PANEVĖŽIO KOLEGIJA ISSN 2029-1280, eISSN 2669-0071. Taikomieji tyrimai studijose ir praktikoje – Applied Research in Studies and Practice, 2024, 20.

ANALYSIS OF SMART HOME MANAGEMENT SYSTEMS AND SECURITY SOLUTIONS

Vakaris ŽILINSKAS[a]*, Oskaras PABRĖŽA*[a]*, Daiva STANELYTĖ*[ab]

[a] *Klaipedos valstybine kolegija – Higher Education Institution, Lithuania*
[b] *Lithuanian Energy Institute, Lithuania*

Annotation. This paper presents a smart home management system with a special focus on security. Smart homes are becoming increasingly popular, incorporating features such as artificial intelligence control and automation, but face unique security challenges. The authors evaluate the different communication standards - ZigBee, Z-Wave and KNX - analyzing each of them according to their security advantages and disadvantages. The aim of the study is to shed light on these differences, explaining the potential threats and providing practical recommendations on how to protect the smart home from cyber threats.

Keywords: smart home, safety, standards, smart systems

INTRODUCTION

The development of smart technologies makes everyday life easier, increasing comfort and safety at home. These systems allow you to automate home functions, control appliances remotely and monitor your environment. However, these devices can be the target of cyber-attacks, so it is important to understand the characteristics and risks of different control systems.

Equipment security is a key aspect of the smart home. IoT devices such as smart cameras and sensors can pose threats. To protect assets, it is essential to choose reliable devices with common standards that ensure stable operation and protection against malicious activities. A centralized system that relies on the internet is vulnerable to loss of network access.

The uniqueness of the paper lies in its systematic analysis and recommendations for improving cyber security, drawing on a variety of sources. In addition, future trends and existing standards to address these issues are discussed.

The subject of the study is Smart Home Management Systems.

Objective - Analysis of Smart Home Management Systems with Integrated Artificial Intelligence

Study objectives:

1. Differentiate smart home standards for cyber security applications.
2. Examine cyber security threats in smart homes.
3. Provide recommendations for cybersecurity solutions in the smart home.

Research methods - comparative analysis and synthesis of data from literature and electronic sources.

The databases used for the analysis *EBSCO ASP, EBSCO CEEAS,* and *Science Direct*.

DIFFERENCES IN SMART HOME STANDARDS FOR CYBERSECURITY APPLICATIONS

The ZigBee wireless standard has been developed using the IEEE 802.15.4 standard introduced by the IEEE and the *ZigBee Alliance* to create a common standard for *ZigBee* applications. The network operates in three frequency bands: 868 MHz, 915 MHz, and 2.4 GHz. The most used frequency is 2.4 GHz. There is a 5 MHz separation between the channels to avoid interference and to ensure stable communication (Grzegorz et.al, 2024). The IEEE 802.15.4 *ZigBee* standard enables wireless technologies for heterogeneous sensors in personal home and building environments. Wireless sensing technologies and their devices are moving from the research level to the industrial stage with applications in smart building monitoring and automation (Hayat et.al, 2016).

Table 1

Comparing communication standards for building automation

Parameters	KNX	Z WAVE ALLIANCE	zigbee
PHY/MAC standard	ISO/IEC 14543-3-10	ITU-T G.9959	IEEE 802.15.4
Frequency band	Twisted pair bus control cable (TP), 30V	900 MHz	2.4 GHz
Nominal range (0 dBm)	Up to 1000 m (above TP)	30 - 100 m	10 - 100 m
Data transfer rate	9600 bit/s	40-100 kbit/s	250 it/s

Z-Wave is a low-power radio wave, wireless communication standard for smart home automation. *Z-Wave* has higher latency (100 MS), and lower network reliability compared to *ZigBee. Z-Wave* operates at a frequency of 908.42

MHz in the US and Canada with regional variations (Kim et.al, 2014). *KNX* acts as a data communication system for exchanging data in a home control system. Shielded twisted-pair bus control cables are used for communication via *KNX* TPs and supply power to the devices. Up to 256 devices can be connected on each line and the system can be expanded using connectors. *KNX* uses the ISO/IEC 14543-3-10:2020 standard. (Grzegorz et.al, 2024).The table below provides comparisons of communication standards for building management systems.*KNX* uses a twisted-pair bus control cable and supports the highest communication range, making it suitable for large building systems*. The Z-Wave* and *ZigBee* standards use wireless frequencies (900 MHz and 2.4 GHz respectively) but have lower range and data rates. ZigBee has higher data rates, but Z-Wave works better in the US and Canada due to regional regulations.

***ZigBee* network architecture and security**. *ZigBee* network topologies include star, hierarchical and mesh structures, where routers can communicate with other routers or coordinators, allowing the network to "self-heal" and optimize message routes (Hillman, 2017). *ZigBee* networks typically use a star or wire topology where devices communicate with a central coordinator or through intermediaries. The communication system uses a standard in which data units contain both control information and transmitted data (Li et.al, 2010).

The Remote Smart Home system uses wireless *ZigBee* devices and a *ZigBee* web interface to control various devices such as switches, blinds, and power sockets. The CC2530 chip manages ZigBee communication and GPRS transmits alarm information to mobile phones (Yuhan, 2024). The CC2530 chip is a wireless chipset for controlling *ZigBee* communication. The CC2530 chipset connects various communication modules that provide wireless communication in a computer monitoring center. The center, which connects to a video module and a GPRS module (Xinyuan, 2018), which transmit alarm information to mobile phone users via a GPRS network. The user can also view video information through a smart device to determine if there is a false alarm in an unsafe situation (Yuhan, 2024).

The CC2530 functional connection socket diagram is shown in Figure 4 below to show how this chipset connects to other devices in the system and provides wireless connectivity.

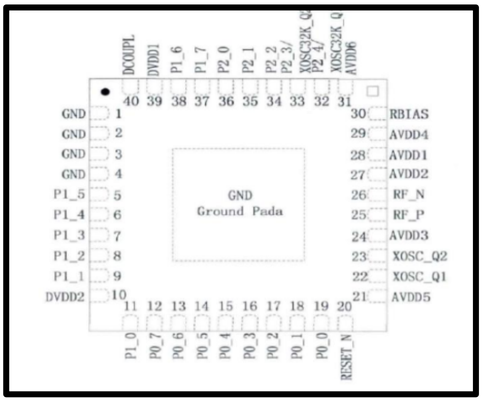

Figure 4: **Functional diagram of the CC2530 connection sockets. Source: Du Yuhan. (2024).** ***Research on Security System of Smart Home Based on ZigBee. International Journal of Computer Science and Information Technology*, 4, 37-45.**

The CC2530 chip supports the 2.4GHz IEEE 802.15*.4/ZigBee* standard and has three memory buses: SFR, DATA and CORE/XDATA. The interrupt can trigger the active mode, while the SFR bus connects the
CPU, DMA, and physical memory to external devices (Xiaoguang, 2012). The CC2530 chip is important for ZigBee communication management due to its compatibility and efficient memory architecture. The CC2530 chip provides reliable and flexible data communication in smart home systems.

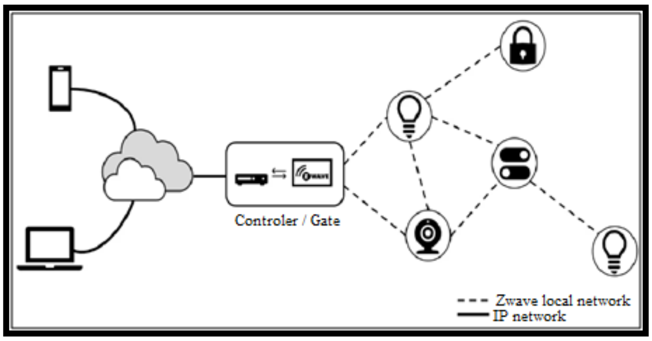

Figure 5: ***Z-Wave* network node diagram. Source. Mailloux. (2017).** ***The Z-Wave routing protocol and its security implications. Computers & Security*, 68.**

Z-Wave network architecture and security. *The Z-Wave* network topology supports up to 232 devices connecting through nodes, allowing you to extend the communication range to 100 meters in an open space. Frequency-shift-locked modulation at 868.42 MHz (Europe) and 908.42 MHz (USA) is used, with a routing algorithm that optimizes the best communication paths (Rahman, 2018). *A Z-Wave* network consists of a controller and slave devices. The controller manages the network topology, while the slave nodes execute commands and enable communication with nodes outside the direct range, as shown in Figure 5 (Xiaoguang, 2012).

The Z-Wave standard uses AES-128 encryption and ECDH key exchange to ensure security and has been evaluated against UL security standards (Sigma Design press release, 2017). *The Z-Wave* S2 standard includes three security classes, S2 Access Control, S2 Authenticated and S2 Unauthenticated, and allows for secure connection establishment with temporary keys (Ujwala et.al, 2018). *Z-Wave* is suitable for larger and more complex building management systems due to its more reliable connectivity and elevated level of security, but compatibility issues with older devices can lead to security gaps.

KNX network architecture and safety. *The KNX* network topology supports different physical layer media, the most popular of which is *KNX-TP*, which uses a data rate of 9600 bps and a CSMA/CA access method. In addition, *KNX* supports other media such as *KNX-PL* (power line), *KNX-RF* (radio frequency) and *Knelt/IP* based on IP networking (Goltz et.al, 2019). *KNX* is widely used in building automation in Europe. *The KNX-Secure* add-on module provides encryption and authentication, but only certified devices can use this security mechanism, which limits the security of the system (Goltz, 2021). The segmentation of the *KNX* network becomes necessary to avoid high loads and to ensure a stable connection, as shown in Figure 6.

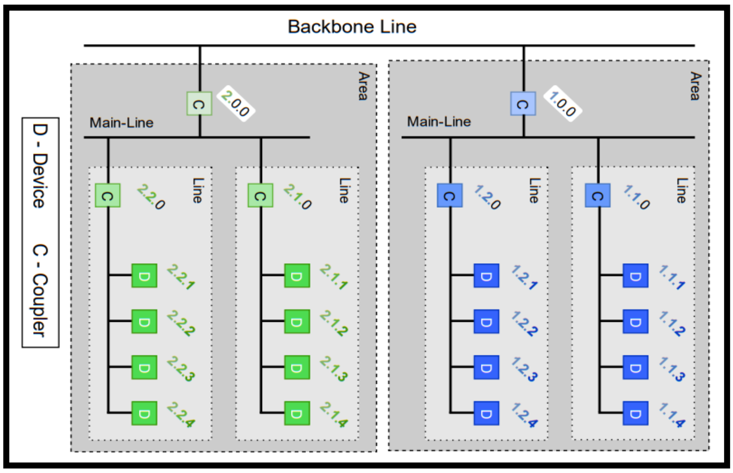

Figure 6: **Logical structure of a *KNX* Network (Capture image). Source. *Investigating the Filter Capacity of Line couplers in KNX regarding network security. International Wireless Communications and Mobile Computing Conference (IWCMC)*, Limassol, Cyprus**

KNX devices have unique physical addresses consisting of three digits separated by slashes. Group addresses are used during network operation and only multicasting ensures the functionality of communication. As each line can only contain 256 devices, segmentation of the *KNX* network becomes necessary to avoid high load and to ensure stable communication (Goltz, 2020). KNX can use an IP network for a higher control layer or directly access the automation layer via ZigBee or BACNet, where devices function as a bridge between the cyber and physical world (Ciholas et.al, 2019).

KNX is a reliable data transmission system for building automation, but the KNX-Secure standard is only applicable to certified devices, so its level of security may be limited. Nevertheless, KNX is appreciated for its applicability in complex systems and its ability to use multiple communication layers.

CYBER SECURITY THREATS IN SMART HOMES

Threats to the ZigBee standard. *ZigBee* is a wireless communication standard based on IEEE 802.15.4, used in smart homes for its low power consumption and cost-effectiveness. However, security vulnerabilities arise because *the ZigBee* protocol uses standardized Global Trust Center Link Keys, which can be known to individuals with malicious intent and used to intercept data traffic. (Leeuwen et.al, 2019). This allows hackers to not only intercept data traffic, but also to analyze the activity of lights, temperature, or other devices in the home, which can help identify when the building is empty, which poses an additional threat (Santos, 2015).

ZigBee is also vulnerable to several types of attacks, including replay attacks. Those with malicious intent can intercept and re-send identical signals, taking advantage of the fact that some *ZigBee* systems do not have effective sequence number validation (Abomhara et.al, 2014). This further exacerbates the security concerns of the smart home network.

In summary, the *ZigBee* standard has advantages in terms of cost-effectiveness, but security weaknesses such as easily accessible encryption keys and ineffective sequence number validation make it vulnerable to malicious intent.

Threats to the Z-Wave standard. Z-Wave, a popular standard that uses robust encryption methods such as AES-128, but it also has its own security flaws. The main threat comes from man-in-the-middle attacks, where hackers can gain access to network authentication keys due to security vulnerabilities while the device is connected (Pen Test Partners, 2021). Despite these vulnerabilities, Z-Wave is improving security with S2 encryption and ECDH authentication, but older devices that cannot support the new security standards remain vulnerable.

In addition, some *Z-Wave* devices use unused or unencrypted data transmission methods (e.g., CS-8 or CRC-16), which can lead to risks of unauthorized remote access and data tampering. This opens the possibility for replay attacks and theft of personal information, which further complicates network security (Badenhop et.al, 2017).

The Z-Wave protocol, while using advanced encryption technologies, remains vulnerable to older devices and certain weaker encryption methods. Upgrading devices to newer security standards is necessary to ensure better security.

Threats to the KNX standard. *The KNX* standard, widely used in Europe for building automation, is not immune to cyber-attacks. *KNX-TP* technology is more secure because it is harder to access by outsiders, but the use of *KNXnet/IP* makes the IP network vulnerable to vulnerabilities (Goltz et.al, 2019). *KNX-Secure* provides encryption and authentication, but only certified devices can use it. Uncertified devices remain vulnerable, and many devices in a network can reduce performance and cause delays (Goltz, 2020). *KNX* networks are vulnerable when *KNXnet/IP* technology is used, as it opens the door to cyber-attacks. Although *KNX-Secure* provides encryption, older or non-certified devices remain vulnerable. Also, network performance can be reduced in the presence of many devices.

CYBERSECURITY SOLUTIONS FOR SMART HOMES: RECOMMENDATIONS

Security is a key concern in smart homes as they can store and transmit sensitive information, making them vulnerable to security and privacy breaches (Abie et.al, 2012). Smart homes need to meet six important security objectives: confidentiality, authentication, integrity, authorization, availability, and non-repudiation (He et.al, 2014). Security threats are classified into internal and external: internal due to network configuration errors or weak passwords (Abomhara et.al, 2014), and external due to external threats such as RF and wireless (Abomhara et.al, 2015).

The main threats to the smart home. Denial of Service (DoS) attack: a Denial of Service (DoS) attack is one of the most common threats in smart homes. In this attack, hackers flood the network or system with a series of requests that block the ability to properly process legitimate requests. This can lead to smart devices such as heating, cooling systems or lighting controls becoming inaccessible (Kouicem, 2018).

Eavesdropping: In an eavesdropping attack, hackers intercept traffic between smart devices and the network. This can lead to the theft of sensitive information such as passwords or login credentials. Using tools such as Wireshark, hackers can connect to the network and monitor the data sent by devices, compromising personal privacy and security (Geneiatakis et.al, 2018).

Impersonation attack: In this attack, hackers try to impersonate a legitimate user to gain unauthorized access to smart home devices or systems. This can be achieved through social engineering or by intercepting login credentials. Identity theft allows hackers to manipulate the home automation system and cause security breaches such as theft or unauthorized access to CCTV cameras (Talal et.al, 2019).

Malicious software, such as viruses and Trojan horses, can be installed on smart devices. This can steal personal information, damage functions or open back doors to control devices. Weak authentication procedures, such as poor passwords, are often used (Ali et.al, 2018).

Information Theft: Hackers can take advantage of vulnerable smart devices to steal sensitive information, such as credit card numbers, personal identification data or even records of daily activities. This data can be used for financial fraud or privacy breaches (Ali et.al, 2017).

The most common cyber threats in smart homes, such as DoS attacks, eavesdropping, identity spoofing and malware, can cause serious security breaches. Proper authentication and device security are essential to protect personal information and devices.

Cybersecurity guidelines and preventive measures. Regular software updates are essential to ensure protection against vulnerabilities. Updates prevent hacks and strengthen defenses, while firewalls protect against external threats (Ali et.al, 2018).

Encrypt data transmissions: using encryption can protect data from interception and malicious attacks. Encryption ensures that even if a hacker intercepts the data, they will not be able to read it. This is particularly important when devices transmit personal data or other sensitive information (Perera et.al, 2016).

Secure communication channels (VPNs): Virtual Private Networks (VPNs) can ensure that only authorized users have access to the network. Using VPNs can ensure that all communications between smart home devices and the network are encrypted and inaccessible to unauthorized people, thereby strengthening the network's security against unauthorized access (Ali et.al, 2018).

Use strong and unique passwords: it is important to create strong passwords made up of numbers, letters, and special characters. It is also necessary to use different passwords for different devices and not to use the same password for all devices. In addition, passwords should be changed regularly to reduce the risk of theft and malicious attacks (NetFormation, 2019).

Backup: backups are important to protect valuable information from loss or theft. Regularly backing up data and storing it in secure locations ensures that data will not be lost even if devices fail or become the target of hacking (Abdullah et.al, 2019).

Keeping your smart home devices secure requires regular software updates, encryption, VPNs, and strong passwords. It is also important to back up your data and make sure your devices are protected against known threats.

CONCLUSIONS

1. Smart home control system standards such as ZigBee, Z-Wave and KNX have fundamental differences in terms of frequency range, data rate and communication range. Each standard has its own advantages and disadvantages which determine their suitability for specific conditions. For example, ZigBee and Z-Wave are better suited for wireless communication, while KNX is effective for wired solutions in large building systems.

2. Each of the standards under consideration faces specific security risks. The ZigBee standard has low power consumption, but its encryption solutions may be insecure due to publicly available keys. Meanwhile, the Z-Wave system is vulnerable to middle layer attacks. The KNX standard, although often seen as dependable for building automation, has limited security due to compatibility with older devices and mediocre performance when many devices are connected on one line.

3. It is recommended that you keep your smart home device software up to date, use secure, encrypted communications, and use firewalls to protect against external attacks. It is also necessary to constantly change default passwords and use unique login credentials for different devices.

REFERENCES

8 best practices for securing the Internet of Things (IoT). (2024, January 10). SecurityScorecard. https://securityscorecard.com/blog/best-practices-for-securing-internet-of-things/

Abdullah, T. A. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges, attacks and solutions for Internet of things based smart home. http://paper.ijcsns.org/07_book/201909/20190917.pdf

Abie, H., & Balasingham, I. (2012). Risk-based adaptive security for smart IoT in eHealth. BodyNets, 269–275. https://doi.org/10.4108/ICST.BODYNETS.2012.250235

Abomhara, M., Department of Information and Communication Technology, University of Agder, Norway, Køien, G. M., & Department of Information and Communication Technology, University of Agder, Norway. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Abomhara, M., & Køien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. IEEE. https://doi.org/10.1109/prisms.2014.6970594

Ali, B., & Awad, A. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors (Basel, Switzerland), 18(3), 817. https://doi.org/10.3390/s18030817

Cc, C. (n.d.). A true system-on-chip solution for 2.4-GHz IEEE 802.15.4 and ZigBee applications. Www.ti.com. Retrieved November 13, 2024, from https://www.ti.com/lit/ds/symlink/cc2530.pdf?ts=1731484894353&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FCC2530

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). Security and privacy issues for an IoT based smart home. IEEE. https://doi.org/10.23919/mipro.2017.7973622

Ghayvat, H., Mukhopadhyay, S. C., & Gui, X. (2016). Issues and mitigation of interference, attenuation and direction of arrival in IEEE 802.15.4/ZigBee to wireless sensors and networks based smart building. Measurement: Journal of the International Measurement Confederation, 86, 209–226. https://doi.org/10.1016/j.measurement.2016.01.045

Goltz, J. (2020). Investigating the Filter Capacity of Linecouplers in KNX regarding network security. IEEE. https://doi.org/10.1109/iwcmc48107.2020.9148402

Goltz, J. (2021). Securing Building Automation Systems. IEEE. https://doi.org/10.1109/ntms49979.2021.9432650

Goltz, J., Mundt, T., & Wiedenmann, S. (2019). Risk analysis in fieldbus networks using the example of KNX. International Conference on Information Networking, 310–315. https://doi.org/10.1109/ICOIN.2019.8718149

Chen, H. C., & Chang, L. Y (2012). Design and Implementation of a ZigBee-Based Wireless Automatic Meter Reading System. PRZEGLĄD ELEKTROTECHNICZNY (Electrical Review), 88(1b). https://www.researchgate.net/publication/290712491_Design_and_Implementation_of_a_ZigBee-Based_Wireless_Automatic_Meter_Reading_System

Johannes, G., Thomas, M., & Wiedenmann, S. (2019). Risk analysis in fieldbus networks using the example of KNX. IEEE. https://doi.org/10.1109/icoin.2019.8718149

Khanji, S., Iqbal, F., & Hung, P. (2019). ZigBee security vulnerabilities: Exploration and evaluating. IEEE. https://doi.org/10.1109/iacs.2019.8809115

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. Computer Networks, 141, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012

Leeuwen, D. V., & Ayuk, L. T. (2019). Security testing of the Zigbee communication protocol in consumer grade IoT devices. https://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Ahh%3Adiva-40189

Li, H., Jia, Z., & Xue, X. (2010). Application and analysis of ZigBee security services specification. IEEE. https://doi.org/10.1109/nswctc.2010.261

Liang, C. B., Tabassum, M., Kashem, S. B. A., Zama, Z., Suresh, P., & Saravanakumar, U. (2021). Smart home security system based on zigbee. In Advances in Intelligent Systems and Computing (pp. 827–836). Springer Singapore. https://doi.org/10.1007/978-981-15-5029-4_71

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-design framework for assessing internet of things applications and platforms. ACM. https://doi.org/10.1145/2991561.2991566

Rahman, A. A. (2015). Comparison of Internet of things (IoT) data link protocols. https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_dlc.pdf

Santos, D. F. S., Almeida, H. O., & Perkusich, A. (2015). A personal connected health system for the Internet of Things based on the Constrained Application Protocol. Computers & Electrical Engineering: An International Journal, 44, 122–136. https://doi.org/10.1016/j.compeleceng.2015.02.020

Unwala, I., Taqvi, Z., & Lu, J. (2018). IoT Security: ZWave and Thread. IEEE. https://doi.org/10.1109/greentech.2018.00040

Xu, C.S., Chen, X.J., Li, D., & Zhong, X.-H. (2008). Automatic electric meter reading system based on ZigBee. IEEE. https://doi.org/10.1109/wicom.2008.712