Journal of Wireless Sensor Networks and IoT, ISSN: 3048-8729 Vol. 2, No. 1, 2025 (pp. 20-30)
RESEARCH ARTICLE ECEJOURNALS.IN

Secure Data Transmission Advances for Wireless Sensor Networks in IoT Applications

Ahmet Fatma[1], Mehmet Ayşe[2]*

[1,2]Sakarya University, Department of Computer Engineering, Serdivan campus, Sakarya, Turkey

Keywords:
Embedded Systems;
Wireless Sensor Networks Protocols;
IoT Device Management;
Sensor Network Architectures;
Energy-Efficient IoT

Corresponding Author Email:
Ayse78mehm@gmail.com

DOI: 10.31838/WSNIOT/02.01.03

Received : 30.07.2024
Revised : 18.10.2024
Accepted : 12.12.2024

Abstract

It's no surprise that the Internet of Things (IoT) has changed the way we interact with the world around us, bringing countless devices and sensors together to connect to create smart, data driven environments. A large number of IoT applications rely on the use of Wireless Sensor Networks (WSNs), which collect and transmit huge amount of data at the core. As these networks get larger and more vital, so do the problems of keeping their data secure. In this paper, we study all the recent advances in securing data transmission in WSNs for use in the IoT where we introduce the recent research on how to provide protection against cyber attacks by means that maintain performances and, at the same time, make data more properly protected. As industries roll out IoT deployments from smart cities to industrial automation, there has never been a more critical need for reliable, robust security in place. The distributed nature of WSNs and often resource constrained nodes poses unique security challenges for which traditional cryptographic solutions might not do a very good job of. In this article, we explore state of the art research and practices to seek the appropriate trade off between security, energy efficiency and network performance, in WSN based IoT systems. Throughout this survey, we will discuss the spectrum of such topics as lightweight cryptographic algorithms designed for WSNs, cross layer security mechanisms, as well as innovative techniques of the key management and distribution. We will also look at how both elliptic curve cryptography and physical layer security is getting integrated to further protect the transmission of data through these networks. By the end of this extensive literature survey, readers will have a more thorough understanding of the status quo of secure data transmission in WSNs for IoT applications, and understandlications and possibilities for what lies ahead in this burgeoning sphere.

How to cite this article: Fatma A, Ayşe M (2025). Secure Data Transmission Advances for Wireless Sensor Networks in IoT Applications. Journal of Wireless Sensor Networks and IoT, Vol. 2, No. 1, 2025, 20-30

The Security Landscape of WSNs in IoT

Many IoT applications rely on Wireless Sensor Networks as the backbone, the eyes and ears of smart systems across different domains. The network, however, consists of hundreds or even thousands of small, low powered sensor nodes whose role is to communicate information from their environment to processing systems, which may or may not be far away. The particular vulnerability of WSNs to a broad range of security threats stems not only from the distributed nature of the WSN, but also from being deployed in potentially hostile or uncontrolled environments. Due to the resource constraints in individual sensor nodes, WSNs are one of the main challenges of securing the network. WSANs nodes have typically limited processing power, memory, and energy reserves unlike traditional computer networks. The network's complexity however, makes it difficult to achieve complex security protocols or provide robust encryption algorithms without significantly affecting the network's overall performance and life.

Furthermore, WSNs use a wireless communication medium and add to vulnerability. Just a few of the threats which lead to the compromise of confidentially, integrity and availability of data transmitted over these networks include eavesdropping, man in the middle attacks and jamming. Physical tampering of sensor nodes that are deployed in unsecured locations only adds more to the security landscape. WSNs experience even more stringent security requirements in the context of IoT applications. Sensitive data is very common in many IoT systems that handle such data as personal health information, industrial process parameters, and critical infrastructure status, among other examples. These networks are extremely exposed to a breach in their security, leading too their economic losses and some of them, the threats to public safety.

To tackle these problems, the researchers and industry professionals have been developing new ways to secure data transmission in WSNs. Clearly these solutions need to be lightweight enough to run on resource constrained devices but at the same time be resistant to strong attack vectors. In this post, we will explain how the evolution in the cryptographic algorithms, network protocols and the system architecture helps to make the WSNs (Wireless Sensor Networks) more robust and secure for IoT based applications. Understood within this unique security landscape, it makes sense to understand the solutions being developed and their potential for the future of IoT security.[1-6]

Wear and Tear Detection Algorithms for WSNs

In the context of Wireless Sensor Networks where computational resources are limited, the implementation of the traditional cryptographic algorithms is often too cumbersome. This limitation has motivated the construction of lightweight cryptographic algorithms that support robust security at the cost of minimal resources. These algorithms attempt to achieve security level in trade for operational efficiency, a balance that makes them easily implementable in the IoT based WSN. In this area, we have also seen the development of RECTANGLE, a lightweight block cipher which is shown to have very good performance characteristics for resource constrained devices. By exploiting a Substitution Permutation Network structure, RECTANGLE is able to run efficiently both in hardware and software. The algorithm is designed so that it stays simple and fast and it is perfectly suited for WSN environments where the encryption and decryption have to happen quickly for the network response.

Table 1: Advanced Encryption Techniques for Secure Data Transmission

Technique	Application
AES (Advanced Encryption Standard)	AES is a symmetric encryption algorithm widely used for securing data transmission in IoT networks, providing high security with minimal overhead.
RSA Encryption	RSA encryption is an asymmetric encryption technique used for secure key exchange and data confidentiality in IoT applications, ensuring privacy during transmission.
Elliptic Curve Cryptography	Elliptic curve cryptography (ECC) offers higher security with smaller key sizes, making it ideal for resource-constrained IoT devices while maintaining strong encryption.
Homomorphic Encryption	Homomorphic encryption allows computations on encrypted data without decrypting it, ensuring data privacy and security during processing in IoT systems.
Quantum Encryption	Quantum encryption leverages quantum key distribution to ensure the security of data transmission in IoT networks, providing resistance against future quantum computing attacks.
Blowfish Encryption	Blowfish encryption is a fast block cipher designed to provide secure data transmission while being computationally efficient for low-power IoT devices.

Another lightweight cryptographic solution is Fantomas of ARX (Add-Rotate-XOR) ciphers family. The simple operations that Fantomas leverages are easily implementable on wide variety of hardware platforms, ranging from low power microcontroller to higher power processors. The flexibility of Fantomas allows it to be a preferable choice for heterogeneous WSN deployment, where different types of sensor nodes will coexist in the same network. While not as lightweight as RECTANGLE or Fantomas, the Camellia algorithm has also been noticed for the possibility of its use in WSNs. Camellia strikes a good balance between security strength and efficiency, and hence is

a good choice for situations when there is a need for a higher security level, than is afforded by, for instance, DES, but performance is still of some concern. Feistel network structure for the network makes it resistant to many types of cryptanalytic attacks to improve the security posture of the whole network.

To compare these lightweight algorithms with more traditional choices like the Advanced Encryption Standard (AES), several key indicator metrics are important. Since WSN nodes commonly have limited RAM and storage capacity, memory usage is an important matter. The throughput is another very important point to consider as this is directly linked to how much the network can actually manage to process real time data stream. Perhaps the most important metric involves battery consumption; many WSN nodes rely on continuous, battery power for an extended amount of time.. Results from SPN based block ciphers such as RECTANGLE are that these structures outperform Feistel based structures in a WSN environment. This superiority is owed to the fact that they use less computational resources and consume less energy. Yet, the selection of algorithm is demanded by the characteristics of WSN deployment and the application of the IoT itself.

For the flexibility and adaptability of security mechanisms in WSNS, some researchers have suggested using reserved bits in the frame control field of Zigbee MAC's header. With this approach users are able to dynamically switch between secure and insecure modes and still have the ability to raise or lower the security level based on current needs or threat level. In addition, interaction mechanisms that span layers have been constructed so networks can change between different encryption algorithms based on changing conditions, including changes in the bit error rate (BER). The road going forward in the field of lightweight cryptography will only get more exciting, as we continue to see even more inventive algorithms and implementation strategies. These advancements will contribute in a fundamental way to the establishment of secure data transmission in WSN for the realization of IoT applications that need to keep the exchanged information safe but do not interfere with the network performance and life time .[7-9]

Cross Layer Secure Mechanisms

Although the traditional layered approach to network security is extensible in many instances, it is not suitable in some cases where the requirements of an application tailored towards Wireless Sensor Networks segments in Internet of Things applications. In order to get past these limitations, researchers have been looking into cross layer security mechanisms, which takes advantage of interactions from the different layers of the network stack to enhance security performance. Cross layer security design exploits such dependencies for more robust and efficient security design. These mechanisms allow information to pass across layers that ordinarily would not work in concert, giving them the ability to make more considered decisions about the security measures to be implemented and about resource allocation (Figure 1).

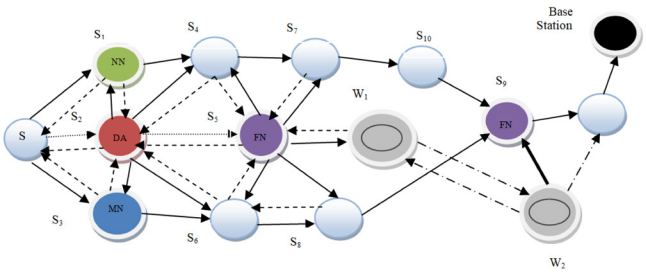

Fig. 1: Cross Layer Secure Mechanisms

One of the key advantages of cross layer security in WSNs is the ability to change the security protocol dynamically in response to the network condition. As an example let's say that the physical layer has information about the signal strength or level of interference that can be used to adjust encryption parameters or routing decisions at the higher (or application) layers. The adaptability of information flowing over such networks is extremely beneficial when considering IoT applications, as network conditions can change dramatically based on the deployment environment.

Cross layer security is accomplished based on use of physical layer characteristics for enhancement of cryptographic key generation and distribution is another noted implementation. Nodes can generate shared key without extensive key distribution or demanding key exchange protocols, by exploiting the natural randomness of the wireless channel. Not only does this improve security, but it also does so at the expense of a reduction in computational and communication overhead compared to traditional key management schemes. Cross layer security thus holds promise for network attack detection and mitigation. WSNs further enhance their accuracy of detecting potential security threat by correlating information from different layers, i.e., unusual traffic patterns in

the network layer and physical layer measurements, and then making decisions on identifying security threat based on the above correlation. This holistic approach to threat detection makes for quicker and more responsive tactics to attack, for a more resilient network.

Also, security requirements can be balanced with other network performance metrics with the help of cross layer optimization techniques. As an example, instead of fixing the security protocol once and allowing its parameters to be determined by the current security threat level, if the remaining energy levels of the sensor nodes are included, the network can dynamically tune its security protocols to favor the trade-offs between protection and energy consumption. By taking an adaptive approach, scarce resources are optimally utilized while protecting the networks security posture. There are challenges to implementing cross layer security mechanisms in WSNs. Increased system complexity can make these systems more difficult to design, implement and maintain. Moreover, the tight coupling between layers can open other vulnerabilities weakly managed. Though, the challenges are imagineable however a compromise with these imbalances is somehow worth it mainly on IoT applications who require resource and flexibility optimization.

With the research in this area continuing to progress, we can expect to see more and more sophisticated cross layer security solutions. What we can expect to see is more of these nearly seamless integration between the layers, to the point that the virtual definition of network stack starts to blur; just like the traditional stack boundaries, if not completely breaking down, to pave way for a more holistic way of protecting the network itself. In order to bring wider adoption and interoperability across different IoT platforms and applications, it will become essential to develop standardized frameworks and protocols for cross layer security in WSNs.[10-15]

New Methods for Key Management and Distribution of Catalogs.

In real IoT applications, making sure that Wireless Sensor Networks remain secure is dependent on effective key management and distribution. Existing traditional key management schemes suffer from the inability to address the special demands imposed by WSNs, such as huge scale, limited computation capacity as well as dynamic network structure. In such challeges, researchers came up with novel approaches to offer strong security at minimal times and complexity. An exciting, new approach is the usage of physical unclonable functions (PUFs) to generate and manage keys. PUFs make use of the natural physical properties of the semiconductor device to dispose device specific keys. This approach no longer stores sensitive key material in memory and consequently reduces the potential for key compromise by physical attack. In particular, PUFs-based key management is a particularly suitable solution to be used in WSNs because it offers an extremely lightweight solution that may be catered to both secure the wireless communication and be implemented in resource constrained sensor nodes.

The use of attribute based encryption (ABE) is another promising technique for fine grained access control for WSNs. One nice feature of ABE is that encryption is based on a set of attributes rather than individual identities (Table 2). This approach also

Table 2: Secure Data Transmission Protocols for IoT

Protocol	Purpose
TLS (Transport Layer Security)	TLS ensures secure communication over a network by encrypting the data transmitted between IoT devices and servers, preventing unauthorized access and tampering.
DTLS (Datagram TLS)	DTLS provides similar security as TLS but works over UDP, ensuring secure communication for real-time IoT applications that require low-latency data transmission.
IPsec (Internet Protocol Security)	IPsec secures IP communications by authenticating and encrypting each IP packet, ensuring end-to-end security for data transmission across IoT networks.
SSL (Secure Sockets Layer)	SSL provides secure, encrypted connections for IoT devices and servers to communicate over the internet, protecting sensitive data from being intercepted.
MQTT with SSL/TLS	MQTT with SSL/TLS enhances the security of the MQTT protocol by ensuring encrypted communication channels between IoT devices and the server, ideal for IoT applications.
Zigbee Security	Zigbee security protocols use encryption and authentication techniques to protect the integrity of data and ensure secure communication in Zigbee-based IoT networks.

allows access policies to be defined upon the roles or characteristics of nodes in the network itself, improving flexibility and also scalability of the key management (Table 2). ABE is a powerful tool in IoT applications where different sensors may have varying degrees of access to their sensitive data, yet no individual key distribution is required to each node in order to enforce complex security policies. The scalability challenges confronting centralized approaches have also led to the emergence of distributed key management protocols.

Another approach researchers employed to address the dynamic nature of many WSN deployments is the introduction of adaptive key management schemes that can modify to changes in network topology or security requirements. Typically, these schemes are hierarchical, placing more importance on cluster heads (gateways, in the case of gateway receiving the keys) in key management. These approaches hope to reduce the burden that the resource constrained sensor nodes inherit while still providing strong security guarantees by delegating key management tasks to more capable nodes. Another area of active research is the integration of blockchain technology in the core essential components, the key management systems in WSNs. The security and tamper resistant nature of blockchain makes Blockchain an ideal place to securely store and distribute cryptographic keys between clients and servers. Blockchain based key management system exploits smart contract and distributed consensus mechanisms to increase security and transparency in key distribution.

In the future, WSN security could be revolutionized by quantum key distribution (QKD) a cutting edge method to exchange keys. Ongoing research will be able to develop more lightweight QKD protocols for IoT applications, while currently being too resource intensive for most WSN applications. Quantum cryptography promises unconditional security, which makes quantum cryptography an excellent area to watch in the future for the security of WSN. The new key management and distribution approaches will continue to evolve, and as we look forward to hybrid solutions combining various techniques that meet the diverse security needs of various IoT applications. The major hurdle ahead is in building standardized protocols and frameworks that can fit naturally inside current WSN architectures while keeping consistent interoperability across distinct IoT platforms.[16-18]

WSN ELLIPTIC CURVE CRYPTOGRAPHY

ECC is an exciting means that has emerged for securing Wireless Sensor Network in IoT applications, and therefore, a compelling alternative to the traditional public key cryptosystem. The main benefit of ECC is that it can offer equivalent security to other public key algorithms, like RSA, but with far smaller keys. This characteristic makes ECC particularly well suited for the resource constrained environments typical of WSNs. ECC's building block is the use of elliptic curves over finite fields to generate cryptographic keys. The creation of such cryptographic systems with keys of short lengths (say, of order 100) by making use of the mathematical properties of these curves is possible. For instance, an 256-bit ECC key gives security similar to that of a 3072 bit RSA key. Such a reduction of key size directly translates into lower computational resources, reduced memory, and less energy consumed, which are necessary requirements for WSN deployments.

Implementing ECC in WSNs offers several key benefits:

1. **Reduced computational overhead:** ECC offers smaller key size and that means faster encryption and decryption process, and this is very important to maintain the responsiveness of network in the real time IoT environment.
2. **Lower memory requirements:** ECC implementations often require less memory than other public key systems, and implement with shorter key length and simpler mathematical operations, making it possible for sensor node use of limited storage resources.
3. **Energy efficiency:** ECC operations have reduced computational complexity, resulting in less power and longer battery life for sensor nodes, and consequently, an extended life span of the network as a whole.
4. **Scalability:** Because of the small size of ECC keys, they are well suited to the practice of growing IoT applications through managing and distributing large number of keys in large scale WSN deployments.

There have been developed different ECC based protocols developed especially for WSNs. They involve lightweight key agreement schemes, digital signature algorithms, and encryption methods adapted for sensor node capability. For example, the Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol can be

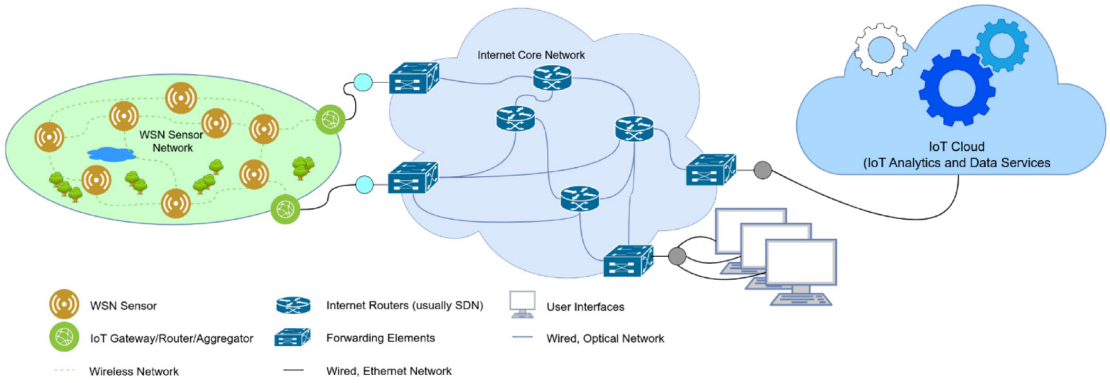

Fig. 2: WSN elliptic curve cryptography

used to securely establish shared secret keys between nodes, or the Elliptic Curve Digital Signature Algorithm (ECDSA) can help us to authenticate messages and verify the integrity of the data transmitted across the network (Figure 2).

For WSNs, ECC also has a strong application in the area of IBC. This is where IBC comes in; with IBC, nodes can use their own unique identifier (which might be a MAC address, or a sensor ID, for example) as a public key, so they don't need to have a PKI system at all. By leveraging this approach, large scale IoT deployments can be simplified with key management and the overhead caused by distribution and verification of certificates as smaller and less distributed, making it the highly desirable approach.

While the benefits of ECC make it attractive for WSNs, some issues must be addressed to make the technology feasible. ECC-based systems crucially depend on the proper choice of curve parameters and the security of random number generation, and can thus be significantly compromised due to mischoice of these factors. This also applies to the fact that ECC operations tend to be less computationally intensive than most public key systems, but they remain expensive for the most resource constrained sensor nodes.

Therefore, the researchers try to develop the hardware ECC implementations with hardware acceleration to significantly improve the performance on the low power devices. Specialized hardware modules can take advantage of complex ECC calculations that can put off the main processor and decrease energy consumption as well as improve overall system efficiency.

The field of ECC, however, is still evolving and there will be even more efficient, and more suitable ECC algorithms for WSN. What will be crucial for wider IoT adoption and interoperation across different platform and device platforms will be the development of standardized ECC protocols.

By the integration of ECC with other security mechanism, like lightweight symmetric encryption algorithm and dedicated physical layer security techniques, they bring the opportunity to design a complete security solutions for WSN and IoT applications. These approaches will eventually mature as enabling technology for the secure and efficient deployment of large scale sensor networks in various applications of IoT.[19-20]

Physical Layer Security Techniques

Physical layer security is an attractive means to secure data transmission in Wireless Sensor Networks for IoT. In contrast to traditional cryptographic methods situated at higher layers of the network stack, physical layer security mechanisms exploit the intrinsic properties of the wireless communication medium to obviate or reduce the risk of eavesdropping and other security attacks.

Physical layer security is based on the fundamental principle that wireless channels are inherently random and unpredictable, and can be utilized to creating secure links. Using this line of reasoning, legitimate communicating parties are able to exploit the fact that they experience correlated channel conditions that are intractable not only for an eavesdropper to replicate, but to predict. Going beyond just computationally intensive cryptographic algorithms, secure communication is achieved via careful designed transmission schemes exploiting these unique communication properties.

One of the attractive aspects of physical layer security in WSNs is its feasibility to provide information theoretic security, that is, security against adversaries

without any computational power. In cases where sensor nodes may have long deployment lifetimes, this characteristic is of huge value because the sixth characteristic protects against advances in computational power which might make crypto approaches (tried and true) vulnerable to compromise.

Several physical layer security techniques have been developed and adapted for use in WSNs:

1. **Secret key generation:** In this approach, shared secret keys are generated between communicating nodes based on the wireless channel reciprocity and randomness. Nodes derive cryptographic keys without explicit key exchange protocols when measuring and quantizing channel characteristics, such as received signal strength or phase.
2. **Artificial noise injection:** This is an approach in which the transmitter deliberately inserts artificial noise into the channel in a way that makes the signals quality worse for potential eavesdroppers, but makes this so the legitimate receiver can cancel out the noise. This approach can give the adversaries a very low signal to noise ratio, making it so that it is hard for them to intercept and decode the transmitted data.
3. **Beamforming:** Beamforming techniques can focus the transmitted signal in the direction of desired receiver while minimizing forwarded radiation in other directions, by utilizing more than one antenna or cooperative transmission from multiple nodes. It tackled the security problem using spatial filtering, thereby reducing the signal strength at the tap outside the main beam to potential eavesdroppers.
4. **Friendly jamming:** In this method trusted nodes in a network transmit jamming signals deliberately to interfere in the areas where eavesdroppers might be located. In particular, this technique has the potential to be particularly useful in situations when the locations of legitimate nodes are known and it is not known where adversaries need to be located.
5. **Channel coding for secrecy:** We design codes that provide error correction and minimize information leakage to eavesdroppers by advanced channel coding techniques. The secure communication is based on these codes that exploit the difference of channel quality between legitimate receiver and the adversary.

Unfortunately, implementing physical layer security in WSNs has some challenges. In wireless channels of the IoT environments, the security is difficult to guarantee as wireless channels are dynamic and mobility of nodes can be present as well as there may be interference from other devices. Further, sensor node ability to process and utilize information can be limited by the node's limited processing capabilities and available energy, and the complexity of physical layer security schemes that can be practically implemented is limited.

Typically, to overcome these challenges, researchers will resort to cross layer techniques, by combining physical layer security with higher layer security mechanisms. Suppose that such information of physical layer security status can be used to dynamically vary encryption parameters or routing decisions at a higher layer of the network stack. By taking an integrated approach, such security solutions provide a more adaptive and robust approach to security compared to solutions offering only stand-alone functionality.

In parallel with the evolution of this field of physical layer security, it will likely see more sophisticated schemes designed for WSN environments. Standardising the protocols and frameworks developed for physical layer security for IoT applications will have to proceed to support wide scale uptake and interoperability across varying platforms and devices.

By integrating physical layer security with other advanced security mechanisms like lightweight cryptographic algorithms and new key management schemes, integrated security solutions can be created defeating the full spectrum of threats WSNs are faced in an IoT application. When these integrated approaches mature, they will be instrumental in realising the secure and efficient mass deployment of large scale sensor networks over a wide range of IoT use cases.

Performance Optimization and Evaluation

Due to the increasing complexity and diversity of security solutions for Wireless Sensor Networks in IoT applications, there is increasing need for robust performance evaluation and optimization techniques. An important issue when making the choice as to which security mechanisms are the most effective and efficient is assessment.

Performance evaluation in the context of secure data transmission for WSNs typically focuses on several key metrics:

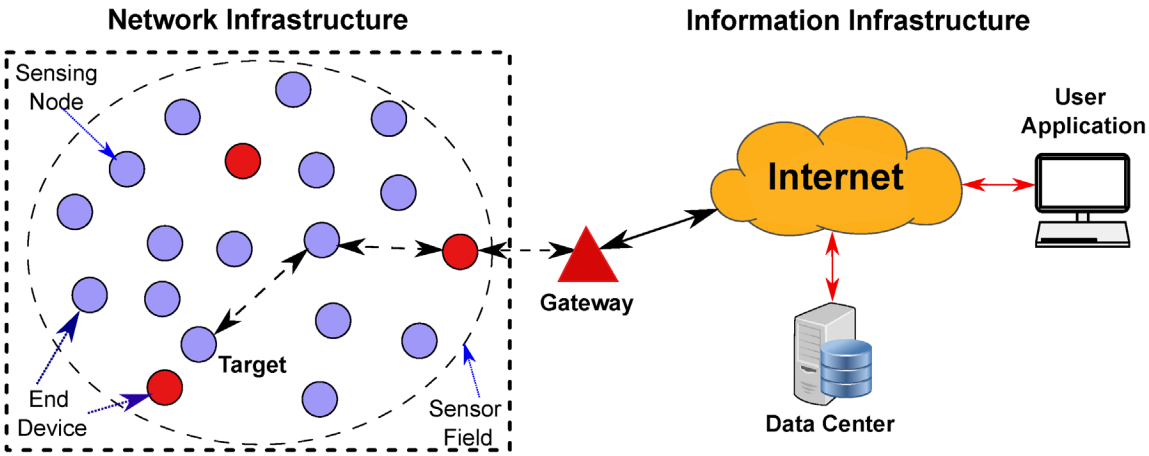

Fig. 3: Performance Optimization and Evaluation

Security strength: This metric measures the security mechanism's resilience against various cryptographic and physical tampering attacks such as cryptanalysis, side channel attacks.

Computational overhead: The processing requirements of the security algorithm are evaluated directly impacting the energy consumption and response time of sensor nodes.

Memory usage: It measures how much of RAM and storage is required to execute the security solution, an important metric for resource limited devices (Figure 3).

Energy efficiency: Additionally, it quantifies the impact of the security mechanism on the total power consumption of the sensor nodes, and hence the network lifetime.

Communication overhead: Measures the additional bandwidth and transmission power necessary to support the security protocol (e.g. for adding extra messages, or enlarging packet sizes).

Latency: It measures the delay of security mechanism for data transmission and processing especially in real time IoT applications.

Scalability: It evaluates the performance of the security solution with respect to the size of the WSN; taking into account the key management complexity and the security coordination over the network.

To study and evaluate comprehensive performance, researchers and developers use a combination of analytical modeling, simulation study, and real world testbed experiments. Simulation allows parameters and different network scenarios to be investigated, while analytical models enable theoretical performance bounds of security mechanisms to be probed. While testbed experiments are less resource intensive they provide valuable real world performance data that can help validate theoretical and simulation results.

The use of adaptive security frameworks on security mechanisms in WSNs is one way of optimizing the performance of security mechanisms.

The other optimization strategy is the selection and combination of complementary security techniques appropriately. With the right fusion of strengths, and mitigating weaknesses, it is possible to come up with more robust and more efficient security solutions of a use. One example is combining the physical layer security techniques with light weight symmetric encryption, which provides strong protection against computational as well as physical layer attacks with acceptable resource consumption.

Another path to security performance optimization in WSNs is hardware acceleration. Sensor nodes can enjoy significant drop in processing speed and energy in consuming sensors thanks to offloading complex cryptographic operations to dedicated hardware modules. As the IoT ecosystem progresses, we should observe emerging specialized hardware solutions specially designed for secure WSN deployments.

Optimizations of security in WSNs are also being investigated based on machine learning and artificial intelligence techniques. These approaches can be used for network behavior prediction, anomaly detection, and the automatic refinement of security parameters depending on changing conditions. Reinforcement learning algorithms, for instance, could be used to select how to trade off security strength against energy consumption to optimization the trade off

through time, according to the specific characteristics and needs of WSN deployment.

The studies regarding the WSN security remains a constantly evolving field and the standardized benchmarking methodologies and performance metrics will gain increasing importance. These standards will create a fair playing field for differing security solutions, and it will use it as a guide in the development of more efficient and effective mechanisms for safeguarding the data transmission in IoT applications.

Thus, performance optimization for WSN security likely will be the seed for continued development of more context aware and self adapting security frameworks. Recognizing the dominant trends in telecommunication, these advanced systems will be continuously monitoring network conditions, assessing security risks, and reconfiguring security mechanisms dynamically to strike optimal balance between security and the resource utilization.

By emphasizing rigorous performance evaluation and constant optimization, security solutions for WSNs in IoT applications can guarantee that not only will they afford robust protection against advancing attacks but can also meet demanding efficiency limitations crucial to extensive use in different IoT scenarios for long durations.

Future Directions, and Emerging Technologies

The field of secure data transmission in Wireless Sensor Networks and IoT applications is evolving ever changing with new challenges and opportunities. Future of WSN security is looking bright, options and new technologies are emerging that are destined to change how data sensitive and important information is protected in an IoT era. The use of quantum technologies to secure WSNsecurity is one of the most exciting areas of development today. A sufficient store of computational hardware does not pose a threat to QKD, which promises unconditionally secure key exchange. Current QKD systems are already too resource intensive for many WSN application instances, but research today is focused on developing lighter and more practical quantum secured communication protocols for IoT environments. With the advancement of this technology, we could witness hybrid systems that blend quantum and classical security mechanisms to keep our network safe across various layers of the network stack.

Another area that has potential is to integrate artificial intelligence (AI) and machine learning (ML) into WSN security frameworks. Real time AI driven security systems that can optimize security parameters based on changing network conditions and evolvng threat landscapes, and detect and adapt to potential attacks. The behavior of network could predict with machine learning algorithms, link to patterns on data traffic, and even foresee security breaks before they actually happen. Given their intelligence, these security systems could greatly boost the resiliency and performance of WSNs in IoT applications. The application of blockchain technology to WSN security solutions also provides new methods of securing storage of data, as well as control over the access to and the identification of individuals. Blockchain is appealing as a means to secure sensor data ledgers and manage cryptographic keys in a distributed environment, because of its decentralized, tamper resistant nature. Blockchain platforms, through the creation of smart contracts, could allow for automation of security policies and access control mechanisms which would diminish the requirement of centralized management and increase network hardness.

With the coming of 5G and future 6G network, WSN security will have a brand new opportunity and problem. With these high speed, low latency networks, there will also be new attack vectors and security considerations for new sophisticated IoT applications. The research into secure 5G and 6G integration for WSNs will be important to guarantee that these new communication technologies are also used on safe grounds in deployment of IoT. Another trend that will have a huge impact on security of WSN in IoT application is edge computing. Edge computing is boasting reduced latency and bandwidth requirements, while potentially improving security by limiting access to wide networks, by allowing data processing closer to the source of interest. Even though edge devices and managing secure edge environments with distributed security policies across heterogeneous edge environments are possible, novel solutions will come into play.

This creates opportunities for the development of new materials and manufacturing techniques enabling the development of more secure hardware platforms for WSN nodes. Physical security of sensor nodes could be improved with physically unclonable functions (PUFs) and tamper resistant packaging that would make the nodes more resilient to hardware attacks

and reverse engineering attacks. Movie developments in IoT application top the critical infrastructure plus business structure will certainly make certain that the emphasis is on producing security and security options that can satisfy strict regulatory requirements and industry criteria. Some of this is bound to translate to specialized WSN security frameworks and certification processes designed especially for WSNs used in high stakes IoT deployments.

We expect the concept of "security by design" to gain more traction, with security considerations built in to every part of the WSN and the IoT system development process from the outset. To support this holistic approach to security, new tools and methodologies for security model and analysis of the security consequences of design decision throughout the development cycle will be needed. Finally, as the scale and complexity of IoT deployments increase, more and more automated security management and orchestration tools will be required. To implement all of these systems, the tasks will include rotating keys, applying updated firmware, and enforcing security policies on sprawling networks of heterogeneous devices with minimal human involvement and with unchecked strict security guarantees.. It is expected that more sophisticated adaptive and resilient security solutions for WSNs in IoT applications will be developed as these future directions and such emerging technologies converge. The core problem lies in turning these innovations into drivers that augment security without hindering the efficiency and scalability that make WSNs such a powerful force in IoT scenarios. Moving forward, staying at the forefront of these technological advancements and continuously adding to them to fight new threats and requirements will be the domain of WSN security and essentially have to shape the future of secure and reliable IoT systems.

Conclusion

Wireless Sensor Networks have emerged as an area of technological innovation at the forefront of rapid expansion of IoT application and have enabled unprecedented levels of data collection and environmental interaction. All of this growth brings with it a sense of urgency to secure this enormous flow of sensitive data that travels through these networks. In this article, we have examined state of the art in secure data communication for WSNs in the IoT, and describe emerging approaches to these issues in resource constrained and often vulnerable systems. The field has made significant progress in balancing the security requirements and limitations of WSN nodes alike from lightweight cryptographic algorithms adapted to WSN environments to novel cross layer security mechanisms. Different and creative approaches to data protection for WSNs are shown by physical layer security techniques and adaptation of elliptic curve cryptography for WSNs. Looking forward, the integration of new, ultra sophisticated technologies like quantum cryptography, artificial intelligence, and blockchain will only afford us increasingly sophisticated and adaptive security options. With continual hardware capability and energy efficiency improvements, these advancements are enabling more secure and resilient WSNs emerging in the more complex IoT ecosystems. However, we also want to stress that the pursuit of better security in WSNs is an ongoing task. Security of IoT applications is constantly evolving with ongoing threat landscape and drive to more efficient and scalable applications. These advancements will need to be standardised and, in cooperation with the development of comprehensive security frameworks, will likely need to be rolled out across diverse IoT deployments. Thus, the success of secure data transmission in WSNs for their use in IoT applications will purely depend on the whole security facet of the system design and its operation. However, by continuing to invest in research, development and practical implementation of innovative security mechanisms, we can lay the groundwork for trustworthy and verifiable IoT system that truly brings about transformative power of this technology and throughout the different sectors of our increasingly intertwined world.

References:

1. Faheem, M., Tuna, G., & Gungor, V. C. (2017). LRP: Link quality-aware queue-based spectral clustering routing protocol for underwater acoustic sensor networks. *International Journal of Communication Systems*, *30*(12), e3257.
2. Parra, L., Sendra, S., Lloret, J., & Rodrigues, J. J. (2017). Design and deployment of a smart system for data gathering in aquaculture tanks using wireless sensor networks. *International Journal of Communication Systems*, *30*(16), e3335.
3. Sharma, R., & Prakash, S. (2020). Enhancement of relay nodes communication approach in WSN-IoT for underground coal mine. *Journal of Information and Optimization Sciences*, *41*(2), 521-531.

4. Javed, A. R., Beg, M. O., Asim, M., Baker, T., & Al-Bayatti, A. H. (2023). Alphalogger: Detecting motion-based side-channel attack using smartphone keystrokes. *Journal of Ambient Intelligence and Humanized Computing*, 1-14.
5. Azmoodeh, A., Dehghantanha, A., & Choo, K. K. R. (2018). Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning. *IEEE transactions on sustainable computing*, *4*(1), 88-95.
6. Nagaraju, V. S., Babu, P. A., Ratna, V. R., & Mariserla, R. (2020, December). Design and implementation of low power 32-bit comparator. In *Proceedings of the International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS 2020), Palai, India* (pp. 459-468).
7. Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal*, *8*(4), 2300-2317.
8. Elsts, A., Fafoutis, X., Duquennoy, S., Oikonomou, G., Piechocki, R., & Craddock, I. (2017). Temperature-resilient time synchronization for the internet of things. *IEEE Transactions on Industrial Informatics*, *14*(5), 2241-2250.
9. Luo, B., Cheng, L., & Wu, Y. C. (2016). Fully distributed clock synchronization in wireless sensor networks under exponential delays. *Signal processing*, *125*, 261-273.
10. Xu, L. D. (2011). Information architecture for supply chain quality management. *International Journal of Production Research*, *49*(1), 183-198.
11. Mohammed, Z. H., Chankaew, K., Vallabhuni, R. R., Sonawane, V. R., Ambala, S., & Markkandan, S. (2023). Blockchain-enabled bioacoustics signal authentication for cloud-based electronic medical records. *Measurement: Sensors*, *26*, 100706.
12. Pudlewski, S., Prasanna, A., & Melodia, T. (2012). Compressed-sensing-enabled video streaming for wireless multimedia sensor networks. *IEEE Transactions on Mobile Computing*, *11*(6), 1060-1072.
13. Caione, C., Brunelli, D., & Benini, L. (2011). Distributed compressive sampling for lifetime optimization in dense wireless sensor networks. *IEEE Transactions on Industrial Informatics*, *8*(1), 30-40.
14. Lazarescu, M. T. (2013). Design of a WSN platform for long-term environmental monitoring for IoT applications. *IEEE Journal on emerging and selected topics in circuits and systems*, *3*(1), 45-54.
15. Cecchinel, C., Jimenez, M., Mosser, S., & Riveill, M. (2014, June). An architecture to support the collection of big data in the internet of things. In *2014 IEEE world congress on services* (pp. 442-449). IEEE.
16. Renjith, P. N., Bharati, R., Thiyagu, T. M., Vallabhuni, R. R., Mouleswararao, B., & Narayanan, L. (2023). Smart filtering for user discovery and availing balance storage space continuity with faster big data service. *Measurement: Sensors*, *26*, 100707.
17. Ishaq, I., Hoebeke, J., Moerman, I., & Demeester, P. (2012, November). Internet of things virtual networks: Bringing network virtualization to resource-constrained devices. In *2012 IEEE International Conference on Green Computing and Communications* (pp. 293-300). IEEE.
18. Vujović, V., & Maksimović, M. (2014, May). Raspberry Pi as a Wireless Sensor node: Performances and constraints. In *2014 37th international convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 1013-1018). IEEE.
19. Alliance, Z. (2004). ZigBee specification (ZigBee document 053474r06, version 1.0). *December 14th*.
20. Lee, J. S., Su, Y. W., & Shen, C. C. (2007, November). A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society* (pp. 46-51). Ieee.
21. Sadulla, S. (2024). Next-generation semiconductor devices: Breakthroughs in materials and applications. *Progress in Electronics and Communication Engineering, 1*(1), 13–18. https://doi.org/10.31838/PECE/01.01.03
22. Hoa, N. T., & Voznak, M. (2025). Critical review on understanding cyber security threats. *Innovative Reviews in Engineering and Science, 2*(2), 17-24. https://doi.org/10.31838/INES/02.02.03
23. Sadulla, S. (2024). A comparative study of antenna design strategies for millimeter-wave wireless communication. *SCCTS Journal of Embedded Systems Design and Applications, 1*(1), 13-18. https://doi.org/10.31838/ESA/01.01.03
24. Rahim, R. (2024). Optimizing reconfigurable architectures for enhanced performance in computing. *SCCTS Transactions on Reconfigurable Computing, 1*(1), 11-15. https://doi.org/10.31838/RCC/01.01.03
25. Prasath, C. A. (2024). Optimization of FPGA architectures for real-time signal processing in medical devices. *Journal of Integrated VLSI, Embedded and Computing Technologies, 1*(1), 11-15. https://doi.org/10.31838/JIVCT/01.01.03
26. Rahim, R. (2023). Effective 60 GHz signal propagation in complex indoor settings. *National Journal of RF Engineering and Wireless Communication, 1*(1), 23-29. https://doi.org/10.31838/RFMW/01.01.03
27. Dorofte, M., & Krein, K. (2024). Novel approaches in AI processing systems for their better reliability and function. *International Journal of Communication and Computer Technologies, 12*(2), 21-30. https://doi.org/10.31838/IJCCTS/12.02.03
28. Botla, A., Kanaka Durga, G., & Paidimarry, C. (2024). Development of Low Power GNSS Correlator in Zynq SoC for GPS and GLONSS. Journal of VLSI Circuits and Systems, 6(2), 14–22. https://doi.org/10.31838/jvcs/06.02.02
29. Alnumay, W.S. (2024). The past and future trends in IoT research. *National Journal of Antennas and Propagation, 6*(1), 13–22