Lightweight Security Protocols for Battery-Powered Wireless Devices

Tarakesh Kotha

1 Introduction

Wireless technologies have changed significantly, making it easier to create huge networks linking many Internet-Of-Things (IoT) devices together. Hundreds of thousands of battery operated, wireless devices are in use today for health care monitoring, automation, environmental sensing and smart cities. These new uses have created many new security issues due to the number of resource-constrained (low power) devices communicating securely but at an extremely low energy level. Research done recently shows that designing a lightweight security architecture is quickly becoming a requirement to solving these types of problems for a resource-constrained wireless environment. [**?**].

The hardware limitations on embedded devices that use battery to power themselves and are connected through wireless networks include limited processing power, limited memory, and finite amounts of battery power. Cryptographic security protocols that were developed many years ago were made for computing systems with high end performance, meaning that now when trying to implement them within low-end wireless devices they cannot be accomplished quickly or efficiently. This has resulted in energy-efficient designed cryptographic protocol becoming critical to current research in embedded wireless security field.

Due to open radio-frequency transmission channels, wireless communication environments also present various types of additional vulnerabilities. These vulnerabilities can allow adversaries to carry out various types of attacks (i.e., passive eavesdropping or replay attacks) without having to gain physical access to the communication infrastructure or impersonate the communication devices involved in the communication. In order to address these vulnerabilities, lightweight security protocols provide confidentiality, integrity, authentication, and availability in addition to minimizing computational and communication overhead. [7].

The development of wireless communication technologies has changed how we connect with each other in computer and data processing systems drastically. Wireless devices are now embedded in everything we use on a daily basis, which allows us to create

many different kinds of networks by combining smaller battery-operated devices to sense, process, and send out information. These devices are what create the foundation for cyber-physical systems, which enable smart systems to exist in many different areas such as health monitoring, industrial automation, and environmental monitoring; agricultural automation; transportation; and smart city systems. The change from central-by-device systems (such as a mainframe computer) to a set of distributed wireless devices (like a smartphone) has allowed for much greater scalability and easier deployment of new systems. But, because there are so many types of devices in these distributed systems, there are many new complexities and vulnerabilities when it comes to designing secure systems within the constraints of their environment.

Energy consumption in wireless embedded devices is dominated by radio frequency communication operations. Wireless data transmission typically consumes significantly more energy compared to local computational processing. As a result, communication overhead directly influences device operational lifetime. Security protocol designers must therefore carefully minimize communication message exchange frequency and optimize message size to reduce transmission energy consumption. In addition to communication energy cost, cryptographic computation energy consumption must also be carefully optimized. Traditional cryptographic algorithms such as RSA and standard implementations of Transport Layer Security require high computational complexity and multiple communication handshake operations. Direct implementation of such protocols in constrained wireless devices results in excessive energy consumption and rapid battery depletion.

The security of any wireless communication environment is affected by the openness of wireless signals - which can be transmitted in any direction, simply by the existence of an open physical space. Thus, an adversary can perform passive eavesdropping on wireless signals by intercepting them without being detected. Furthermore, an adversarial attack that causes disruption of network communications and/or integrity of data is accomplished through active eavesdropping (e.g., through replay attacks, impersonation attacks, and/or man-in-the-middle attacks). If a given distributed wireless sensor network node has a vulnerability, the physical device may also be compromised due to the distributed and usually unattended nature of wireless equipment installations. Through a hardware-based attack (e.g., by taking advantage of a side-channel analysis), attackers can extract cryptographic secrets directly from the memory of a device.

Lightweight security protocols have developed as a specific research area designed to solve these issues through the provision of both energy-efficient security and optimized computationally-based security mechanisms. They provide the basic security services such as data confidentiality, message integrity, device authentication, and network availability while minimizing the computational overhead and communication cost.

Lightweight security protocols are required to optimize the design of the cryptographic primitives, communication handshake protocols, and key management architectures. The

main objective is to obtain an optimal trade-off between the strength of security and energy consumption. Security computations require the use of excessive amounts of energy and can decrease the operational lifetime of the devices. Conversely, if there is not enough security protection, critical infrastructure systems can be subject to cyber-attacks.

As a result of the IoT ecosystem's evolution, lightweight security protocol research has become increasingly relevant to the security of the IoT ecosystem. Today's IoT deployments have a large number of different devices (i.e., heterogeneous populations) that differ from each other in terms of their computation, power, and communication technologies. Therefore, security protocols need to be scalable and flexible enough to accommodate the variety of different deployment environments throughout the IoT ecosystem. When deployment of a large number of devices occurs through a wide range of geographical locations in a large-scale IoT environment, a centralized security architecture has the potential to introduce scalability constraints and a single point of failure within that architecture. On the other hand, lightweight distributed security architectures allow for greater scalability and resiliency than centralized architectures, but they also add complexity to the protocols.

The advancements in semiconductor manufacturing techniques and architectures of embedded systems have recently led to the introduction of application-specific hardware accelerators for performing cryptographic algorithms in a more efficient manner compared to software implementations running on general-purpose microcontrollers. By using hardware instead of software to accelerate cryptographic operations, embedded wireless devices will be able to utilize stronger cryptographic protocols while still keeping their energy costs low. Current research is being conducted on the use of energy harvesting technologies that could help to improve the operation length of wireless devices in the future. Wireless devices that use energy harvesting can also dynamically vary their level of security based on the amount of energy that they have been able to harvest.

The increased use of wireless embedded systems in critical infrastructure demonstrates the need for strong light-weight security measures. Wireless body sensor networks (WBSN) are used for continuous monitoring of patient vital signs within healthcare monitoring systems. Wireless sensor networks (WSNs) are used to monitor industrial production processes and identify real-time anomalies in industrial automation systems. Wireless communications are used for real-time monitoring and control of power distribution within smart grid energy distribution systems. Security incidents in these systems can create safety hazards, monetary losses and disruption to operations. Therefore, there is an immediate need for the creation of strong energy-efficient lightweight security protocols to enable reliable implementation of next-generation wireless embedded systems.

2 Background and Conceptual Foundations

Wireless embedded devices work under limited resources such as limited processing power and battery size. The design of security protocols must take into consideration both the performance of algorithms and level of protection provided due to limited computational resources. [6].Many wireless sensor networks are deployed in areas that make changing out batteries costly. In addition, communication is typically a much more energy intensive operation than performing local computations, making the development of communication-efficient security protocols essential.

Lightweight cryptographic protocols are continuing to be developed in order to create secure solutions for wireless embedded systems operating under energy constraints. [7].

Current Lightweight Cryptography focused on creating testing security primitives for embedded devices. Lightweight Cryptography algorithms were developed to minimize the processing complexity of hardware while still providing a suitable level of resistance against all attacks using traditional means of cryptoanalysis. [7].Additionally, research has also begun looking into development of Post-Quantum Lightweight Cryptography to provide an ongoing level of secure protection against possible future threats from Quantum Computers. [2].

Battery-powered wireless system designs rely on the architectures of embedded communication devices, which help establish the connection between the two. The difference between traditional computing systems and those based on the wireless communication conventions is that the wireless environment places stricter constraints on the design of the embedded communication system to conserve energy, and because of this, embedded wireless systems are generally constructed to be as small as possible physically and to operate autonomously for extended periods of time without recharging their batteries.

In order for any existing wireless design to accommodate an embedded wireless device, the design requirements must include considerations for the constraints of the available resources on that device, the properties of the wireless communication and the evolution of research into cryptographically secure solutions in resource-constrained environments.

Ultra-Low Power Microcontrollers are typically used in wireless battery operated products. Ultra-low power microcontrollers must operate at lower clock frequencies than what is typical for General Purpose Processors, and overall have a limited throughput for executing instructions. The memory architecture for these devices is also limited in terms of the available volatile and non-volatile storage resources for cryptographic purposes and storing the states of protocols in the memory of the device. As a result, implementations of crypto protocols need to be sized and designed to use minimal code size and minimum memory allocations at runtime. As such, if the library of cryptography becomes too large, it will potentially overflow in the memory and cause excess numbers of instructions to have to be executed, which will consume energy as well as potentially lead to a total

failure of the device due to its excess number of memory overflow conditions.

In regards to wireless and embedded devices, the availability of energy is considered to be the core operational constraint. Many wireless sensor networks are located at sites which are inconvenient to replace batteries, and as such, tend to be very costly to replace. Examples of this are structural health monitoring systems on bridges, environmental monitoring systems within forests, and industrial monitoring systems located within hazardous environments. In these instances, devices are required to function over several years with limited energy stored within them. Wireless radio transmission requires more energy to transmit than local computational processing uses; thus, the design of communication efficient security protocols is thus very important when trying to extend the lifetime of a device.

Radio frequency broadcasts do not require actual access to an area before they can be intercepted because wireless communication utilizes radio waves to connect devices. Instead of using cables to connect to the Internet, users can establish a connection without being at the same location as the device they are connecting to. An attacker can conduct passive traffic analysis to determine how the network or system behaves based on its communication patterns and eventually gain access to the target device after reviewing that data. A form of active attack could occur with replay attacks or through impersonation. A replay attack is defined as the unauthorized re-transmission of data that has already been sent to the network and will interfere with the operation of the network or device it is targeting. An impersonation attack is defined as the use of a rogue device attempting to connect to a legitimate wireless network and sending invalid or incorrect information to that network as if it were actually connected to that network. In order to mitigate these attacks, all devices that access wireless networks, including constrained devices, must implement strong authentication and encryption methods.

The compromise of physical devices presents another attack vector for wireless embedded systems. Many wireless systems are found in physical environments that are primarily unattended; therefore, an attacker may conduct hardware-level attacks against the system in order to retrieve cryptographic keys. Examples of the types of attacks that could be used to compromise an embedded device include fault injection attacks, memory extraction attacks, and side channel analysis attacks. Consequently, lightweight security architectures must implement mechanisms for secure key storage, key revocation, and the isolation of compromised nodes; these mechanisms will allow for continued protection of network security regardless of whether or not individual nodes have been compromised.

In recent years, there have been many advancements in lightweight security research due to the development of global standards for the use of cryptography. Many organizations around the world run evaluation programs that analyze the performance of numerous lightweight cryptographic algorithms to determine their suitability to be used as commercial grade solutions. In addition, by testing different types of algorithms against multiple

performance metrics (such as energy efficiency, computation complexity, and memory requirements) and providing the results from vulnerability analysis using confidentiality methods, organizations also have completed an international standards certification process with some trade-offs associated with these algorithms. Ultimately, this work has resulted in the creation of numerous standardised lightweight cryptographic primitives that can be used as part of commercial embedded product solutions.

The current landscape of contemporary lightweight security research encompasses the assessment of sustainable longevity regarding the domain of cryptography. The emergence of sizable quantum computers could jeopardize the security of multiple existing cryptographic methods; therefore, researchers are developing lightweight and quantum-proof alternatives to current standards to use with embedded devices. The intended design criteria for these new methods are to provide resistance to quantum cryptanalysis without requiring excess CPU cycles or power usage.

A major advancement to lightweight security research is the integration of cross-layer optimization strategies. Security protocol designs today typically treat each of their independent system layers (e.g. Communication, computation and routing) as distinct systems. Cross-layer security optimization allows these protocols to be responsive to the current state of the network e.g. (load, availability, the energy of device), the network and characteristics of the communication channel and dynamically adjust. Therefore, efficient use of limited resources on devices can be achieved with cross-layer security optimization through providing a necessary level of security.

Lightweight Wireless Security (Protection) Measures rely on a number of basic principles that include: multiple types of physically limited capabilities (constraints), communication characteristics, algorithmic design for cryptography, and an evolving set of cyber threats; to develop lightweight secured protection protocols. Future work in developing lightweight secured protection protocols can be accomplished by employing a multidisciplinary approach, which will include developing loyalty-based systems; using wireless telecommunications engineers' processes; applying cryptographic and mathematical techniques; and utilizing cyber threats models to support the development of lightweight secured protection protocols.

3 Core Concepts and Approaches

Encryption algorithms are continuously modified for less energy usage and reasonable security levels; the algorithms have less complex substitution and permutation structures along with fewer number of computational rounAuthentication protocols that provide sufficient integrity to maintain secured communications across distributed IoT systems will still apply encryption and authentication together to reduce communication overhead. [9].

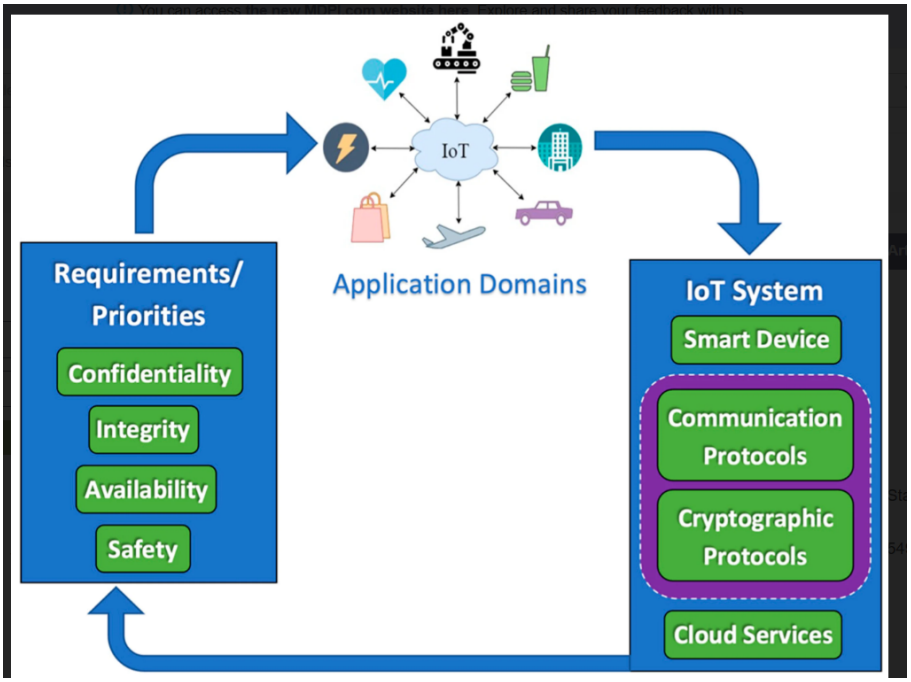

Figure 1: Lightweight security architecture for battery-powered wireless IoT devices. The architecture illustrates interaction between sensing nodes, gateway nodes, and cloud-based secure processing layers. Source: Adapted from Li et al., 2024 [**?**].

Using an adaptive security framework allows for dynamic adjustment of the strength of encryption based on how much battery is left, and the risk level of the network at any given time. Adaptive systems are a major improvement to overall energy efficiency while still providing a high level of security. [**?**].

As shown in Figure 2, cryptographic algorithm selection significantly impacts energy consumption in constrained wireless devices. Lightweight cryptographic primitives provide improved battery efficiency compared to computationally intensive security algorithms.

Deriving a light weight security protocol for battery operated wireless devices includes efficiently combining optimized cryptography algorithms, efficient authentication method(s) (s) and means, scalable key management systems (s) and means, and energy conscious wireless communications means/methods.

When these components are combined they will provide a secure solution which provides strong security assurances while having a low to no power consumption and a low to no computational burden.

In order to provide lightweight security methods it will be necessary to find a proper balance between the mathematics used for the cryptography and the hardware implementation. This balance is extremely important due to the limited resources present on most wireless devices which do not allow for the same level of computationally extensive type of security operations as those normally performed in a more traditional computer

environment.

Lightweight stream cipher encryption presents a viable alternative to the traditional key set-based block cipher approach when working with constrained devices. In contrast to the traditional key set-based block cipher approach, which utilizes multiple keys each creating unique encryptions of data, stream ciphers produce encrypted messages through the process of combining original data with some other input (key) that can change frequently enough to create a pseudo-random value. Compared to a comparable block cipher implementation, most stream ciphers will require less memory space for performing encryption and decryption operations and are ideal for real-time wireless communication systems exchanging continuous streams of information between both ends of the communication medium. Additionally, stream cipher hardware can provide less latency and improved energy efficiency than their block cipher algorithm counterparts.

The protocols known as lightweight authentication are a key component of lightweight security. As wireless networks utilize open radio frequency communications, there is a risk of unauthorized devices gaining access to them. Lightweight authentication protocols are intended to limit participation in wireless network communication to legitimate devices and therefore limit the amount of communication needed for authentication. The requirement of exchanging multiple messages for authentication is a typical characteristic of traditional authentication protocols. The development of lightweight authentication protocols has resulted in significant reductions in communication overhead through the combination of authentication and encryption functions into a single protocol, which provides strong identity verification with lower latency and energy consumption.

Challenge-response authentication is commonly used as a lightweight security protocol, allowing two devices to authenticate their identities with minimal authentication data exchanged. Efficient authentication methods include cryptographic hash functions and message authentication codes that have low resource requirements. Currently, there are ongoing studies into new emerging wireless physical layer authentication methods that are based on the characteristics of radio frequency signals (e.g. channel state information) and how those signals propagating through the real world can be used for device authentication. Adding a physical layer authentication mechanism provides an additional layer of security with negligible resource requirements.

Cryptographic acceleration also referred to as hardware-assisted cryptography, is another important principle of lightweight security design. Many microcontrollers now have specialized hardware blocks that can perform cryptographic acceleration much faster than a software implementation may be able to do. By using hardware-based cryptographic acceleration, any computation/computed operation required by the security solution will consume less energy; therefore, using cryptographic hardware-based accelerators will improve the total amount of energy consumed while performing computations/computer operations, improve performance of the security solution and provide greater protection

from side channel attacks (the exploitation of an application by the misuse of software).

The design of lightweight security protocols involves multiple core components, such as optimizing cryptographic algorithms, efficient authentication techniques, scalable key management frameworks, adaptive energy-aware security strategies, and hardware-assisted cryptographic processing. By combining these different components together, you can establish an effective level of security protection that has very little energy usage and is not computationally intensive for wireless devices operating on batteries.

3.1 Lightweight Encryption Mechanisms

Lightweight encryption systems have been designed to reduce the computational complexity associated with performing operations requiring only moderate levels of security. To do this, lightweight encryption systems make use of a reduced number of rounds of cryptographic transformation (i.e., fewer numbers), smaller keys (i.e., keys that are appropriate for devices having limited amounts of resources), and very simple substitution-permutation structures. The goal of lightweight encryptions is to reduce the total number of processor cycles and memory consumption while providing classical attack resistance using traditional encryption techniques. Because frequent encryptions occur within wireless sensor networks, lightweight encryption technologies have become increasingly important in these types of networks.

3.2 Lightweight Authentication Techniques

Wireless networks rely on many different types of authentication to ensure that only authorized devices can communicate over a wireless network. To reduce the cost of handshaking, lightweight authentication protocols use a single protocol that combines both authentication and encryption functions. Challenge-response authentication and message authentication code based (MAC) methods of authenticating devices in constrained wireless environments have been extensively employed. Recently, physical layer or RF characteristics of RF signals (for example) are also being used as an additional security mechanism for authenticating device identity.

3.3 Efficient Key Management Strategies

In wireless networks having multiple access points, the need for efficient key management is imperative to provide long-term security. The lightweight methods for key establishment, key pre-distribution, dynamic generation of keys, or hybrid key lifecycle management frameworks all allow the use of less storage space and less computing power during the runtime of the network. The secure storage methods of cryptographic keys should prevent attackers who breach the physical device from using the cryptographic keys.

3.4 Energy-Aware Security Protocol Design

In order to create security protocols that take into consideration the power levels of devices, it is important to develop security protocols that take into consideration device battery levels as a factor when designing a secure communication framework. For example, adaptive security protocols may adjust their level of encrypted data or authentication based on the battery level of the device. Additionally, communications scheduling techniques can be used to coordinate cryptographic operations with a device's sleep cycle to help minimize the energy consumed to perform these operations.

4 Comparative Discussion

In limited-resource wireless networks, hybrid cryptographic architectures balance energy performance and security strength. Due to using asymmetric cryptography for authenticating the user and symmetric cryptography for data transmission, the combined use of both types of cryptography will allow performance to meet user expectations at a lower cost per transaction symmetric cryptography for efficient data transmission [7]. Increasing cryptographic strength usually increases the amount of computational energy used by the device to process all of the encryption/decryption operations; therefore, very careful optimization of devices powered by batteries must take place.

Long-term security and resilience for post-quantum lightweight cryptography is a developing area of research by academia and industry to provide strong cryptographic protection against new quantum computing threats while minimizing the amount of computational resources required to do this. [2].

With respect to computational efficiency and energy use, lightweight versions of cryptographic protocols based on symmetric (secret key) cryptography typically outperform those based on asymmetric (public key) cryptography. By requiring fewer processor cycles and using less total memory space, symmetric encryption operations are an appropriate candidate for use on ultra low power/wireless embedded devices. Furthermore, many symmetric encryption algorithms can be constructed with a simpler type of hardware architecture, which subsequently makes integration into the embedded microcontroller architectures much more efficient. Major operational difficulties exist when trying to distribute symmetric (secret) keys in a secure manner and also having secured (revoked) keys in large scale wireless networks so that the symmetric keys can be distributed to thousands of devices without the risk of being intercepted or compromised.

Using lightweight asymmetric protocols provides a more scalable method for establishing trust than traditional means of doing so, because a device can authenticate another device using a public key instead of having to know the private keys they share. This ability to perform this type of mutual authentication between two wireless devices without

knowing their common shared keys is beneficial to dynamic wireless networks in which the number of devices connected can frequently change with devices joining and leaving the network. Implementing public key cryptography allows for easier provisioning of new devices onto an existing wireless network, making onboarding procedure for secondary devices much less cumbersome. However, as compared with symmetric function algorithms, asymmetric cryptographic function algorithms require a significant amount of resources to perform their cryptographic operations; therefore, even though public-key cryptography uses less processing power when utilizing optimized public-key algorithms than non-optimized algorithms, asymmetric functions will still require significantly more processing power to achieve the encryption capabilities than would be required using symmetric encryption, and thus use a much higher level of energy to execute functions as asymmetric encryption. Although elliptic curve cryptography has improved efficiency of constrained wireless environments through reducing computation overhead and increasing practicality, it continues to generate higher levels of energy use than more traditional forms of symmetric cryptography.

Energy use will be one of the key evaluation criteria when deciding if a lightweight security protocol can be selected to provide adequate security. For protocols that have complicated handshaking, and/or have many pairs of authenticated messages, will typically require much more energy to provide security because of the increased radio communications. Also, cryptographic algorithms require a lot of energy to run on a processor due to the large number of complex mathematical computations required. Lightweight protocols that combine authentication and encryption in one operation will typically use the least amount of energy. Energy used for cryptographic operations can be reduced dramatically by using hardware acceleration when performing these operations with lightweight protocols.

Another significant element to compare between different encryption algorithms is the amount of memory used. Many low-resource cryptographic methods have larger table lookups / pre-computed S-boxes and, therefore, tend to use more memory than ultra low power / cost devices can support, though the minimum memory footprint protocols are the best fit for ultra-low-cost embedded devices with very little internal memory. While developing a low/memory footprint protocol, the resultant design will often create a balancing act (or trade-off) between computational complexity and storage requirements.

Emerging cybersecurity threats bring with them new metrics to evaluate how well organizations can protect themselves from cyber attacks and how quickly they can return to normal operations thereafter. While most of the lightweight cryptographic protocols that are currently being used to secure data and communications over the Internet do so based upon conventional computational-principle-based encryption, the new technology that has been evolving rapidly and has the potential for widespread use in the next 10

to 20 years will likely lead to the vulnerabilities of many of the current deployed cryptographic algorithms being fully exposed. Thus, all those engaged in research to create lightweight post-quantum cryptographic protocols will very likely create secure cryptographic algorithms that can be used to protect against quantum-based computer attacks, but the post-quantum cryptographic protocols being developed today will require considerably more computational processing power per transaction than existing generation wireless communications devices can provide.

.

When comparing different lightweight security protocols, in addition to understanding how strong the protocol is, end-users also need to look at other aspects of the system as a whole. The ideal lightweight security protocol offers a reasonable trade-off among energy consumption, computing power required, ability to manufacture large amounts, ease of maintenance, and robustness against attacks. The study of future lightweight security protocols will likely include developing adaptive protocols that are able to modify their security operations based on the energy available (battery charge), the current state of the network and the presence of possible attacks.

4.1 Symmetric and Asymmetric Cryptography Comparison

When it comes to cryptography, symmetric cryptography provides greater computational effectiveness and consumes less energy than asymmetric cryptography due to how the two forms of cryptography operate. The disadvantage of symmetric cryptography, however, is that it is much more difficult to distribute encrypted keys when there are many wireless devices. In this regard, asymmetric cryptography eliminates the difficulty of establishing trust between devices; however, it uses more computing resources than symmetric cryptography. Hybrid security architectures use both symmetric and asymmetric cryptography.

4.2 Energy Efficiency and Security Tradeoff

In general, there is a direct relationship between enhanced cryptographic strength and increased energy consumption (both computation and communications). As such, when designing lightweight security protocols, designers use a trade-off method to provide adequate security protection while minimizing battery energy use. In some cases, the use of a hardware-based cryptographic accelerator will significantly reduce energy consumption.

4.3 Scalability Considerations in Large IoT Networks

There is a requirement for security protocols in large IoT networks for efficient group-authentication and to scale the size of the keys. Centralised security architectures tend

to offer simpler management procedures, but also have a higher degree of a single point of failure. On the other hand, distributed architectures provide higher levels of redundancy, but also add complexity to the protocol.

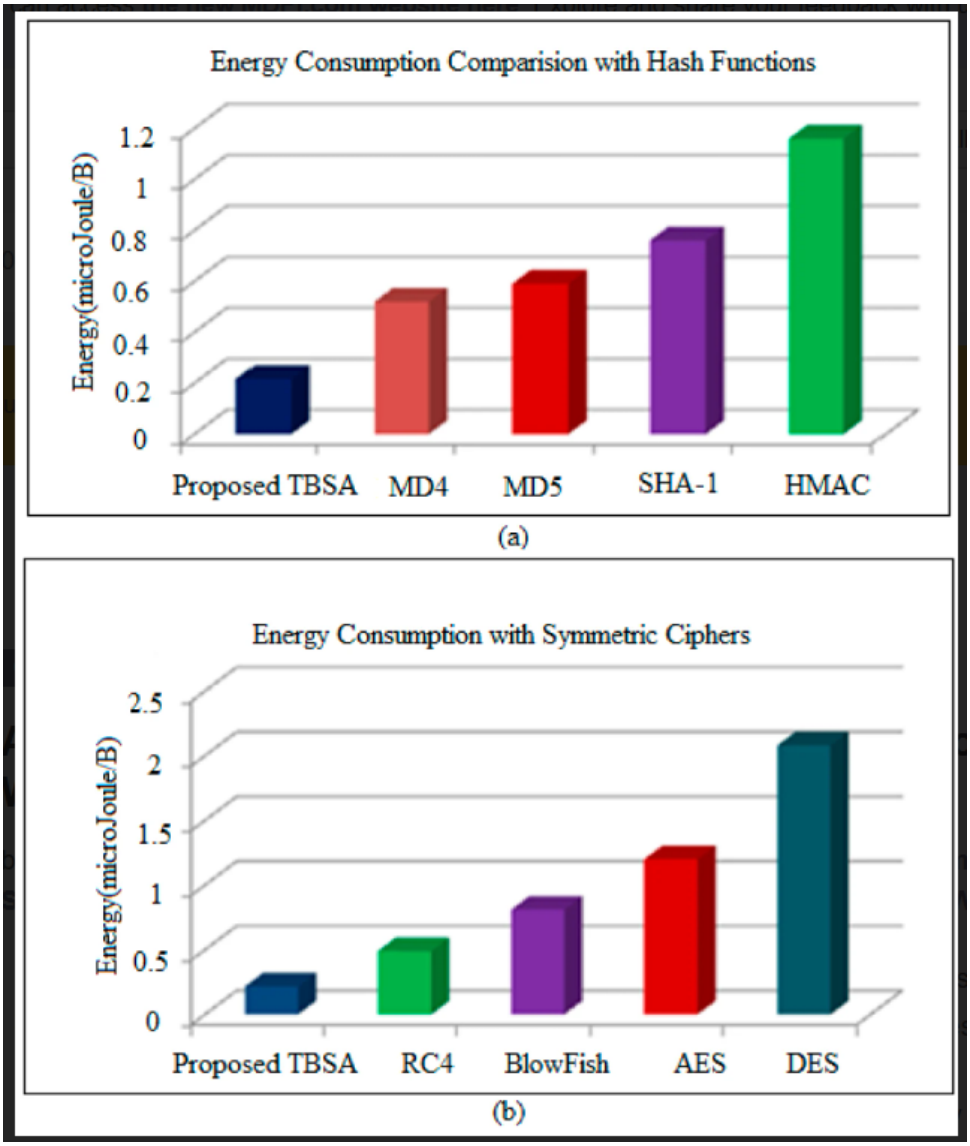

Figure 2: Energy consumption comparison of cryptographic primitives in wireless embedded systems. The upper graph shows energy usage of hash functions, while the lower graph compares symmetric encryption algorithms. The results highlight the importance of lightweight cryptographic design for battery-powered wireless devices. Source: Adapted from recent lightweight cryptographic energy evaluation studies [7, 7].

Table 1: Comparison of lightweight cryptographic techniques for constrained wireless environments. Adapted from recent IoT security performance studies [**?**].

Technique	Energy Consumption	Security Strength	Device Suitability
Lightweight Symmetric Encryption	Low	Medium	High
Lightweight Asymmetric Encryption	Medium	High	Medium
Hybrid Lightweight Cryptography	Medium	High	High
Post-Quantum Lightweight Crypto	High	Very High	Low

5 Practical Insights and Use Cases

Secure wireless healthcare monitoring systems require strong encryption and authentication while maintaining low power consumption. Wireless body sensor networks continuously transmit sensitive physiological data and must maintain secure communication to protect patient privacy [9]. Industrial wireless sensor networks also require secure firmware update mechanisms to prevent malicious software injection.

Energy harvesting aware security architectures enable adaptive wireless security performance based on available energy resources. These approaches allow wireless devices to dynamically adjust security strength based on available environmental energy sources [5].

An important area where lightweight security implementation can be accomplished is within the scope of wireless sensor networks in an industrial setting. Industrial monitoring systems utilize wireless sensors to provide continuous monitoring of the performance of manufacturing equipment, as well as provide an indication of the environmental conditions and production processes. The failure of security technology used within an industrial environment has significant consequences, including downtime for production, equipment damage, and in some instances, large-scale losses.

Lightweight security protocol technologies designed for the implementation of secure communications between thousands of distributed industrial nodes will help to achieve this goal of providing secure communications while also conserving energy. In addition, many industrial deployments require deterministic real-time communication security solutions that will allow for ongoing system responsiveness, while ensuring strong data authentication and encryption services.

Furthermore, secure firmware update solutions are a critical component of an industrial wireless deployment solution, which will help to prevent devices from becoming compromised by malicious software injection attacks or changes in device configuration from unauthorized sources.

Wireless sensor networks used for environmental monitoring (EM) are typically installed in areas that are inaccessible from a geographic standpoint or where the environ-

ment is extreme. Examples of applications for these networks include forest fire detection, wildlife tracking, oceanographic research, climate monitoring, and determining agricultural soil conditions. The possibility exists that devices used with EM sensor networks operate potentially autonomously, without any physical maintenance necessary, for many years. Lightweight security protocols provide long-lasting remote secure collection of environmental data with minimal energy use due to the protocols being very lightweight and efficient. Reliable and accurate collection of EM data is achieved through the use of secure communications; that is, the use of encryption algorithms to encrypt data transmitted over a communication line or network. Also, EM deployment must take preventive actions to mitigate damage / loss of device(s) due to being physically damaged. The systems used in smart city infrastructures involve integrating different types of wireless device networks so that they can work together for purposes like managing traffic, monitoring public safety, monitoring air quality, and managing public infrastructure. For this to happen, these wireless deployments need security architectures that can provide scalable security for thousands of distributed devices. Lightweight authentication protocols allow secure communications to take place among large groups of devices in an efficient manner. Secure data aggregation protocols ensure the security of all sensor data when it is transmitted over multiple hops wirelessly on urban communication networks.

Emerging Applications of Lightweight Wireless Security Protocols in Agricultural Wireless Monitoring Systems

The deployment of precision agriculture uses wireless sensors to collect real-time data on soil moisture levels, plant health, and irrigation performance. By using these data in conjunction with automated irrigation systems and optimized fertilizer use, precision agriculture can help to provide better yield in the field than conventional farming practices.

Wireless technology and secure wireless communication will allow agricultural producers to continue receiving accurate and timely information related to their field operations without worrying that someone may tamper with their data or privacy. Having reliable and lightweight security protocols in place allows agricultural producers to continue to use agricultural sensor networks over long distances for an extended period of time.

Transportation monitoring systems use wireless sensor networks to support vehicle tracking, traffic monitoring, and infrastructure condition monitoring. Lightweight security protocols enable secure wireless communication between mobile transportation monitoring devices and centralized traffic management systems. Transportation wireless security systems must maintain reliable communication even in high mobility environments where communication channel characteristics continuously change.

Table 2: Security requirement characteristics across wireless IoT application domains. Adapted from IoT deployment security studies [7].

Application Domain	Confidentiality	Integrity	Energy Constraint
Healthcare Monitoring	Very High	Very High	High
Industrial IoT	High	Very High	Medium
Smart Home Systems	Medium	High	High
Environmental Monitoring	Medium	Medium	Very High

6 Challenges and Open Issues

Secure firmware lifecycle management remains a major challenge in long-term IoT device deployment. Secure firmware update mechanisms must prevent malicious firmware injection while maintaining low communication overhead $5_f irmware.Side-channelresistantlightweightcry$

Although there have been great strides made in developing lightweight security protocols for battery-operated wireless devices, many technical and operational issues still exist that have yet to be resolved. These issues stem from the inherent contradiction between strong cryptographic protection requirements and the extreme resource limitations found in wireless embedded systems. Working to address these issues means developing a coordinated research approach that encompasses many areas, including the design of cryptographic algorithms, the architecture of embedded hardware, the optimization of wireless communication protocols, and the modeling of cyber-security threats.

Low energy consumption while providing strong cryptographic security has become another significant challenge. Most of the current types of cryptography were created for enhanced computing environments. Even lightweight versions of traditional cryptographics may use too much computational power when used in very limited category wireless devices. Therefore, there is a continuing research effort to design new cryptographic primitives with good security guarantees with as little computational complexity as possible. In addition to having low energy consumption, developing new cryptographic primitives that provide robust security against modern cryptanalysis is also a research challenge.

The problem with physical device compromise poses a significant challenge for embedded security in wireless devices. Wireless devices deployed in public areas or isolated from support can be the target of physical level attacks by an attacker who attempts to extract cryptographic keys through various methods including: memory extraction, fault injection and side channel techniques, with side-channel attacks being particularly dangerous since they rely on using characteristics of the device such as power usage, electromagnetic interference or timing differences during calculations as an attack vector. Designing lightweight cryptographic implementations that are resistant to side-channel attacks has proven difficult due to the additional compute and energy cost associated

with using countermeasures.

Wireless embedded systems pose significant challenges for lifecycle security management as many wireless devices may be deployed over long tenure periods (multiple years). Over those timeframes, cryptographic vulnerabilities could emerge in previously trusted algorithms used for encryption/decryption. As such, it is necessary to implement secure over-the-air firmware update mechanisms to give remote wireless devices new security protocols. Securing the protocol for firmware updates to prevent malicious firmware from being injected while using minimal energy is also challenging and an engineering problem. In addition, the need to support backward compatibility with legacy devices makes maintaining long-term security more difficult.

Creating lightweight security protocols is an additional challenge due to network heterogeneity. In today's wireless IoT landscape, many different devices exist with various levels of computing power, memory and energy availability. As such, one major research hurdle to overcome is developing universal security protocols that can function efficiently with heterogeneous devices. Adaptive security protocols that vary the degree of security (i.e., adjust security operation based on each device's capabilities) could lead to a viable solution; however, they will add further complexity to the protocol design.

The challenge of quantum computing technology has begun to make an impression on the long-term lightweight wireless security industry. Most currently used cryptographic algorithms are based on the mathematical hardness assumptions which will almost certainly be unbreakable; however, as quantum computers evolve, the mathematical toughness of these algorithms will undoubtedly provide a means of attack against them. As a result, there is significant interest in developing lightweight cryptographic algorithms that can be considered resistant to quantum attacks; however, many post-quantum algorithms will significantly increase the requirements for CPU processing power and physical storage. Thus, finding additional methods to implement post-quantum cryptography on resource-constrained devices continues to be a focus area for many researchers in this space.

To address these problems, researchers from different fields must work together. These areas include cryptology, engineering of embedded systems, wireless communication and cybersecurity. Developing increasingly effective lightweight security protocol will continue to be a key factor in helping to promote the successful deployment of future large-scale wireless embedded systems infrastructure.

7 Future Directions

It is clear that developments in areas such as cryptographic techniques, semiconductor component design, artificial intelligence based security analysis software strategies, as well as new types of wireless communication methods will greatly affect how lightweight secu-

rity protocols evolve for battery operated wireless devices in the future. The increasing use of wireless based embedded systems within critical infrastructure sectors will lead to an increasing need for strong, long term security protocols with ultra-low levels of energy consumption. Future research will focus on building adaptive/scalable/quantum-resistant security frameworks specifically for 'constrained' device environments.

Recent research also focuses on optimizing lightweight security protocols specifically for wireless sensor network deployments [6].

A significant direction for future research is the design of lightweight cryptographic algorithms that are resistant to quantum attacks (post-quantum). Currently established cryptographic protocols being used in wireless embedded systems rely on mathematical hardness assumptions. These systems are likely to become compromised due to advances in large-scale quantum computing and the introduction of quantum computing algorithms, which can significantly reduce the complexity of a number of existing cryptographic problems. The current research effort is to develop post-quantum cryptographic algorithms that maintain a high level of security against quantum attacks while reducing the computational complexity and memory requirements associated with the implementation of many post-quantum algorithms. Post-quantum implementation in constrained wireless devices will be challenging because the key sizes used with most post-quantum algorithms will be larger than those currently being used, and the computational overhead will also be higher than the current algorithms.

The development of energy-harvesting wireless security systems is an area of research that has the potential to greatly impact how wireless devices are designed for security in the future. Energy-harvesting wireless devices get their energy from the environment, such as from light (solar), vibrations (kinetic), heat (thermal), and radio wave (RF) sources. This allows these devices to operate with different levels of security based on how much energy is collected at any given time. For example, when a wireless device has a lot of collected energy, it can do more secure (stronger) crypto operations and more regularly check that it is who they say they are (via authentication checks). When a wireless device does not have much energy available, it can switch to lower-security modes, but still maintain the same level of basic security protection.

Lightweight Security Protocol Development Will Be Influenced By Hardware-Software Co-design Concepts In The Future. Future Embedded Microcontrollers Are Likely To Contain Custom Cryptographic Acceleration Modules Linked To The Processor Architecture. Due To Their Nature As Hardware Based Systems, The Energy Use Required For Cryptographic Operations Using Hardware Is Considerably Less Than For Software Based Systems. Hardware Based Cryptographic Accelerators Also Offer Superior Security From Side Channel Attacks Than Do Software Based Systems. In The Future, There May Be Semiconductor Fabrication And Packaging Technologies Available That Will Support The Design And Construction Of Secure Hardware Enclaves In Microcon-

troller Architectures To Provide Tamper Resistant Key Storage And Secure Execution Environments.

Another potential area of research to look into for future wireless security systems are the use of decentralized trust architectures. Distributed ledger technology (DLT) can be utilized to create distributed authentication and verification frameworks in order that new models for establishing wireless device trust may be developed. The potential reduction in the reliance on centralised security infrastructure as well as an increase in network resiliency are two key benefits of these types of architectures. However, creating distributed trust mechanisms in resource-constrained wireless devices is a difficult problem from a research perspective because of the communication overheads and computation requirements required by the various distributed consensus algorithms used to establish those distributed trust mechanisms.

The design of security protocols that adapt to different layers will be an important area for future research. Future wireless security protocols may automatically adjust their security function, based on the conditions of the communication channel, the congestion level in the network, the state of the device's power supply and any information available about existing threats. Using a cross-layer optimization of security for the overall system will greatly decrease the energy consumed by the system, while still maintaining an acceptable level of protection. In order to implement a cross-layer adaptive approach to security protocols, advanced coordination between the communication, networking and security protocol layers will be necessary at an overall system level.

A growing trend in ultra low power wide area wireless communications technology (ULPWAWC) will impact the future requirements of lightweight security protocols. Wireless networks will soon provide connectivity for a vast number of devices (billions) connecting to a global telecommunications infrastructure. Security protocols will therefore need to support an extremely large volume of devices with regard to both authenticated communication (device authentication) and secure management of the communication resources (secure management of communication). Scalable group authentication (GA), as well as hierarchical key management architectures (KMA) will be crucial elements in managing large device populations.

Standardization will remain significant for how lightweight wireless security architecture will evolve in the future. International standardization organizations will likely keep reviewing and developing lightweight cryptographic algorithms, in conjunction with global security framework standards designed for resource constrained devices. The development of these standards will promote interoperability within multi-vendor ecosystems of wireless devices, allowing for a more secure deployment of large-scale wireless infrastructures.

In order to create lightweight security protocols in the future, it is going to require people from different areas of study (e.g., cryptography research, embedded system design,

wireless communication engineering) to work together to create these new protocols. In addition, continued research funding is going to be important for developing new lightweight technologies for wireless security so that we will be able to deploy next-generation cyber-physical systems safely and worldwide.

8 Conclusion

Modern digital infrastructure has been completely changed by the rapid development of wireless embedded systems and large-scale IoT installations. Throughout several industries, battery-powered wireless devices are now generating constant environmental monitoring through real-time health monitoring, intelligent automation in manufacturing, and smart infrastructure management solutions. However, the widespread use of these technologies has also created very complex security issues with respect to limited hardware resources, energy resources, or even open wireless channels; thus, lightweight security protocols have become an integral technology for ensuring security to meet these needs while maintaining sustainable operation of devices over their lifetime.

To construct lightweight secure communication protocols requires integrating multiple design disciplines such as crypto algorithm optimization, embedded hardware architecture design, wireless protocol engineering, and cyber security threat analysis. Standard crypto protocols cannot work on constrained wireless embedded devices because of their high computational complexity and communication overhead. Lightweight secure communications protocols provide optimised encryption processes, efficient authentication systems, scalable key management architectures and adaptive energy aware security strategies to overcome these limitations. The design goal is to balance the security strength with the energy efficiency so that wireless devices maintain secure communications during long term operation.

Analyzing lightweight security architectures shows that no one security protocol design can effectively meet all of the wireless deployment needs. Different applications require different security optimization priorities. Patient data must be strongly confidential for healthcare monitoring systems. For industrial automation systems, strong authentication and integrity protections are needed to prevent disruptions. Ultra-low energy consumption must be achieved by environmental monitoring systems to support multiple years of autonomous operation. There are therefore a variety of application needs that require adaptability and flexibility for the design of lightweight security protocols.

Symmetric, asymmetric, and hybrid cryptography all have different pros and cons based on the comparison of the three methods. While symmetric cryptography tends to be more energy efficient, the challenges of key management make it difficult to use. On the other hand, although asymmetric cryptography provides a simple way to establish trust, it requires a large amount of energy for computation. Hybrid security architectures

provide a balance of performance; however, there is more complexity related to the implementation of these types of systems. In the future, the design of lightweight security protocols will likely involve developing adaptive hybrid architectures which will adjust security functions based on the energy level of the end user's device(s) as well as on the current network threats.

While much has been accomplished through research, many challenges in lightweight wireless security are still not addressed (e.g., Scaling secure key distribution, counteracting side-channel attacks, creating a secure firmware lifecycle, sustaining long-term cryptography). The emergence of quantum computing will also create new long-term security challenges that post-quantum cryptographic research must address. Finally, as wireless communication technologies continue to evolve, new attack surfaces and security requirements will be created.

The development of lightweight security protocols in the future will greatly benefit from advancements in AI supported Adaptive Security Systems, Wireless Energy Harvesting Device Architecture, Hardware based Cryptographic Acceleration and Decentralized Trust Management. As these new technologies emerge, they will provide significant enhancements to wireless security but do so while still achieving ultra-low energy consumption. In addition, standardized methods will continue to be necessary for the interoperability of global wireless device ecosystems, as well as for supporting the secure deployment of large size global wireless infrastructures.

The growth of wireless embedded systems throughout many key infrastructure sectors such as healthcare, transportation, energy distribution, and industrial automation increases the need for ongoing investment in lightweight wireless security technologies through continued research. Likewise, secure wireless embedded communication will play an essential role in enabling the deployment of next generation Cyber Physical Systems and Smart Infrastructure. Finally, the creation of robust, scalable and energy-efficient lightweight security protocols will continue to be a core enabling technology for the safety and reliability of future global wireless communication ecosystems.

References

[1] Abubakr Abdulgadir and Sammy Lin. Side-channel resistant implementations of a novel lightweight authenticated cipher with application to hardware security. In *Proceedings of the ACM Great Lakes Symposium on VLSI*, 2021.

[2] M. Almutairi and F. T. Sheldon. Resilience of post-quantum cryptography in lightweight iot protocols: A systematic review. *Eng*, 2025.

[3] J. Bojic Burgos and M. Pustisek. Decentralized iot data authentication with signature aggregation. *Sensors*, 2024.

[4] L. Catuogno and C. Galdi. Secure firmware update: Challenges and solutions. *Cryptography*, 2023.

[5] Khalid Haseeb, Ikram Ud Din, Ahmad Almogren, and Naveed Islam. An energy efficient and secure iot-based wsn framework: An application to smart agriculture. *Sensors*, 2020.

[6] Taejoon Park and Kang G. Shin. Lisp: A lightweight security protocol for wireless sensor networks. *ACM Transactions on Embedded Computing Systems*, 2005.

[7] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli. Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained iot devices. *Sensors*, 2024.

[8] A. Rehman and O. Alharbi. Qesif: A lightweight quantum-enhanced iot security framework for smart cities. *Smart Cities*, 2025.

[9] Pedro Rosa, Andre Souto, and Jose Cecilio. Light-sae: A lightweight authentication protocol for large-scale iot environments made with constrained devices. *IEEE Transactions on Network and Service Management*, 2023.

[10] S. S. Sefati, R. Craciunescu, B. Arasteh, S. Halunga, O. Fratu, and I. Tal. Cybersecurity in a scalable smart city framework using blockchain and federated learning for internet of things. *Smart Cities*, 2024.

[11] A. Sevin and U. Cavusoglu. Design and performance analysis of a speck-based lightweight hash function. *Electronics*, 2024.

[12] C. Silva, N. Tenorio, and J. Bernardino. Lightweight encryption algorithms for iot. *Computers*, 2025.

[13] Catarina Silva, Vitor A. Cunha, Joao P. Barraca, and Rui L. Aguiar. Analysis of the cryptographic algorithms in iot communications. *Information Systems Frontiers*, 2023.

[14] SungJin Yu and YoungHo Park. Slua-wsn: Secure and lightweight three-factor-based user authentication protocol for wireless sensor networks. *Sensors*, 2020.

[15] Y. Zhang and L. Chen. Secure and lightweight blockchain-enabled access control for fog-assisted iot cloud based electronic medical records sharing. *IEEE Access*, 2023.