Security Comparison of Powerline Communication and Wi-Fi Technologies for Internet of Things

Jacob Dimmitt, Mark Reith and Derek Neal
Air Force Institute of Technology, Wright-Patterson Air Force Base, USA

jacob.dimmitt.1@au.af.edu
mark.reith.3@au.af.edu
derek.neal@au.af.edu

Abstract: With the rise of system automation, more devices require intelligence and communication capabilities with a network, which is commonly provided via Internet of Things (IoT) devices. Providing communication stack security for these networks becomes increasingly challenging as the expectations of the systems increase. This paper reviews the current status of physical security network technology and explores innovations made in the past five years to identify and solve cyber vulnerabilities in a variety of contexts and then relates them back to IoT applications. These networked devices are often produced as simply and cheaply as technically feasible, which results in them lacking computational capacity, robust networking hardware and inherent security measures. The review focuses on two main technologies, WiFi and Powerline communications (PLC), to compare research on guided and un-guided media. These technologies can both be considered shared, as it is typical for multiple users to be expected to utilize a shared channel. This means both mediums are vulnerable to wireless jamming, but the effectiveness of this varies greatly based on factors such as the environment, cable shielding and transceiver distance. Similarly, the propagation of signals from the two technologies jeopardizes the potential privacy of communications by leaving them vulnerable to various means of eavesdropping. This can be addressed by using methods such as encryption, which is usually implemented at higher layers of the communication stack to provide confidentiality but can also be applied at the physical layer. Encryption also has the challenge of ensuring key exchange occurs securely which requires unique solutions when the limits of IoT devices are considered. Eavesdropping can also be defeated by controlling the signal-to-noise ratio that is presented to unintended receivers. Additionally, methods of device fingerprinting are being developed to create more robust authentication regimes between devices. Several research opportunities have been proposed where new concepts in one medium are applied to the other.

Keywords: Internet of Things, Powerline communications, WiFi, Physical layer security

1. Introduction

Internet of Things (IoT) devices are a significant portion of the current information technology landscape. The security of these devices can be provided at every layer of the TCP/IP stack, but the physical and data-link layers, which are treated as interchangeable in this paper, provide an interesting collection of challenges and opportunities. The main distinction between different data-link layer technologies is whether they use guided media, such as ethernet and PLC, or unguided media, such as the various frequencies of the electromagnetic spectrum. Both media have received extensive research into their performance and security. In Section 2 of this paper general characteristics of WiFi, IoT and PLC are summarized. Section 3 will cover the physical layer vulnerabilities faced by these technologies. Various countermeasures to these vulnerabilities are covered in section 4. Section 5 will cover the feasibility of applying these countermeasures to IoT implementations. Section 6 will suggest future work and research.

2. IoT, WiFi, and PLC Characteristics

IoT is a broad term that is used to describe a class of computing devices that are typically single purpose and rely on connecting to a network to share information. Another common aspect of these devices is that they are not designed to use robust security methods and are therefore largely insecure (Singh & Singh, 2015). In a study of the device binding methods of 24 popular IoT devices Chen (2019) was able to show that 20 of these devices could be exploited. (Chen et al., 2019). Findings such as these are repeated in a study of smart home devices by Heiding et al. where common IoT vulnerabilities included interception and replay attacks (Heiding et al., 2023). The common explanation for these vulnerabilities is that IoT device designers are constrained by stringent cost and power requirements (Kampourakis et al., 2023).

WiFi is a subset of radio frequency technologies that is a common solution for building IoT networks. Many other radio frequency technologies are also used by IoT devices, but WiFi remains a representative implementation that is explored in this paper. Due to WiFi's ubiquity in today's networking solutions, it has been the subject of intense research into both its performance and security. The main limitation of WiFi implementations is that data rates decrease precipitously with increased distance between transceiver and receiver.

Powerline Communications (PLC) refers to a class of protocols that can be at all levels of the TCP/IP stack, but which are mostly focused on the data-link layer. The main feature of PLC is that it is intended to be used over the existing power line infrastructure. Using such links can be convenient in many scenarios, one of the most common is in Advanced Metering Infrastructure (AMI). Electrical distribution companies can use PLC to measure electrical usage to properly charge customers. One of the main limitations of PLC technologies is that the cables used are often incredibly susceptible to noise generated by various electrical devices on the shared electrical grid (López et al., 2019).

3. Wifi and PLC Vulnerabilities

When assessing the physical layer security of unguided technologies such as WiFi, the first concern is that the signals spread in all directions from a transceiver. An eavesdropper can collect these signals and compromise the secrecy of WiFi communications. In a systematic review of wireless testbeds focusing on IoT devices a team found that WiFi attacks such as eavesdropping and jamming, conducted at the data link layer, constituted a significant portion of the attacks against IoT devices (Kampourakis et al., 2023). Furthermore, since the electromagnetic spectrum is shared other vulnerabilities such as impersonation become possibilities. Impersonation can be achieved using a variety of techniques such as the forging of passwords, SSIDs, and MAC/IP addresses (Yan et al., 2023) .

Guided technologies such as PLC do not suffer from these vulnerabilities in the same way. Since powerlines are usually unshielded and their physical security not assured, an attacker can exploit them to eavesdrop on a channel. (Filomeno 2023). Camponogara (2022) has shown that wireless receivers can be installed near a PLC transmitter to effectively extract the signal from the unintentional emissions of the power line. Their technique required being within two meters of the transceiver when a single device was used or being within six meters when 10 devices were strategically placed around the transceiver. As shown by Uwaezuko (2021), PLC networks can also be vulnerable to jamming attacks that, in their paper, were used to further enable MAC and DHCP spoofing. However, they asserted that “To execute these attacks, the attacker should have access to the power line wiring where the PLC network is hosted.” (Uwaezuko 2021).

4. Security Techniques

Several different frameworks for physical layer security have been proposed. In the comprehensive study done by Hamareh et. al. the mechanisms of physical layer security are split into two primary categories: Signal-to-Interference-and-Noise Ratio (SINR) and Complexity. SINR utilizes various technologies to make a transceiver’s signal difficult to discern by an eavesdropper while minimizing disturbance to the intended receiver. Complexity methods focus on encryption systems to provide security (Hamamreh et al., 2019). Similarly, in a review of how artificial intelligence is being used to provide IoT security the main security recommendations for physical layer security focused on the use of encryption (Kuzlu et al., 2021). A different framework for categorizing IoT security is used by Rachit et al. that values a system’s ability to provide confidentiality, integrity, availability, trust, and authenticity (Rachit et al., 2021).

The introduction of artificial noise to a PLC network is a primary method of achieving SINR security. A mathematical model to determine the theoretical secrecy of a PLC network is derived by Mohan (2019). In their model both distance from the transceiver and noise are significant variables in the effectiveness of an eavesdropper (Mohan et al., 2019). The model is shown to be held in experiments conducted by Camponogara (2022), where they concluded that secrecy is severally compromised when a single wireless receiver can be placed within 2 meters of a PLC transceiver or when an array can be placed within 6 meters. The experiment was conducted on an ‘in-home’ PLC environment where intentional noise generation was not used. When intentional noise generation was used by De L. Filomeno et al. (2023), the noise caused an elevated Bit Error rate for the passive eavesdropper beyond that of the intended receiver, even when the eavesdropper was close to the transceiver.

Artificial noise has applications for WiFi physical layer security as well. The basic concept is explored thoroughly in the Hamamreh et al. paper. Recent experiments such as those conducted by Wang (2021) show an evolution of the idea where artificial interference is combined with secret spreading codes. In most implementations the transceiver produces the noise, however a receiver can also be tasked with creating noise (Costa et al., 2023).

In the Hamamreh paper, authentication is mostly presented as a byproduct of channel secrecy. However, several techniques have developed that can utilize physical characteristics of a device to provide authentication and therefore increase resistance to impersonation. The need for such identification techniques was stated explicitly

by Mamdouh et al. (2021) to improve the security of IoT devices in the health field. Migulez-Gomez and Rojas-Nastrucci (2022) show a technique on discerning unique fingerprints from the WiFi signals of an additively manufactured antenna. Similar results are obtained by Zhang et al. (2019) where the Specific emitter identification of a WiFi preamble signal to discern between different devices. Finally, Yan et al. (2019) demonstrates the real time identification of rouge WiFi devices via channel state information, which has the advantage of being difficult for a rouge actor to impersonate. It is proposed that any of the methods can be used as an additional step when conducting authentication, increasing the security of a system.

Device fingerprinting has also been extended to be used to uniquely identify devices on a PLC network. Ross et al. (2017) shows that it is possible to discriminate between PLC devices by observing the slight differences in how they transmit standard signals. They conclude that utilizing this as part of a two-factor authentication solution "will vastly improve the systems intrusion detection/prevention."

The above identification methods could be integrated into the Software Defined Networking (SDN) scheme proposed by Szymanski (2017). In their method, deterministic schedules for channel use and encryption parameters are used to identify unauthorized communication at the data link layer. Combining SDN with identifying physical characteristics of the individual devices could improve a network's ability to ensure trust and authenticity.

Also of interest are Hybrid networks, where both PLC and WiFi are used, which can be advantageous for performance reasons, with the drawback of complex synchronization processes (Dib et al., 2018). In their paper, Camponogara shows that these systems can also be configured to provide security that exceeds that of either communication system on their own. (Camponogara et al., 2019)

5. IoT Challenges

Current IoT devices will not be good fits for many of the above physical layer security solutions. Those that rely upon intentional noise generation generally require an additional method of transmitting such as a secondary antenna or network interface, which could significantly increase cost. More complex encryption methods require greater computation capacity, which is limited in IoT devices. IoT devices that are on networks with separate devices responsible for security may be feasible as suggested by Uwaezuoke & Swar (2021). These separate devices could be crafted to utilize the techniques discussed such as device discrimination based on fingerprinting. The additional hardware could also produce the artificial noise and Software defined networking capabilities suggested.

6. Future Work

The secrecy of a physical layer implementation is explored greatly in the above resources, however many of the experiments performed are on systems with less than 3 devices. Obvious future research projects include applying the individual techniques directly to IoT implementations, with a focus on mesh networks that have multiple transceivers and receivers. Another avenue would be implementing multiple of these controls simultaneously to ensure they can coexist. For example, Intentional noise generation may interfere with the capability of a system to perform effective fingerprinting. Current physical layer security could also be improved by research into other aspects of security than confidentiality such as the integrity and availability of a system. Since it has been shown that a wireless receiver can eavesdrop on a PLC channel a logical next step is if a wireless transmitter could be used to effectively interfere with that same channel. Finally, since many authors have presented device fingerprinting as an effective security measure, research into programmatic ways of spoofing these immutable characteristics should be conducted.

7. Conclusion

The specific challenges to the physical layer security of IoT devices relies upon the communication medium they utilize. The methods to combat these challenges, however, share several similarities. The signal to noise ratio of a transmission can be manipulated in various ways to prevent a potential eavesdropper from being able to discern the original signal. Difficult to replicate physical features of transmitters, and the resulting unique characteristics of their transmissions, can also be used as additional means of device authentication. Complex ways of controlling communications such as encryption or deterministic scheduling represent aspirational goals but may not be achievable on the common low power IoT device.

Material and Methods: Conducting Research was done by searching on IEEE Xplore. Two searches were conducted. The first included the key words 'PLC Security' and 'Internet of Things' and was restricted to the years after 2014. This yielded 80 results. The second included the key words 'Wi-Fi Security' and 'Cyber Security' and was also restricted to the years after 2014. This yielded 64 results. Springer Nature Link was searched with the term Powerline communication, after 2019, subject Internet of Things. This yielded 78 results. Springer Nature Line was also searched with the term Wifi security, after 2019, subject Internet of Things, and restricted to review articles. This yielded 77 results. Computers & Security was searched via Science Direct with the search term Powerline communication which yielded 8 results. Computers & Security was also searched with the term Wifi Security and restricted to the years after 2019 which yielded 114 results. The above searches were manually filtered by reviews of the papers' titles and abstracts for relevance to this paper. Resulting in a total of 23 sources being included.

Data Availability: Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Conflicts of Interest: The author declares that they do not have a conflict of interest in the subject of this article.

Funding Statement: The author declares they did not receive any funding to support this research.

Disclaimer: The views expressed are those of the authors and do not reflect the official policy or position of the US Air Force, Department of Defense or the US Government.

AI Declaration: AI tools, offered by Grammarly, were used for proofreading. These pointed out spelling and grammar issues and suggested changes.

Ethics Declaration: Ethical clearance was not required for this research.

References

Camponogara, Â., Poor, H. V., & Ribeiro, M. V. (2019). The Complete and Incomplete Low-Bit-Rate Hybrid PLC/Wireless Channel Models: Physical Layer Security Analyses. *IEEE Internet of Things Journal*, *6*(2), 2760–2769. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2018.2874377

Camponogara, Â., Souza, R. D., & Ribeiro, M. V. (2022). The Effective Secrecy Throughput of a Broadband Power Line Communication System Under the Presence of Colluding Wireless Eavesdroppers. *IEEE Access*, *10*, 85019–85029. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3197528

Chen, J., Sun, M., & Zhang, K. (2019). Security Analysis of Device Binding for IP-based IoT Devices. *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 900–905. https://doi.org/10.1109/PERCOMW.2019.8730580

Costa, G., Degano, P., Galletta, L., & Soderi, S. (2023). Formally verifying security protocols built on watermarking and jamming. *Computers & Security*, *128*, 103133. https://doi.org/10.1016/j.cose.2023.103133

De L. Filomeno, M., Campos, G. M., Camponogara, Â., Sartorello, P. H., & Ribeiro, M. V. (2023). Artificial Noise for In-Home PLC Networks Under the Presence of PLC and Wireless Eavesdroppers. *2023 Symposium on Internet of Things (SIoT)*, 1–5. https://doi.org/10.1109/SIoT60039.2023.10389936

Dib, L. de M. B. A., Fernandes, V., de L. Filomeno, M., & Ribeiro, M. V. (2018). Hybrid PLC/Wireless Communication for Smart Grids and Internet of Things Applications. *IEEE Internet of Things Journal*, *5*(2), 655–667. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2017.2764747

Hamamreh, J. M., Furqan, H. M., & Arslan, H. (2019). Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1773–1828. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2018.2878035

Heiding, F., Süren, E., Olegård, J., & Lagerström, R. (2023). Penetration testing of connected households. *Computers & Security*, *126*, 103067. https://doi.org/10.1016/j.cose.2022.103067

Kampourakis, V., Gkioulos, V., & Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. *Computers & Security*, *133*, 103383. https://doi.org/10.1016/j.cose.2023.103383

Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(1), 7. https://doi.org/10.1007/s43926-020-00001-4

López, G., Matanza, J., De La Vega, D., Castro, M., Arrinda, A., Moreno, J. I., & Sendin, A. (2019). The Role of Power Line Communications in the Smart Grid Revisited: Applications, Challenges, and Research Initiatives. *IEEE Access*, *7*, 117346–117368. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2928391

Mamdouh, M., Awad, A. I., Khalaf, A. A. M., & Hamed, H. F. A. (2021). Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. *Computers & Security*, *111*, 102491. https://doi.org/10.1016/j.cose.2021.102491

Miguélez-Gómez, N., & Rojas-Nastrucci, E. A. (2022). Antenna Additively Manufactured Engineered Fingerprinting for Physical-Layer Security Enhancement for Wireless Communications. *IEEE Open Journal of Antennas and Propagation*, *3*, 637–651. IEEE Open Journal of Antennas and Propagation. https://doi.org/10.1109/OJAP.2022.3181325

Mohan, V., Mathur, A., Aishwarya, V., & Bhargav, S. (2019). Secrecy Analysis of PLC System with Channel Gain and Impulsive Noise. *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, 1–6. https://doi.org/10.1109/VTCFall.2019.8890986

Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. *SN Applied Sciences*, *3*(1), 121. https://doi.org/10.1007/s42452-021-04156-9

Ross, B. P., Carbino, T. J., & Stone, S. J. (2017). Physical-Layer discrimination of Power Line Communications. *2017 International Conference on Computing, Networking and Communications (ICNC)*, 341–345. https://doi.org/10.1109/ICCNC.2017.7876151

Singh, S., & Singh, N. (2015). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 1577–1581. https://doi.org/10.1109/ICGCIoT.2015.7380718

Szymanski, T. H. (2017). Strengthening security and privacy in an ultra-dense green 5G Radio Access Network for the industrial and tactile Internet of Things. *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 415–422. https://doi.org/10.1109/IWCMC.2017.7986322

Ul Haq, S., Singh, Y., Sharma, A., Gupta, R., & Gupta, D. (2023). A survey on IoT & embedded device firmware security: Architecture, extraction techniques, and vulnerability analysis frameworks. *Discover Internet of Things*, *3*(1), 17. https://doi.org/10.1007/s43926-023-00045-2

Uwaezuoke, E. C., & Swart, T. G. (2021). Network Attack Analysis of an Indoor Power Line Communication Network. *2021 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, 96–101. https://doi.org/10.1109/ISPLC52837.2021.9628606

Wang, Q. (2021). Defending wireless communication against eavesdropping attacks using secret spreading codes and artificial interference. *Computers & Security*, *103*, 102175. https://doi.org/10.1016/j.cose.2020.102175

Yan, D., Yan, Y., Yang, P., Song, W.-Z., Li, X.-Y., & Liu, P. (2023). Real-Time Identification of Rogue WiFi Connections in the Wild. *IEEE Internet of Things Journal*, *10*(7), 6042–6058. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2022.3223682

Zhang, Y., Lin, Y., Dou, Z., Wang, M., & Li, W. (2019). Monitoring and Identification of WiFi Devices for Internet of Things Security. *2019 IEEE Globecom Workshops (GC Wkshps)*, 1–5. https://doi.org/10.1109/GCWkshps45667.2019.9024626