On Building Automation Systems and Attacks

Christopher Morales-Gonzalez[†], Matthew Harper[†], Michael Cash[*], Qun Zhou Sun[*], Xinwen Fu[*†]
[*]University of Central Florida. Email: mcash001@knights.ucf.edu, qz.sun@ucf.edu
[†]University of Massachusetts Lowell
Email: {christopher_moralesgonzalez, matthew_harper}@student.uml.edu, xinwen_fu@uml.edu

***Abstract*—Building Automation Systems (BASs) are seeing increased usage in modern society due to the plethora of benefits they provide such as automation for climate control, HVAC systems, entry systems, and lighting controls. Many BASs in use are outdated and suffer from numerous vulnerabilities that stem from the design of the underlying BAS protocol. In this paper, we provide a comprehensive, up-to-date survey on BASs and attacks against seven BAS protocols including BACnet, EnOcean, KNX, LonWorks, Modbus, ZigBee, and Z-Wave. A case study is provided which describes a real-world BAS and showcases its vulnerabilities. We seek to raise awareness of BAS security to those in academia and industry.**

I. Introduction

A Building Automation System (BAS) is a type of cyber physical system whose purpose is to automate numerous processes such as maintaining HVAC controls, granting physical access through electronic locks, and lighting control within a building. BASs can be found controlling nuclear power plants [1], maintaining the climate in medical facilities, [2], ensuring the operation of an energy grid [3], enabling a city resource management system [4] and use in smart homes [5].

A BAS is often based on the OSI model given their history. Wired BAS protocols such as BACnet, KNX, LonWorks and Modbus were created in 1995, 1999, 1988 and 1979 respectively. Wireless BAS protocols such as EnOcean, ZigBee, and Z-Wave were created in 2012, 2003, 1999 respectively. Recall that TCP/IP became popular after the release of its soruce code into the public domain by UC Berkley in 1989. Many of the BAS protocols now provide TCP/IP support given the convenience of the Internet. BACnet is the predominant communication standard in smart building automation with an estimated market share of 60%.

There have been numerous attacks against BASs. For instance, in 2016, attackers targeted the central heating and hot water systems of a Finnish facilities services company [6]. In 2021, hundreds of building automation control devices of a German engineering company were fully locked, forcing manual operation of the BAS [7], [8]. Most recently in June 2022, a BAS was targeted by hackers using an advanced persistent threat against the BAS engineering computers which allowed access to the main network. [9].

Although there are efforts to perform surveys on BASs and their security including attacks against them [10]–[12], in this paper, we provide a comprehensive, up-to-date survey with an emphasis on the latest technologies while acknowledging findings in previous works. We cover a total of seven popular BAS protocols: Building Automation and Control Networks (BACnet), EnOcean, KNX, LonWorks, ModBus, ZigBee, and Z-Wave and primarily focus on their network architectures. We provide a thorough review of many types of attacks against BASs including: brute-force attacks, covert channel attacks, cryptographic attacks, device reprogramming, denial-of-service attacks, eavesdropping attacks, false data injection, fuzzing attacks, man-in-the-middle attacks, node compromise, physical attacks, reconnaissance attacks, replay attacks, spoofing attacks, and side channel attacks. We also provide a case study that showcases vulnerabilities within a real-world BAS.

II. Building Automation Systems

In this section we introduce a total of seven popular wired and wireless BASs with a focus on their network architectures.

A. Wired BAS

Fig. 1 illustrates an example wired BAS network. The BACnet, KNX and LonWorks network architectures are based on the OSI model while Modbus is only defined for the application layer of the OSI model. There can be many physical mediums within a BAS and are not required to use Ethernet. BACnet, KNX, and LonWorks have their own routing protocols and routers for their local networks while special BAS/IP routers can be used to interconnect multiple BASs together using the Internet. Modbus is different as it uses gateways for Internet access rather than routers.

1) BACnet: A BACnet BAS is logically separated into three main portions; *internetworks*, *networks* and *segments* [13]. A BACnet *segment* consists of physical electrical media to which BACnet devices are connected to. A BACnet *network* has one or more BACnet *segments* that are connected via bridges. Multiple BACnet networks can be connected through BACnet *routers* to form a BACnet *internetwork*.

2) KNX: A KNX BAS is logically separated into three portions: 1) Domain, 2) Area, 3) Line. A *Domain* is made up of 15 connected *areas*. An *Area* is made up of a series of connected *lines*. A *Line* is a culmination of many KNX devices (up to 256). Individual lines can have the same or different communication mediums but they must be connected by a line coupler(s). The same premise can be applied for connecting multiple areas to create a domain.

3) LonWorks: A LonWorks BAS consists of a peer-to-peer network that is logically separated into two major sections: 1) *Domains* and 2) *Subnets*. The *Domains* logically separate LonWorks networks and subnets. *Subnets* can be used to separate devices in a domain. The topologies available to the

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

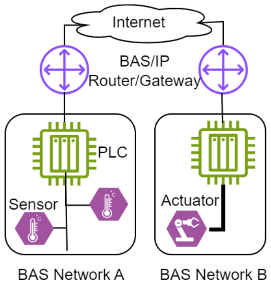

Fig. 1. Example Wired BAS Network

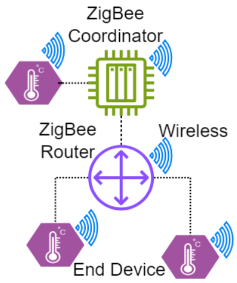

Fig. 2. Example ZigBee Network

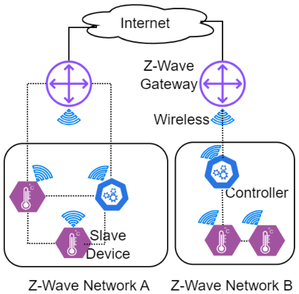

Fig. 3. Example Z-Wave Network

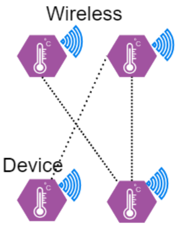

Fig. 4. Example EnOcean Network

LonWorks network are dependent on the physical mediums that are used. LonWorks provides support for twisted pair, ethernet, power line, fiber optic, and radio frequency. The network stack and thus, the network topology of a LonWorks network changes slightly depending on the physical medium used.

4) *Modbus:* Modbus is an application-layer-level protocol. The network model is defined based on the underlying data link communication protocol (i.e. RS-485) and the communication scheme is known as *Modbus on* X where X is that communication protocol, e.g., Modbus on RS-485 serial communication. Modbus TCP/IP is the Ethernet-oriented variant of the protocol that uses the Internet for communication between servers and clients such as sensors and actuators.

B. Wireless BAS

ZigBee, Z-Wave, and EnOcean are based on the OSI model and designed for low-power wireless communications. There has been limited effort to integrate ZigBee and EnOcean with the Internet while gateways can be used in Z-Wave networks for communications over IP networks.

1) *ZigBee:* ZigBee is designed for wireless personal area networks (WPANs) and can only communicate in the ISM and 2.4 GHz frequency ranges [14]. [14]. It provides support for three network topologies; namely, star, tree (shown in Fig. 2) and mesh. Regardless of the topology chosen, there are three entities that are present inside a ZigBee network at all times: *coordinator*, *router*, and *end device*. Fig. 2 shows an example ZigBee BAS network with a simple tree topology. The ZigBee coordinator is the root of the tree and the router can forward messages to/from devices that the coordinator is not directly connected to. The end devices cannot talk to another device on the network except for its parent node.

2) *Z-Wave:* Z-Wave is a wireless communication protocol that operates on a master-slave model in a mesh network topology. There are two classes of devices: the *controllers* issue commands to the *slave devices*. The *slave devices* perform operations or report information as requested by the controller. The logical separation of a Z-Wave network is provided by a 32-bit *HomeID* and nodes (controllers and slave-devices) are identified using the tuple of the *HomeID* and a unique 8-bit *NodeID*.

Fig. 3 shows a sample Z-Wave BAS network. The slave devices report back to their controllers, which process and handle the data. The Z-Wave Gateway is one of these controllers and it may report to a user's client (i.e. phone) or forward the information to another gateway. Slave devices may have the capability to act as routers in the mesh network where their routing behaviors are set by the controllers.

3) *EnOcean:* EnOcean is a wireless protocol based on the Low-Rate Wireless Personal Area Network (LR-WPAN) that supports mesh, star or point-to-point topologies in which all communications can only utilize the ISM bands [15]. EnOcean devices have to register with each other to communicate. Due to the nature of LR-WPAN and its limited range, EnOcean does not contain mechanisms for network segmentation. The only requirement for a device to communicate on an EnOcean network is an EnOcean radio transmitter. Fig. 4 shows a sample EnOcean BAS network in which all the devices get the same messages. However, the devices only accept messages if the sender's address has been verified.

III. Attacks against BAS

In this section, we first discuss attack surfaces present in BASs and then review existing attacks against BASs.

A. Attack Surfaces

A BAS has various components such as *hardware*–physical components that make up the device, *firmware*–low level program that control's a device's hardware components, *software*–applications used to perform high-level operations to carry out the function of a BAS, *network*–protocols which allow devices to transfer information and commands within the network to facilitate the functions of the BAS, and the *data* generated and stored within a BAS. Attacks may break confidentiality, integrity, availability, authentication, non-repudiation and other security requirements of these components.

B. Attacks

Table I provides an overview of the attacks against BASs and provides guidance for future research on BAS security. For example, we find there is little work on the secure extensions and software security of a BAS.

1) *Brute-Force Attack:* In brute-force attacks, an attacker tries to gain access to a system by guessing credentials or encryption keys. For example, this can include the usage of the leaked default master key for the ZigBee Light Link Profile [74] which violates the confidentiality requirement. This attack was also performed on ZigBee networks in [17]–[19].

2) *Covert Channel Attack:* Covert channels misuse existing systems and procedures to establish unauthorized communication channels. For example, if a protocol defines a field to be left as empty, then a covert channel can be established by placing messages into that field that another entity can parse

TABLE I
ATTACKS AGAINST BAS IN THE BIBLIOGRAPHY

Attack	BACnet	EnOcean	KNX	LonWorks	ModBus	ZigBee	Z-Wave
Brute Force Attack			[16]	[17]–[19]			
Covert Channel	[20]				[21]		
Cryptographic Attacks						[22], [23]	
Device Reprogramming	[24]		[25]		[26]	[27], [28]	[29], [30]
DoS	[24], [31]–[34]	[31]	[25], [31], [35]–[37]	[18], [38]	[26]	[12], [23], [31], [39]–[44]	[28], [29], [45], [46]
Eavesdropping	[33]	[47]–[49]	[16], [25], [35], [50], [51]	[17], [18], [38]	[26]	[11], [22], [23], [27], [28], [39]–[43], [52]–[54]	[29], [55]–[59]
False Data Injection	[51]	[49]	[36], [50], [51]	[18]	[26], [60], [61]	[54]	[56], [62]
Fuzzing Attacks			[37]			[63]	[64], [65]
MITM	[66]		[35], [51], [67]	[68]	[26], [69]	[12], [54], [70]	[55]
Node Compromise		[31]	[71], [72]			[39], [41]–[43], [73]	
Physical Attack	[31], [34], [66]	[31]	[25], [31], [35]	[19]		[23], [28], [31], [42], [43], [52], [53], [74], [75]	[29], [30], [76]
Reconnaissance	[24], [34], [67], [77]–[79]		[67]		[26], [80]	[27], [52], [54], [81]	[55]
Replay Attack		[49]	[51], [67]	[68]	[26], [60], [61]	[23], [28], [39], [52], [82]	[29], [58], [83]
Spoofing	[34]	[12]	[36]	[18], [68]	[26], [80]	[39], [70]	[12], [29], [55], [57], [58]
Side Channel		[48], [84]			[85]		[86]

out and interpret which breaks the confidentiality requirement if sensitive information is extracted. This method of using reserved bits to share data was found to be present in both BACnet networks [20] and Modbus/TCP networks [21]

3) Cryptographic Attack: Some cryptographic functions used in BASs are inherently insecure. An example is the XOR operation for encryption as this was shown to be vulnerable in the encryption scheme of ZigBee in [22]. Attackers have also exploited the reutilization of nonce values in ZigBee's encryption algorithm to extract the original plaintext [23] violating the confidentiality requirement which may lead to later attacks which break the authentication and non-repudiation requirements.

4) Device Reprogramming: If an attacker gains access to a device and has control over the device's firmware or software, they can make the device perform actions that they were not originally programmed to do; violating the integrity requirement. Some researchers reprogrammed a device entirely in a KNX network [16], and Morgner et al in [27], developed a framework called *Z3sec* that had the capability to factory reset any device or block a device permanently in a ZigBee network violating the integrity, availability, authentication and non-repudiation requirements.

5) Denial-of-Service Attack: Denial-of-service (DoS) and *distributed* DoS (DDoS) attacks are also utilized against BASs which affect their availability. (i) *Resource Consumption*: Resource consumption is one of the most popular methods used in a DoS attack. Physical devices have limited resources; when all of those resources are allocated, then the device won't be able to handle any more requests. Works such as [74], [75] have shown that the battery on devices is a vulnerable target as attackers are able to drain it and stop the device from functioning entirely. (ii) *Jamming*. A jamming attack is one where an attacker sends out frequencies that cause the legitimate frequencies to either drop or cause enough interference to not be processed correctly as was done in ZigBee networks [42], [44], [87]. This is particularly dangerous for wireless-only BAS protocols as they rely solely on radio signals to deliver their data. The plausibility of this attack is high as the attack can be carried out with a Software-Defined Radio (SDR).

6) Eavesdropping: All BAS protocols surveyed suffer from this type of attack as shown in multiple works [11], [16], [18], [22], [23], [25]–[29], [33], [35], [38]–[43], [47]–[59], [88] as BAS protocol communications are typically unencrypted violating the confidentiality requirement.

7) False Data Injection: In a false data injection (FDI) attack, an attacker injects false data into the network violating the integrity and authentication requirements. The requirement is that an attacker has to gain access to the BAS network. This can be done through physical access such as connecting a device onto the bus via a TP-wire for a hybrid BACnet-KNX system [51]. Other methods we reviewed which carry out a FDI use the following methods: using an old key that is still accepted by a BACnet network [24], finding and using the correct function codes in a Modbus/IP network [26] or directly connecting into the switch [60], hacking the wireless access point for a KNX/IP network [36], [50], using an EnOcean developer kit [49], using specialized USB sticks for ZigBee [54] and Modbus [61], sniffing out the network key for LonWorks [18], using a specialized C1110 chip or a Software-Defined Radio (SDR) [56], [62] for Z-Wave networks.

8) Fuzzing: Fuzzing is a technique that is used to find security flaws in software and hardware in hopes of breaching the integrity of the device while potentially breaching confidentiality and availability. The basic principle of fuzzing is to generate inputs rapidly and automatically, send them to a target and observe the response. This can either be done randomly or by adhering to the standards used by the target. An example of the latter is a smart fuzzer that would input a valid message code and then try to input invalid data to see if the target device crashes or interprets it wrong. Existing fuzzing works target KNX/IP [37], ZigBee [63], and Z-Wave [64], [65] networks.

9) Man-in-the-Middle: In a Man-in-the-Middle (MITM) attack, the attacker is able to place themselves between two communicating parties and can perform a suite of actions including interception, interruption, modification, or fabrication all of which affect the aforementioned security requirements. Some methods used to gain this access include ARP poisoning or CAM table attacks for protocols that use the IP-based communications such as KNX/IP, BACnet/IP and Modbus TCP [32]. Other methods include gaining physical access to the TP wires of a KNX-BACnet system and placing two Raspberry Pis into it [51]. (i) *Interception.* The attacker may choose to simply perform the equivalent of an Eavesdropping attack. In [29], Kim et al. used this capability to register a rogue device after they had sniffed out the network key from a Z-Wave network while Cash et al. in [51] simply forwards the messages in their attack on a KNX-BACnet system. (ii) *Interruption.* Because the messages have to go through the attacker's machine, the attacker can drop the packet to ensure that the message doesn't reach the intended destination. In a BAS, this could be dropping a message from a management app such as the IKEA Home Smart app used in a ZigBee network [70]. (iii) *Modification.* As the attacker has full control of the messages, the attacker can modify a portion of the message or create a new message entirely to cause some desired behavior. In a BAS, this could be modifying normal data between a router and controller on a Z-Wave network [29], modifying normal sensor traffic in a simulated LonWorks environment [68], modifying command/response messages in a Modbus network [26], [69] or a BACnet network [66]. (iv) *Fabrication.* Because the attacker has a communication channel with both parties, they can send a message to one entity as the other. In [29], Kim et al. are able to send messages as the controller in a Z-Wave network to start a pairing process for a remote device while others were able to impersonate any device on a LonWorks network [68] or a ZigBee network [12].

10) Node Compromise: A node compromise refers to a single device on the network that, when compromised, can leak sensitive information about the network such as various keys that may be used for securing communications. This violates the confidentiality, integrity, and potentially the authentication of the BAS. Judmayer et al. in [71] show that a single device can expose an entire KNX network through normal communications, while Morenas et al. in [72] attacked a particular web-based program *Node-Red* that would also lead to the exposure of an entire KNX network. The notion of stealing credentials from a device that had to leave a ZigBee network, which contained a network key is echoed in [39], [41]–[43], [73].

11) Physical Attack: During a physical attack, the physical components of the BAS are targeted. How they perform this attack can vary depending on the goal of the attacker. For example, an attacker could seek to manipulate, tamper, damage or destroy a physical component to carry out a DoS attack violating the availability requirement on the service that particular component provides [31], [34], [52], [66].

Other goals of a physical attack can include network intrusion as demonstrated by Cash et al. in [51] in which an attacker split a TP wire and connected their Raspberry Pi to it; granting access to the KNX network. They performed a FDI attack that could reach the BACnet network that the KNX network was attached to. Other works have also accessed a KNX network through exposed TP wires in buildings [25], [35]. It is important to also realize that the physical hardware a device contains can also be a target. For instance, authors have extracted a Z-Wave device's firmware and from it, extracted information such as various keys that were in use for normal communications as well as modifying the firmware [29], [30], [56], [76], [83]. This was also done to ZigBee devices in [23], [43], [53]. Some other methods against ZigBee include performing physical jamming attacks through a SDR [42] and draining a device's battery [75]. Other physical attacks that have been done on protocols include standing next to a smart card reader and using a SDR to attack the card reader on a LonWorks network [19] as well as simply reading the sticker on an EnOcean device that contains the device's key used when adding it to an EnOcean network [28].

12) Reconnaissance Attack: In a reconnaissance attack, the attacker is trying to actively gather information about a network or device that they're targeting. During this process, they may discover sensitive information which would violate the confidentiality requirement. Some key information that an attacker may want includes: the number of other devices on a network, getting the other devices' serial numbers or figuring out which application version a device is running.

These attacks have been done before in [67], [77], [78] in which BACnet's *Who-Is* requests are sent to find BACnet devices. BACnet device enumeration was done in [79] where Cash et al. made a tool to enumerate a device's object and property lists automatically. Attacks on KNX networks follow a similar idea in which they use the inherent *discovery* requests for KNX/IP servers [25], [67], [77]. Modbus researchers performed scans for the different controllers on the network [26], [80]. ZigBee researchers actively search for different networks and devices through the *beacon request* and *scan* services of ZigBee [27], [52], [54], [81]. Badenhop et al. in [55] describe using the *Get NL* primitive of Z-Wave to get the neighbor list of devices to gather a network topology [55].

13) Replay Attack: In a replay attack, a valid previous message can be resent onto the network and will be accepted by the network or the entity that the original message was intended for - violating the integrity requirement. This was shown by Fuller et al. in [58] in which they were able to attach a rogue controller to a Z-Wave network and replayed messages to reset a device into pairing mode. This was also shown in [83] in which Merdis was able to use an SDR, logic analyzer and multimeter to replay packets in a Z-Wave network. Other methods exist and have been acknowledged for EnOcean [49], KNX [51], [67], LonWorks [68], Modbus [26], [60], [61], and ZigBee [29], [58], [83].

14) Spoofing: In a spoofing attack (sometimes called an impersonation attack), an attacker impersonates a device on the network and sends out/responds to messages as the original device; violating the authentication requirement. Because of the lack of authentication in these BAS protocols, spoofing is a major issue that has been acknowledged and exploited in BACnet [34], EnOcean [12], KNX [36], LonWorks [18], [68], Modbus [26], [80], ZigBee [39], [70], and Z-Wave [12], [29], [55], [57], [58] networks.

15) Side Channel Attacks: Side channel attacks are those that utilize the normal implementation of systems to gain access to restricted information which violates the confidentiality requirement. For example, Jonas et al. in [84] find there is a side channel attack in EnOcean networks because there is unintentional data leakage from the signals that are sent from the open and close signals. The different signals had different lengths. Therefore, an attacker doesn't need to know the specifics of the message being sent. They only need to look at the lengths and understand that one is shorter than the other to understand which message was sent. Tsalis et al. also described the reality of side channel attacks in the ModBus protocol with regards to the time between packet intervals [85]. Liou et al. in [86] had discussed the reality of side channels within the ZigBee protocol based on the packet interval, number of packets sent and total packet size.

IV. Case Study

This section presents a case study on a real-world BAS.

A. Example Real-world BAS

Fig. 5 provides a simplified overview of a real-world BAS which consists of two buildings; Building A (top) and Building B (bottom). The backbone network used between and within the buildings is a BACnet/IP network connected via Ethernet cables. This BACnet/IP network is segmented using VLANs that are implemented with managed switches and firewalls to provide additional security and isolation between the buildings and control systems. Desigo CC [89] is the Building Management System (BMS) used in this BAS.

Building A contains a backbone BACnet/IP network connected to a BACnet MS/TP sub-network through a controller in which the various MS/TP devices are interconnected with RS-485 cables. This MS/TP sub-network includes another controller which provides access to an additional KNX sub-network whose devices are interconnected with KNX Red-Black connectors. Building B only contains the backbone BACnet/IP network and a BACnet MS/TP sub-network using the same appropriate wires.

B. Vulnerabilities

We briefly discuss three major vulnerability types in the real-world BAS in Fig. 5 which uses insecure BAS protocols and may be subject to other attacks reviewed in Section III.

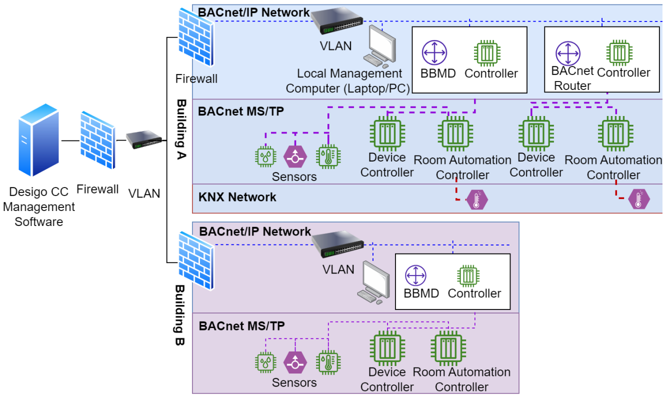

Fig. 5. Simplified Real-world BAS Network

1) Physical Vulnerabilities: Devices such as temperature sensors and presence detectors in public areas may be tampered with. In [51], we plug Raspberry Pis between a temperature sensor and a BAS controller, and deploy MITM attacks to inject false sensor data, affect readings within DesigoCC, and cause energy loss.

2) Software Vulnerabilities: There are a number of common software vulnerabilities in BAS devices. Lack of security awareness and skill may have caused the issues. For example, we have reported software vulnerabilities to ETS and Calimero. Although the bugs are fixed, no CVE was generated to notify the public of the danger.

3) Protocol Vulnerabilities: The attacks discussed in Section III regarding the base BACnet and KNX protocols are all feasible within this BAS as the security extensions to these protocols are not used. For example, in KNX, *access level*s are used to authorize access to services such as datapoints and memory locations within a device and are protected via 8-character keys. If KNX traffic is not encrypted, these keys are subject to eavesdropping. If this happens, an attacker can reset these keys and lock the devices, making them unusable.

V. Conclusion

In this paper, we performed a comprehensive survey of BAS protocol network architectures and attacks against BASs and confirm they are vulnerable. These BAS protocols are widely utilized in modern buildings such as those in businesses, university campuses, apartments and houses, therefore they are susceptible to wide range of attacks. If a BAS is connected to the Internet or components of the BAS are physically accessible, severe consequences may follow. We seek to raise the awareness of the security issues of BASs to both academia and industry members.

Acknowledgment

This research was supported in part by US National Science Foundation (NSF) awards 1931871 and 1915780, and US Department of Energy (DOE) Award DE-EE0009152. Any opinions, findings, conclusions, and recommendations in this paper are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] I. B. de Brito and R. T. de Sousa Jr, “Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants,” *Applied Sciences*, vol. 12, no. 15, p. 7942, 2022.

[2] N. Kraus, M. Viertel, and O. Burgert, “Control of knx devices over ieee 11073 service-oriented device connectivity,” in *2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS)*, vol. 1. IEEE, 2020.

[3] P. Amaro, R. Cortesão, J. Landeck, and P. Santos, “Implementing an advanced meter reading infrastructure using a z-wave compliant wireless sensor network,” in *Proceedings of the 2011 3rd international youth conference on energetics (IYCE)*. IEEE, 2011.

[4] I.-V. Sita and P. Dobra, “Knx building automations interaction with city resources management system,” *Procedia Technology*, vol. 12, 2014.

[5] D.-F. Pang, S.-L. Lu, and Q.-Y. Zhu, “Design of intelligent home control system based on knx/eib bus network,” in *2014 International Conference on Wireless Communication and Sensor Network*. IEEE, 2014.

[6] L. Mathews, “Hackers use ddos attack to cut heat to apartments,” "https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/?sh=7cfc8dfa1a09", 2021.

[7] L. Security, “Knxlock - an attack campaign against knx-based building automation systems,” "https://limessecurity.com/en/knxlock/", 2021.

[8] K. J. Higgins, “Lights out: Cyberattacks shut down building automation systems,” "https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems", 2021.

[9] T. Seals, “China-backed apt pwns building automation systems with proxylogon,” "https://www.darkreading.com/attacks-breaches/china-backed-apt-pwns-building-automation-proxylogon", 2021.

[10] P. Ciholas, A. Lennie, P. Sadigova, and J. M. Such, “The security of smart buildings: a systematic literature review,” *arXiv preprint arXiv:1901.05837*, 2019.

[11] L. Li, P. Podder, and E. Hoque, “A formal security analysis of zigbee (1.0 and 3.0),” in *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, 2020, pp. 1–11.

[12] H. M. Rouzbahani, H. Karimipour, E. Fraser, A. Dehghantanha, E. Duncan, A. Green, and C. Russell, “Communication layer security in smart farming: A survey on wireless technologies,” *arXiv preprint arXiv:2203.06013*, 2022.

[13] A. S. Publications, “Ansi/ashrae standard 135-2020,” ASHRAE, Tech. Rep., 2020.

[14] *ZigBee Specification*, 05th ed., ZigBee, 2015. [Online]. Available: https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

[15] E. S. IoT, “Radio technology,” https://www.enocean.com/en/technology/radio-technology/#:~:text=The%20standard%20uses%20the%20868,and%20928%20MHz%20in%20Japan., 2021.

[16] A. Antonini, F. Maggi, and S. Zanero, “A practical attack against a knx-based building automation system,” in *2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014) 2*, 2014.

[17] A. Antonini, A. Barenghi, G. Pelosi, and S. Zonouz, “Security challenges in building automation and scada,” in *2014 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2014.

[18] W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus, “Security in networked building automation systems,” in *2006 IEEE International Workshop on Factory Communication Systems*. IEEE, 2006.

[19] C. Schwaiger and A. Treytl, “Smart card based security for fieldbus systems,” in *EFTA 2003. 2003 IEEE Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.03TH8696)*, vol. 1, 2003, pp. 398–406 vol.1.

[20] J. Kaur, J. Tonejc, S. Wendzel, and M. Meier, “Securing bacnetâĂŹs pitfalls,” in *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings 30*. Springer, 2015, pp. 616–629.

[21] K. Lamshöft and J. Dittmann, “Assessment of hidden channel attacks: Targetting modbus/tcp,” *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 11 100–11 107, 2020.

[22] M. Qianqian and B. Kejin, “Security analysis for wireless networks based on zigbee,” in *2009 International Forum on Information Technology and Applications*, vol. 1. IEEE, 2009, pp. 158–160.

[23] J. Ďurech and M. Franeková, “Security attacks to zigbee technology and their practical realization,” in *2014 IEEE 12th international symposium on applied machine intelligence and informatics (SAMI)*. IEEE, 2014, pp. 345–349.

[24] D. G. Holmberg, Jul 2003. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916765

[25] D. Schneider and W. Przybilla, “Ernw newsletter 49/august 2015,” https://ernw.de/download/ERNW_Newsletter_49_SecurityOfHomeAutomationSystems_signed.pdf, 2015.

[26] M. Bashendy, S. Eltanbouly, A. Tantawy, and A. Erradi, “Design and implementation of cyber-physical attacks on modbus/tcp protocol,” in *World Congress on Industrial Control Systems Security (WCICSS)*, 2020.

[27] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, “Insecure to the touch: attacking zigbee 3.0 via touchlink commissioning,” in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017, pp. 230–240.

[28] G. Kambourakis, C. Kolias, D. Geneiatakis, G. Karopoulos, G. M. Makrakis, and I. Kounelis, “A state-of-the-art review on the security of mainstream iot wireless pan protocol stacks,” *Symmetry*, vol. 12, no. 4, p. 579, 2020.

[29] K. Kim, K. Cho, J. Lim, Y. H. Jung, M. S. Sung, S. B. Kim, and H. K. Kim, “WhatâĂŹs your protocol: Vulnerabilities and security threats related to z-wave protocol,” *Pervasive and Mobile Computing*, vol. 66, p. 101211, 2020.

[30] C. W. Badenhop, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, “Extraction and analysis of non-volatile memory of the zw0301 module, a z-wave transceiver,” *Digital Investigation*, vol. 17, 2016.

[31] M. Zeng, “A review of smart buildings protocol and systems with a consideration of security and energy awareness,” in *13th International Green and Sustainable Computing Conference (IGSC)*. IEEE, 2022.

[32] V. Graveto, T. Cruz, and P. Simöes, “Security of building automation and control systems: Survey and future research directions,” *Computers & Security*, vol. 112, p. 102527, 2022.

[33] L. P. Rondon, L. Babun, A. Aris, K. Akkaya, and A. S. Uluagac, “Survey on enterprise internet-of-things systems (e-iot): A security perspective,” *Ad Hoc Networks*, vol. 125, p. 102728, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870521002171

[34] D. G. Holmberg, Nov 2003. [Online]. Available: https://search.proquest.com/openview/11de4f48550d34fec12de2d8aab2a273/1?pq-origsite=gscholar&amp;cbl=41118

[35] T. Mundt and P. Wickboldt, “Security in building automation systems-a first analysis,” in *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*. IEEE, 2016.

[36] M. Ibrahim and I. Nabulsi, “Security analysis of smart home systems applying attack graph,” in *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*. IEEE, 2021.

[37] C. Vacherot, “Sneak into buildings with knxnet/ip,” in *Sneak into buildings with KNXnet/IP*, 2020.

[38] W. Granzer, F. Praus, and W. Kastner, “Security in building automation systems,” *Industrial Electronics, IEEE Transactions on*, vol. 57, pp. 3622 – 3630, 12 2010.

[39] X. Fan, F. Susan, W. Long, and S. Li, “Security analysis of zigbee,” *MWR InfoSecurity*, vol. 2017, pp. 1–18, 2017.

[40] B. Yang, “Study on security of wireless sensor network based on zigbee standard,” in *2009 international conference on computational intelligence and security*, vol. 2. IEEE, 2009, pp. 426–430.

[41] M. A. B. Karnain and Z. B. Zakaria, “A review on zigbee security enhancement in smart home environment,” in *2015 2nd International Conference on Information Science and Security (ICISS)*. IEEE, 2015, pp. 1–4.

[42] S. Khanji, F. Iqbal, and P. Hung, “Zigbee security vulnerabilities: Exploration and evaluating,” in *2019 10th international conference on information and communication systems (ICICS)*. IEEE, 2019.

[43] W. Razouk, G. V. Crosby, and A. Sekkaki, “New security approach for zigbee weaknesses,” *Procedia Computer Science*, vol. 37, pp. 376–381, 2014.

[44] D.-G. Akestoridis, M. Harishankar, M. Weber, and P. Tague, “Zigator: Analyzing the security of zigbee-enabled smart homes,” in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 77–88.

[45] N. Boucif, F. Golchert, A. Siemer, P. Felke, and F. Gosewehr, “Crushing the wave–new z-wave vulnerabilities exposed,” *arXiv preprint arXiv:2001.08497*, 2020.

[46] D. Cheng, P. Felke, F. Gosewehr, and Y. Peng, “S0-no-more: A z-wave nonceget denial of service attack utilizing included but offline nodeids,” *arXiv preprint arXiv:2205.00781*, 2022.

[47] K. Hofer-Schmitz, “A formal analysis of enoceanâĂŹs teach-in and authentication,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–8.

[48] Y. Wu and T. Feng, “An anonymous authentication and key update mechanism for iot devices based on enocean protocol,” *Sensors*, vol. 22, no. 17, p. 6713, 2022.

[49] A. Camek, F. Hölzl, and D. Bytschkow, “Providing security to a smart grid prosumer system based on a service oriented architecture in an office environment,” in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2013, pp. 1–7.

[50] J. Molina, “Learn how to control every room at a luxury hotel remotely: The dangers of insecure home automation deployment,” *Black Hat USA*, 2014.

[51] M. Cash, C. Morales-Gonzalez, S. Wang, X. Jin, A. Parlato, J. Zhu, Q. Z. Sun, and X. Fu, “On false data injection attack against building automation systems,” in *2023 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2023, pp. 35–41.

[52] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, “Three practical attacks against zigbee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned,” in *2014 14th International Conference on Hybrid Intelligent Systems*. IEEE, 2014, pp. 199–206.

[53] P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen, and S. Carlsen, “Zigbee/zigbee pro security assessment based on compromised cryptographic keys,” in *2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. IEEE, 2010, pp. 465–470.

[54] J. Wright, “Killerbee: practical zigbee exploitation framework,” in *11th ToorCon conference, San Diego*, vol. 67, 2009.

[55] C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, “The z-wave routing protocol and its security implications,” *Computers & Security*, vol. 68, pp. 112–129, 2017.

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

[57] L. Rouch, J. François, F. Beck, and A. Lahmadi, “A universal controller to take over a z-wave network,” in *Black Hat Europe*, 2017.

[58] J. D. Fuller and B. W. Ramsey, “Rogue z-wave controllers: A persistent attack channel,” in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*. IEEE, 2015, pp. 734–741.

[59] T. Oluwafemi, T. Kohno, S. Gupta, and S. Patel, “Experimental security analyses of $\{Non-Networked\}$ compact fluorescent lamps: A case study of home automation security,” in *LASER*, 2013.

[60] L. Rajesh and P. Satyanarayana, “Detection and blocking of replay, false command, and false access injection commands in scada systems with modbus protocol,” *Security and Communication Networks*, vol. 2021, 2021.

[61] W. Alsabbagh, S. Amogbonjaye, D. Urrego, and P. Langendörfer, “A stealthy false command injection attack on modbus based scada systems,” in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*. IEEE, 2023, pp. 1–9.

[62] C. W. Badenhop, “A multifaceted security evaluation of z wave, a proprietary implementation of the internet of things,” AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH WRIGHT-PATTERSON âĂę, Tech. Rep., 2017.

[63] X. Wang and S. Hao, “Don’t kick over the beehive: Attacks and security analysis on zigbee,” in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2857–2870.

[64] C. K. Nkuba, S. Kim, S. Dietrich, and H. Lee, “Riding the iot wave with vfuzz: discovering security flaws in smart homes,” *IEEE Access*, vol. 10, 2021.

[65] J. L. Hall, “A practical wireless exploitation framework for z wave networks,” AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH WRIGHT-PATTERSON âĂę, Tech. Rep., 2016.

[66] T. Yimer, E. Smith, P. Harvey, M. Tienteu, and K. Kornegay, “Error correction attacks on bacnet ms/tp,” in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2022, pp. 77–80.

[67] V. Graveto, T. Cruz, and P. SimÃţes, “Security of building automation and control systems: Survey and future research directions,” *Computers & Security*, vol. 112, p. 102527, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003515

[68] T. Feng and Y. Wu, “Formal security analysis and improvement based on lontalk authentication protocol,” *Security and Communication Networks*, vol. 2022, p. 8104884, Jul 2022. [Online]. Available: https://doi.org/10.1155/2022/8104884

[69] C. Parian, T. Guldimann, and S. Bhatia, “Fooling the master: exploiting weaknesses in the modbus protocol,” *Procedia Computer Science*, vol. 171, pp. 2453–2458, 2020.

[70] N. Hussein and A. Nhlabatsi, “Living in the dark: Mqtt-based exploitation of iot security vulnerabilities in zigbee networks for smart lighting control,” *IoT*, vol. 3, no. 4, pp. 450–472, 2022.

[71] A. Judmayer, L. Krammer, and W. Kastner, “On the security of security extensions for ip-based knx networks,” in *2014 10th IEEE Workshop on Factory Communication Systems (WFCS 2014)*. IEEE, 2014.

[72] J. de las Morenas, C. M. da Silva, G. S. Funchal, V. Melo, M. Vallim, and P. Leitao, “Security experiences in iot based applications for building and factory automation,” in *2020 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2020.

[73] C. Müller, F. Armknecht, Z. Benenson, and P. Morgner, “On the security of the zigbee light link touchlink commissioning procedure,” *Sicherheit 2016-Sicherheit, Schutz und Zuverlässigkeit*, 2016.

[74] D.-G. Akestoridis and P. Tague, “Hiveguard: A network security monitoring architecture for zigbee networks,” in *2021 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2021.

[75] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, “Ghost-in-zigbee: Energy depletion attack on zigbee-based wireless networks,” *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, 2016.

[76] C. W. Badenhop, S. R. Graham, B. E. Mullins, and L. O. Mailloux, “Looking under the hood of z-wave: Volatile memory introspection for the zw0301 transceiver,” *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 2, 2018.

[77] F. Praus and W. Kastner, “Identifying unsecured building automation installations,” in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*. IEEE, 2014.

[78] O. Gasser, Q. Scheitle, B. Rudolph, C. Denis, N. Schricker, and G. Carle, “The amplification threat posed by publicly reachable bacnet devices,” *Journal of Cyber Security and Mobility*, vol. 6, no. 1, p. 77âĂŞ104, Nov. 2017. [Online]. Available: https://journals.riverpublishers.com/index.php/JCSANDM/article/view/5227

[79] M. Cash, S. Wang, B. Pearson, Q. Zhou, and X. Fu, “On automating bacnet device discovery and property identification,” in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[80] H. Ochiai, M. D. Hossain, P. Chirupphapa, Y. Kadobayashi, and H. Esaki, “Modbus/rs-485 attack detection on communication signals with machine learning,” *IEEE Communications Magazine*, 2023.

[81] T. Zillner and S. Strobl, “Zigbee exploited: The good, the bad and the ugly,” *Black Hat–2015. Available online: https://www. blackhat. com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly. pdf (accessed on 21 March 2018)*, 2015.

[82] S. S. Rana, M. A. Halim, and M. H. Kabir, “Design and implementation of a security improvement framework of zigbee network for intelligent monitoring in iot platform,” *Applied Sciences*, vol. 8, no. 11, p. 2305, 2018.

[83] V. Merdis, “Wireless communication protocols for home automation exploring the security and privacy aspects of smart home iot devices communicating over the z-wave protocol,” Master’s thesis, University of Twente, 2019.

[84] K. Jonas, B. Vogl, and M. Rademacher, *Security mechanisms of wireless building automation systems*. Dean Prof. Dr. Wolfgang Heiden, 2017.

[85] N. Tsalis, G. Stergiopoulos, E. Bitsikas, D. Gritzalis, and T. K. Apostolopoulos, “Side channel attacks over encrypted tcp/ip modbus reveal functionality leaks.” in *ICETE (2)*, 2018, pp. 219–229.

[86] J.-C. Liou, S. Jain, S. R. Singh, D. Taksinwarajan, and S. Seneviratne, “Side-channel information leaks of z-wave smart home iot devices: Demo abstract,” in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020.

[87] Y. Liu, Z. Pang, G. Dán, D. Lan, and S. Gong, “A taxonomy for the security assessment of ip-based building automation systems: The case of thread,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, 2018.

[88] L. N. Whitehurst, T. R. Andel, and J. T. McDonald, “Exploring security in zigbee networks,” in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, 2014, pp. 25–28.

[89] Siemens, “Desigo cc - better. of course,” "https://www.siemens.com/global/en/products/buildings/automation/desigo/building-management/desigo-cc.html", 2023.