Smart Home IoT Communication Protocols and Advances in their Security and Interoperability

Ismael Holguin, Sai Mounika Errapotu
Department of Electrical and Computer Engineering, University of Texas at El Paso, El Paso, TX 79968

***Abstract*—Advances in sensor and communication technologies have transformed traditional homes into smart homes, equipped with sensors and actuators for various functionalities like smart lighting, temperature control, irrigation, solar monitoring, entertainment, and security. This transition is powered by the Internet of Things (IoT) architecture, enabling smart home hubs to integrate and control devices with different communication protocols. However, this shift has also introduced new security and privacy issues in the Smart Home IoT (SH-IoT) environment. To address these challenges, new communication protocols with cryptographic features have been developed, and a unified standard called Matter has been created to promote interoperability among different device manufacturers. This paper presents a comprehensive survey of recent trends and advances in the smart home IoT landscape, focusing on communication protocols, their security issues and protection features against vulnerabilities in the SH-IoT environment.**

***Index Terms*—Smart Home Communication Protocols; Architecture; Security**

I. Introduction

Advances in sensor and communication technologies have revolutionized home living, introducing unprecedented comfort and personalization options for users. The emergence of the Internet of Things (IoT) enabled smart devices has given rise to a new industry of consumer electronics, catering specifically to Smart Home-Internet of Things (SH-IoT) environments. TVs, vacuums, temperature controls, and irrigation systems when coupled with the internet have all transformed how people interact with and manage their homes. To facilitate communication among the increasing number of smart devices in homes, various communication protocols have been adopted. The Internet Protocol (IP) is still the most widely used, but its power consumption limits its application in battery-powered devices for SH-IoT. As a result, other protocols like Zigbee, Z-wave, and Bluetooth Low Energy (BLE) have been developed, each forming its own network for communication. However, this diversification raised the need for security features in smart homes devices such as encryption and authentication to safeguard against breaches and to prevent unauthorized access. Given the growing interest in smart home IoT, this survey discusses advances in SH-IoT protocols, their security features, and developments in new interoperability standards.

II. Smart Home-IoT Architecture

A. IoT Elements in Smart Homes

Smart home IoT relies on smart devices and applications, offering a wide range of functionalities. These devices include sensors for monitoring mail delivery, tracking solar energy consumption/generation, and controlling various aspects like temperature, lighting, garage doors, appliances, entertainment, and home security. The application platform gathers data from home devices through sensors and uses software to create a personalized user experience [1].

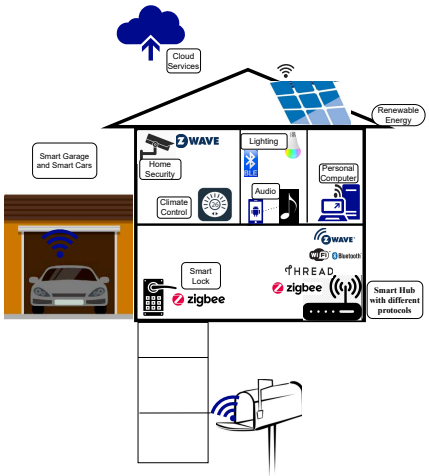

Fig. 1. Smart Home IoT Architecture

B. Layers in Smart Home-IoT Architecture

SH-IoT architecture is structured into three layers in a top-down approach:

- Cloud Layer: Servers and cloud-based infrastructure
- Fog Layer or Gateway Layer: Network gateway devices like routers that serve as intermediaries between cloud and edge devices.
- Edge Layer: Consists of devices such as smartphones and tablets and sensored devices like thermostats and lights.

C. SH-IoT Communication Network Structures

In this section, we will briefly discuss communication network structures related to smart home environments: (1) Wide Area Network (WAN) is a network configuration used to communicate data between large distances (used in smart home neighborhoods). The internet is a WAN setup as it interconnects different computers for sending and receiving data packets. (2) Local Area Network (LAN) as the name entails is a network confined to a smaller area such as a home (home area network) or business. LAN tends to have a higher transmission rate than WAN but within shorter distances, its

2023 7th Cyber Security in Networking Conference (CSNet) | 979-8-3503-4287-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/CSNET59123.2023.10339739

similar to WAN, and typically has one device (modem/router) acting as a door in communicating to the internet. (3) Wireless Personal Area Network (WPAN) is a network that is typically used with short-range communication protocols such as Bluetooth, Zigbee, Z-wave, Thread, BLE, and as of Fall 2022, Matter. WPAN has a low data rate, making it slower than LAN, but the topology is more versatile and can be configured to be a star or mesh structure.

III. Smart Home IoT Communication Protocols - Operation and Security

In this section, we will discuss widely used SH-IoT protocols, their advanced security features, and configurations. SH-IoT communications protocols and their security mechanisms are listed in Fig 2.

A. Bluetooth

Bluetooth is a wireless communication protocol found in most smart devices, operating within the IEEE 802.15 for WPAN standards. It creates a Wireless Personal Area Network, allowing Bluetooth-enabled devices to connect and share data, such as audio and images. Bluetooth operates in the 2.4GHz to 2.48GHz unlicensed band and supports Piconet (star), or Scatternet (mesh) topologies, with one master and up to seven slaves. It has a data rate of 1Mbps or 3Mbps depending on the version of Bluetooth. Bluetooth is vulnerable to various attacks, including eavesdropping, man-in-the-middle (MITM), denial of service (DoS), and message modification. To address security concerns, different security modes are defined, ranging from no security required to authenticate link keys and encryption algorithms for data integrity [2].

The modes for Bluetooth Security are defined here [2]:
Mode 1: Devices are never considered to be secure in any implementation.
Mode 2: Security procedures occur during the setup of the Service Layer, i.e., security is in effect after a link is established but not before logical channel is established. The concept of device authorization is introduced in this mode.
Mode 3: Security procedures occur during the setup of the Link Layer before the physical link is fully established. This mode of operation makes authentication and encryption a hard requirement for all connections established between devices. This mode makes it impossible for service discovery to take place until authentication, encryption, and authorization have been completed.
Mode 4: Security procedures occur during the setup of the Service Layer, similar to mode 2. However, mode 4 implements Secure Simple Pairing(SSP), in which Elliptic Curve Diffie-Hellman (ECDH) [3] [4] key agreement is utilized for link key generation. The P-192 Elliptic Curve was used for the link key generation until Bluetooth 4.0. Bluetooth 4.1 introduced the Secure Connections feature, which now implements P-256 Elliptic Curve for link key generation, and upgraded the authentication algorithm to FIPS-approved 256-bit Hash Message Authentication Code Secure Hash Algorithm [5] (HMAC-SHA-256). The encryption algorithm was also upgraded in 4.1 to FIPS-approved AES-Counter with CBC-MAC (AES-CCM) to ensure data integrity [2].

B. Bluetooth Low Energy (BLE)/ Bluetooth Smart

BLE was introduced in Bluetooth 4.0 and updated in 4.1 and 4.2 versions, specifically for devices with low computation power requirements [2]. BLE was initially created to be able to implement a Bluetooth stack in coin cell battery-powered devices, by periodically engaging in data transmission. It usually is in sleep mode, i.e., BLE remains in sleep mode unless a connection initiates, significantly reducing power consumed. One difference between Bluetooth and BLE is key generation. BLE generates a Long-Term Key (LTK), which is fundamentally similar to the Link Key. In BLE legacy pairing the LTK is generated by one of the devices, which then sends it to the other device during the pairing. BLE also was upgraded in Bluetooth 4.1 and the same security algorithms apply [2]. BLE is unencrypted by default, it is important to select a security mode.

C. Zigbee (now the Connectivity Standard Alliance)

Designed as a low data rate wireless personal area protocol, Zigbee has found its application in smart home IoT environments. The low data rate feature makes it useful for controlling home lighting, smart switches/dimmers and occupancy sensors to name a few applications; its mesh topology makes it very useful as a Personal Area Network (PAN). Zigbee has two bands on which it operates, on 868/915MHz providing a data rate of around 20-40Kbps, and 2450MHz providing a data rate of around 250Kbps. Zigbee protocol stack consists of four layers; the application layer, the network layer, the MAC layer, and the physical layer. The security in Zigbee is implemented in the network layer when enabled. If it is enabled then AES 128-bit symmetric keys [6] are used, the keys can either be preinstalled or obtained after the joining process [7].

A Zigbee node can support over 240 end points, each end point specifies a specific application. The topology of Zigbee consists of the Coordinator, Router, and End Devices. The controller/coordinator is always the first device that is setup when configuring a Zigbee network. The controller picks the channel and PAN ID i.e., the device is responsible for establishing the PAN. Once the PAN is established other Zigbee devices may join its network such as router and End devices. The controller is always powered by the main line in a home (i.e., outlet), and it never goes into sleep mode. The controller can act as a router if needed to help in routing data through the network, and can trigger the acceptance of other routers [7]. End devices have limited authority in the network, they cannot give authorization to devices to join the network or assist in data routing. End devices are battery-powered, and are put to sleep periodically to help in power consumption [7].

D. Z-Wave

Z-wave is a low-bandwidth communication protocol commonly used in smart home IoT applications like security sensors and alarms. It operates in the ISM band, with

Protocol	Security
Bluetooth	P256 EC, HMAC SHA256, AES 128-bit CCM
BLE	P256 EC, HMAC SHA256, AES 128-bit CCM
Zigbee	AES 128-bit CCM
Z-Wave	ECDH, AES 128-bit CCM
Thread	AES 128-bit CCM, PAKE
Matter	AES 128-bit CCM, SHA256, ECDH

Fig. 2. SH-IoT Protocols and Security Features

specific frequencies for the USA (908.42MHz) and Europe (868.42MHz). The protocol uses a master-slave mesh network topology, comprising controllers (primary and secondary) and slaves. Controllers initiate commands to the slave nodes, with the primary controller hosting the routing table and controlling node additions and removals. Slaves execute or relay commands as instructed by the controller. Z-Wave ensures network encapsulation using a 32-bit identifier Home ID for each controller. To enhance security, Z-wave implements the S2 framework based on Elliptic Curve [4] Diffie-Hellman [3] cryptography, providing resistance to attacks. It also incorporates AES 128-bit [6] symmetric cryptography for additional protection. Previous vulnerabilities related to a hard-coded default key have been addressed through firmware updates in the S2 framework [8].

E. Thread

Thread standard is low powered, low latency wireless mesh network protocol based on IPv6 over low-power wireless area networks (6LoWPAN). It is based on the IEEE 802.15.4 standard for low rate WPAN (LoWPAN). Thread comprises of a Physical layer and MAC layer that operate with 250kbps data rate in 2.4GHz band for link layer communication [9]. IEEE 802.15.4 standard's Carrier Sense Multiple Access-Collision Avoidance (CSMA-CA) is the basis for Thread's reliable transmission. CSMA-CA allows multiple devices to share 2.4GHz band, and initiates transmission only after confirming the channel is empty. Thread was designed to be a battery supply friendly protocol, even though it uses IPv6 it compresses the packet headers to minimize the size of the transmitted packet [9].

Thread network comprises of full thread devices and minimal thread devices. Full thread devices set constitutes of a Router that manages the routing needs of the network, a Leader that can make decisions as well as act as router, Router-Eligible End Devices (REED) that are non routing devices with capabilities to act as router when called by leader, and Full End Devices (FED) which are full thread devices that cannot be promoted to routers but can act as border routers. Thread network is dynamic in nature, if the Leader is knocked offline for some reason, network will select a different router to be the Leader creating zeros point of failures in the network. Full thread devices that can be border routers, act as hub and create IPv6 subnets of the thread network (since devices are IP-addressable), essentially becoming gateways [9].

Minimal thread devices set constitutes of Minimal End Devices (MED) which cannot forward messages but only can communicate with parent router, Sleepy End Devices (SED) are similar to MEDs whose radios are turned off and periodically wakes up to check for communication with parent router, and Synchronized Sleepy End Devices (SSED) are similar to SEDs whose radios are turned off and wake up at scheduled intervals to check for communication with parent router.

Thread implements AES-CCM [10] based network-wide key for payload encryption, in which the cipher works by implementing a check tag, appends some data to individual messages that can later be verified against the network-wide key, to verify if a message originated from where it says it did and to ensure that message integrity has not been violated. A new device joining thread network is oblivious to what the network key is. Since key cannot be sent over in an unsecured manner due to risks in compromise, Thread uses Password-Authenticated Key Exchange (PAKE) method to send key in a secure manner [9].

F. Matter/Project CHIP (Connected Home over IP)

Matter is the newest standard released in October 2022, created by the Zigbee alliance now called Connectivity Standards Alliance (CSA) which includes companies like Apple, Google, Amazon, Samsung, Comcast and many other silicon valley manufacturers, to achieve "interoperability" between devices in smart home IoT environment. Matter is similar to the interoperability standard DNP3 developed for smart grid environment [11]. Matter is built on the internet protocol that enables communication with Thread, Ethernet, and WiFi devices in a network.

Matter standard was designed with robust security as a top priority and to provide capabilities to detect and recover from attacks. Matter supports a comprehensive approach with authentication and attestation for commissioning, message integrity, and secure over the air firmware updates. It implements AES in CCM mode [10] with 128 bit keys for integrity and confidentiality, AES in CTR mode is used for protecting identifiers to preserve privacy, and SHA-256 [5] for integrity. It uses ECC for enabling interoperability, along with use for digital signatures, key exchanges, standard key derivation, and true random number generation [11]. Matter development has attracted over 500 industry leading companies to join the alliance in creating a secure and robust communication standard for SH-IoT environment, with many of them being security focused developers.

IV. Conclusion and Future Works

In this work, we discussed most widely used SH-IoT protocols, their communication networks and topologies, their security and interoperability features. In future works we will be presenting findings from our packet level security testing with border router prototypes and edge devices in SH-IoT communications.

Acknowledgement

This work was supported by the US Department of Energy (DoE) National Nuclear Security Administration research grant under Award Number DE-NA0004016.

REFERENCES

[1] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[2] J. Padgette, K. Scarfone, and L. Chen, "Guide to bluetooth security," *NIST special publication*, vol. 800, p. 121, 2017.

[3] N. Li, "Research on diffie-hellman key exchange protocol," in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4, 2010, pp. V4–634–V4–637.

[4] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 62–67, 2004.

[5] R. Martino and A. Cilardo, "Sha-2 acceleration meeting the needs of emerging applications: A comparative survey," *IEEE Access*, vol. 8, pp. 28 415–28 436, 2020.

[6] W. Burr, "Selecting the advanced encryption standard," *IEEE Security Privacy*, vol. 1, no. 2, pp. 43–52, 2003.

[7] Z. Alliance, "zigbee specification[white paper]," Tech. Rep., 2017. [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/01/docs-05-3474-22-0csg-zigbee-specification-1.pdf

[8] B. Fouladi and S. Ghanoun, "Security evaluation of the z-wave wireless protocol," *Black hat USA*, vol. 24, pp. 1–2, 2013.

[9] T. Group, "Thread specification [white paper]," Tech. Rep., 2017. [Online]. Available: https://www.threadgroup.org/ThreadSpec

[10] M. J. Dworkin, "Sp 800-38c. recommendation for block cipher modes of operation: The ccm mode for authentication and confidentiality," 2004.

[11] CSA, "Matter specification," Tech. Rep., 2022. [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf