared with an open, non-secure network. We then measured the expected packet delivery rate in a typical home. Finally, we recommended the most optimal combinations of LoRa network performance tuning parameters. Through this work, we have demonstrated that LoRa 2.4 GHz is suitable as a basis for a secure HAN with appropriate security mechanisms.

A summary of the key findings and conclusions from this study are:

- LoRa 2.4 GHz is a suitable technology for use in the HAN, however, security measures must also be put in place to mitigate against attacks.
- The implementation of encryption, authentication, and key management adds additional latency to the network. This increase in network latency is insignificant to the overall network performance for the HAN.
- To achieve an optimal latency of under 200 ms, the correct management of the SF, BW, and CR parameters is vital.

As this study focused on a small-scale HAN environment, we did not specifically address scalability and multiple access protocols. Future work will include the evaluation and improvement of the scalability of LoRa 2.4 GHz networks, as well as examining and designing strategies to mitigate jamming attacks. We also plan to study mitigation against side-channel attacks.

## REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.
[2] E. Kabalci and Y. Kabalci, "Introduction to smart grid architecture," in *Smart Grids and Their Communication Systems*. Singapore: Springer, 2019, pp. 3–45.
[3] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct. Protection*, vol. 25, pp. 36–49, Jun. 2019.
[4] J. A. Nazabal, F. J. Falcone, C. Fernandez-Valdivielso, and I. R. Matias, "Energy management system proposal for efficient smart homes," in *Proc. Int. Conf. New Concepts Smart Cities, Fostering Public Private Alliances (SmartMILE)*, Dec. 2013, pp. 1–5.
[5] C. Bing and S. Kelly. *Cyber Attack Shuts Down U.S. Fuel Pipeline 'Jugular,' Biden Briefed*. Accessed: Jun. 7, 2022. [Online]. Available: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline%-operations-after-cybersecurity-attack-2021-05-08/
[6] J. Bair and J. Blas. *Petrol Shortages Sweep U.S. as Colonial Pipeline Remains Down*. Accessed: Jun. 7, 2022. [Online]. Available: https://www.aljazeera.com/economy/2021/5/11/petrol-shortages-sweep-us-a%s-colonial-pipeline-remains-down
[7] iTnews. *Queensland's CS Energy Has its Corporate Systems Infected by Ransomware*. Accessed: Jun. 7, 2022. [Online]. Available: https://www.itnews.com.au/news/queenslands-cs-energy-has-its-corporate-%systems-infected-by-ransomware-573352

[8] CS Energy. *CS Energy Responds to Cyber Security Incident*. Accessed: Jun. 7, 2022. [Online]. Available: https://www.csenergy.com.au/news/cs-energy-responds-to-cyber-security-incident

[9] A. Bari, J. Jiang, W. Saad, and A. Jaekel, "Challenges in the smart grid applications: An overview," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 2, Feb. 2014, Art. no. 974682.

[10] A. Padhan, P. R. Sahu, and S. Samantaray, "Performance of smart grid dynamic HAN with RQAM and GMSK modulation," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 1940–1943, Nov. 2019.

[11] Semtech. *Semtech SX1280 Datasheet Rev3.2*. Accessed: May, 31, 2021. [Online]. Available: https://www.semtech.com/products/wireless-RF/lora-24ghz/sx1280#downloa%d-resources

[12] J. Day and H. Zimmermann, "The OSI reference model," *Proc. IEEE*, vol. 71, no. 12, pp. 1334–1340, Dec. 1983.

[13] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Gener. Comput. Syst.*, vol. 96, pp. 579–590, Jul. 2019.

[14] N. S. Nafi, K. Ahmed, M. A. Gregory, and M. Datta, "A survey of smart grid architectures, applications, benefits and standardization," *J. Netw. Comput. Appl.*, vol. 76, pp. 23–36, Dec. 2016.

[15] M. Kuzlu, M. Pipattanasomporn, and M. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Comput. Netw.*, vol. 67, pp. 74–88, Jul. 2014.

[16] *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation With the Electric Power System (EPS), End-Use Applications, and Loads*, IEEE Standard 2030–2011, 2011, pp. 1–126.

[17] A. Hafeez, N. H. Kandil, B. Al-Omar, T. Landolsi, and A. R. Al-Ali, "Smart home area networks protocols within the smart grid context," *J. Commun.*, vol. 9, no. 9, pp. 665–671, 2014.

[18] C. Long, J. Wu, Y. Zhou, and N. Jenkins, "Aggregated battery control for peer-to-peer energy sharing in a community microgrid with PV battery systems," *Energy Proc.*, vol. 145, pp. 522–527, Jul. 2018.

[19] T. D. Mendes, R. Godina, E. M. Rodrigues, J. C. Matias, and J. P. Catalão, "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources," *Energies*, vol. 8, no. 7, pp. 7279–7311, 2015.

[20] Q. Hu and F. Li, "Hardware design of smart home energy management system with dynamic price response," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1878–1887, Dec. 2013.

[21] H. C. Jo, S. Kim, and S. K. Joo, "Smart heating and air conditioning scheduling method incorporating customer convenience for home energy management system," *IEEE Trans. Consum. Electron.*, vol. 59, no. 2, pp. 316–322, May 2013.

[22] B. Zhou, W. Li, K. W. Chan, Y. Cao, Y. Kuang, X. Liu, and X. Wang, "Smart home energy management systems: Concept, configurations, and scheduling strategies," *Renew. Sustain. Energy Rev.*, vol. 61, pp. 30–40, Aug. 2016.

[23] M. S. Kumar, S. Srinivasan, and B. Subathra, "A deterministic demand response program for schedulable loads in power distribution system," *Int. J. Pure Appl. Math.*, vol. 118, no. 18, pp. 2071–2077, 2018.

[24] A. Augustin, J. Yi, T. Clausen, and W. Townsley, "A study of LoRa: Long range & low power networks for the Internet of Things," *Sensors*, vol. 16, no. 9, p. 1466, Sep. 2016.

[25] I. B. F. De Almeida, M. Chafii, A. Nimr, and G. Fettweis, "Alternative chirp spread spectrum techniques for LPWANs," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 4, pp. 1846–1855, Dec. 2021.

[26] D. Magrin, M. Centenaro, and L. Vangelista, "Performance evaluation of LoRa networks in a smart city scenario," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.

[27] J. Sanchez-Gomez, R. Sanchez-Iborra, and A. Skarmeta, "Transmission technologies comparison for IoT communications in smart-cities," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6.

[28] G. D. Campo, I. Gomez, S. C. Sierra, R. Martinez, and A. Santamaria, "Power distribution monitoring using LoRa: Coverage analysis in suburban areas," in *Proc. EWSN*, 2018, pp. 233–238.

[29] M. R. Seye, B. Gueye, and M. Diallo, "An evaluation of LoRa coverage in Dakar peninsula," in *Proc. 8th IEEE Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Oct. 2017, pp. 478–482.

[30] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 34–40, Sep. 2017.

[31] L. Angrisani, P. Arpaia, F. Bonavolonta, M. Conti, and A. Liccardo, "LoRa protocol performance assessment in critical noise conditions," in *Proc. IEEE 3rd Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2017, pp. 1–5.

[32] L. Polak and J. Milos, "Performance analysis of LoRa in the 2.4 GHz ISM band: Coexistence issues with Wi-Fi," *Telecommun. Syst.*, vol. 74, no. 3, pp. 299–309, Jul. 2020.

[33] T. Janssen, N. BniLam, M. Aernouts, R. Berkvens, and M. Weyn, "LoRa 2.4 GHz communication link and range," *Sensors*, vol. 20, no. 16, p. 4366, Jan. 2020.

[34] F. R. Andersen, K. D. Ballal, M. N. Petersen, and S. Ruepp, "Ranging capabilities of LoRa 2.4 GHz," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–5.

[35] D. Zorbas, G. Z. Papadopoulos, P. Maille, N. Montavont, and C. Douligeris, "Improving LoRa network capacity using multiple spreading factor configurations," in *Proc. 25th Int. Conf. Telecommun. (ICT)*, Jun. 2018, pp. 516–520.

[36] The Things Network. *Spreading factors*. Accessed: Jun. 9, 2022. [Online]. Available: https://www.thethingsnetwork.org/docs/lorawan/spreading-factors/

[37] U. Noreen, A. Bounceur, and L. Clavier, "A study of LoRa low power and wide area network technology," in *Proc. Int. Conf. Adv. Technol. Signal Image Process. (ATSIP)*, May 2017, pp. 1–6.

[38] LoRa Alliance. *What is LoRaWAN Specification*. Accessed: May 1, 2022. [Online]. Available: https://lora-alliance.org/about-lorawan/

[39] LoRa Alliance. *LoRaWAN Security Full End-To-End Encryption for IoT Application Providers*. Accessed May 1, 2022. [Online]. Available: https://lora-alliance.org/sites/default/files/2019-05/lorawan_security%_whitepaper.pdf

[40] D. McGrew, *An Interface and Algorithms for Authenticated Encryption*, document RFC 5116, Jan. 2008. [Online]. Available: https://www.rfc-editor.org/info/rfc5116

[41] Y. Nir and A. Langley, *ChaCha20 and Poly1305 for IETF Protocols*, document RFC 8439, Jun. 2018. Accessed: Feb. 14, 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc8439

[42] G. Procter, "A security analysis of the composition of ChaCha20 and Poly1305," *Cryptol. ePrint Arch.*, Aug. 2014, Paper 2014/613. [Online]. Available: https://eprint.iacr.org/2014/613

[43] F. De Santis, A. Schauer, and G. Sigl, "ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2017, pp. 692–697.

[44] N. M. Kumar and P. K. Mallick, "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," *Proc. Comput. Sci.*, vol. 132, pp. 109–117, Jan. 2018.

[45] L. Li, "Study on security architecture in the Internet of Things," in *Proc. Int. Conf. Meas., Inf. Control*, vol. 1, May 2012, pp. 374–377.

[46] X. Liang and Y. Kim, "A survey on security attacks and solutions in the IoT network," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 0853–0859.

[47] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.

[48] L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. Mckague, "Security and performance in IoT: A balancing act," *IEEE Access*, vol. 8, pp. 121969–121986, 2020.

[49] B. Javed, M. W. Iqbal, and H. Abbas, "Internet of Things (IoT) design considerations for developers and manufacturers," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2017, pp. 834–839.

[50] H. Luo, L. Xiao, L. Wu, Z. Ruan, and W. Lin, "How to select SF and BW for 2.4 GHz LoRa ad-hoc communication: From energy consumption perspective," in *Proc. Int. Conf. Mobile Netw. Manag.* Cham, Switzerland: Springer, 2021, pp. 89–99.

[51] G. Kaur, S. H. Gupta, and H. Kaur, "Performance exploration of LoRa network in indoor environment," in *Proc. 8th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Aug. 2021, pp. 134–138.

[52] M. Schappacher, A. Dant, and A. Sikora, "Implementation and validation of LoRa-based systems in the 2.4 GHz band," in *Proc. IEEE 4th Int. Conf. Adv. Inf. Commun. Technol. (AICT)*, Sep. 2021, pp. 106–111.

[53] L. Alliance, "LoRaWAN L2 1.0.4 specification (TS001–1.04)," Version 1.0.4, LoRa Alliance, Fremont, CA, USA, Tech. Rep., 2020. Accessed: Jun. 9, 2022. [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-104-specification-package/

[54] *IT Security Techniques—Key Management—Part 2: Mechanisms Using Symmetric Techniques*, Int. Org. Standardization, Geneva, Switzerland, ISO/IEC Standard 11770-2:2018, 2018.

[55] *IT Security Techniques. Entity Authentication. Mechanisms Using Authenticated Encryption*, Int. Org. Standardization, Geneva, Switzerland, ISO/IEC Standard 9798-2:2019, 2019.
[56] *Information Technology—Security Techniques—Key Management—Part 6: Key Derivation*, Int. Org. Standardization, Geneva, Switzerland, ISO/IEC Standard 11770-6:2016, 2016.
[57] *Information Security—Message Authentication Codes (MACs)—Part 2: Mechanisms Using a Dedicated Hash-Function*, Int. Org. Standardization, Geneva, Switzerland, ISO/IEC Standard 9797-2:2021, 2021.
[58] Espressif. *ESP32 Series Datasheet Version 3.6*. Accessed: Jun. 7, 2021. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/esp32_data% sheet_en.pdf
[59] S. Robinson. *SX12XX Library*. Accessed: May 31, 2021. [Online]. Available: https://github.com/StuartsProjects/SX12XX-LoRa
[60] R. Weatherley. *Arduino Cryptography Library*. Accessed: May 31, 2021. [Online]. Available: https://github.com/rweather/arduinolibs
[61] Apple Inc. *Network—Apple Developer Documentation*. Accessed: Nov. 2, 2021. [Online]. Available: https://developer.apple.com/documentation/network
[62] C. Attig, N. Rauh, T. Franke, and J. F. Krems, "System latency guidelines then and now—Is zero latency really considered necessary?" in *Proc. Int. Conf. Eng. Psychol. Cogn. Ergonom.* Cham, Switzerland: Springer, 2017, pp. 3–14.
[63] S. C. Seow, *Designing and Engineering Time: The Psychology of Time Perception in Software*. Boston, MA, USA: Addison-Wesley, 2008.
[64] Espressif Systems Co. *ESP-IDF Programming Guide—Random Number Generation*. Accessed May 1, 2022. [Online]. Available: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-referen%ce/system/random.html

**LUKE KANE** received the B.Info.Tech. degree (Hons.) in computer science from the Queensland University of Technology (QUT), Brisbane, Queensland, Australia, in 2019, where he is currently pursuing the Ph.D. degree in the Internet of Things (IoT) performance and security. He currently works at QUT as a Sessional Academic, teaching undergraduate students in the areas of networking, network security, and system administration. His research interests include implementation and design of secure IoT architectures to support critical infrastructure.

**VICKY LIU** received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2011. Her Ph.D. dissertation proposed information system architecture to facilitate the enforcement of privacy and security. She is currently a Senior Lecturer at the Faculty of Science, Queensland University of Technology, Australia. She is actively involved in several government-funded research projects in addressing solutions for designing appropriate IoT architectures and balancing performance and security for IoT ecosystems. Her research interests include network and security, in particular, focusing on the Internet of Things (IoT) technologies and security aspects.

**MATTHEW MCKAGUE** received the B.Sc. degree (Hons.) in mathematics from the University of Regina, Regina, Canada, in 2004, and the M.Math. and Ph.D. degrees in combinatorics and optimization from the University of Waterloo, Waterloo, ON, Canada, in 2005 and 2010, respectively. He is currently a Lecturer in cryptography at the Queensland University of Technology, Brisbane, Australia. Previously, he worked as a Research Fellow at the Centre for Quantum Technologies, Singapore, and a Lecturer at the Department of Computer Science, University of Otago, Dunedin, New Zealand.

**GEOFFREY R. WALKER** (Senior Member, IEEE) received the B.E. and Ph.D. degrees from The University of Queensland (UQ), Brisbane, QLD, Australia, in 1990 and 1999, respectively. From 1998 to 2007, he was the Power Electronics Lecturer with UQ. From 2008 to 2013, he was a Senior Electrical Engineering Consultant with the Aurecon's Transmission and Distribution Group, Brisbane, across various areas, including rail traction, grounding studies, electricity transmission planning, and renewable energy project design and review. In 2013, he joined the Electrical Power Engineering Group, Queensland University of Technology, Brisbane, as an Associate Professor. His current research interests include applying power electronics to applications in renewable energy (especially photovoltaics and battery storage), power systems, and electric vehicles. A specific area of research interest is the modulation of high bandwidth multilevel converters. He has also worked and maintains an active interest in the pro-audio and industrial electronics sectors.