UMYU Scientifica, Vol. 2 NO. 2, June 2023, Pp 44 – 52
https://doi.org/10.56919/usci.2322.007
ISSN: 2955 – 1145 (print); 2955 – 1153 (online)
A periodical of the Faculty of Natural and Applied Sciences, UMYU, Katsina

REVIEW ARTICLE

Resource Limitations for Wireless Sensor Networks to Establish a Comprehensive Security System in the 5G Network.

Muhammad Muntasir Yakubu[1,3*], Umar Danjuma Maiwada[2,3]
[1]Department of Information Technology, Federal University Dutsin-Ma, PMB 5001, Katsina, Nigeria.
[2]Department of Computer Science, Umaru Musa Yar'adua University, PMB 2218, Katsina, Nigeria.
[3]Computer & Information Sciences Department, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, PMB 32610 Perak, Malaysia.

ARTICLE HISTORY
Received June 05, 2023
Accepted June 25, 2023
Published June 30, 2023

KEYWORDS
Wireless, Sensor, Network, Holistic, Quantum, 5G.

ABSTRACT
The difficulty with safety in Wireless Sensor Networks (WSNs) requires comprehensive, holistic security techniques that can offer a long-term solution. Quantum security is anticipated to assist in the overall security strategy for WSN systems, given the broad adoption of WSNs around the world, notably the Internet of Things (IoTs). With the use of WSN and these quantum safeguards, data security can be offered whenever and anywhere. This study examines the security limitations of WSNs and offers a comprehensive approach through all network layers that will function as an Equal security mechanism solution and a solution to shield nodes from threats such as attacks on sensitive data, eavesdropping, disruption, destruction, and alteration. WSNs are used in a range of missions, especially the armed forces, ecological, and health ones, for evaluation, tracking, and regulating purposes. However, problems arise from being aware of their resource limitations. Data and node security are difficulties when using WSN because of low computation capabilities, small memory, few power sources, and unreliable connectivity, to name just a few. Therefore, as the demand for WSNs increases, so does the need for better security measures.

INTRODUCTION

One of the emerging disciplines that draw academics in the realm of information technology's emphasis is the study of wireless sensor networks (WSN). Considerations for this domain's current research include hardware, software, self-identification methods, energy and memory restrictions, deployment techniques, system navigation, security, and data management (Strumberger et al., 2019). The main objective of WSN is to use tiny, diminutive devices that are capable of gathering data from an actual place for a variety of uses, including target tracking, military missions, pipeline observing, weather forecasting, habitat monitoring, and traffic avoidance (Orogun et al., 2020).

The security component of WSN has not yet received priority, despite the fact that various components of WSN are receiving a lot of attention, including routing techniques, communication protocols, energy-saving techniques, and wireless sensor modeling. Since WSN implementation is constrained by a number of factors, including energy consumption, computing power, memory requirements, WSN selection/election methods, and self-organizing capabilities, WSN security issues are a serious issue. WSNs consist of extraordinarily small devices for sensing with embedded sensors, a data analysis unit, a small cache for storage, and short-range radio communication signals. In order to collect data from location in an unsecured wireless system, consolidate the results, and then send it to a sink, WSN nodes are typically put in the field. The bulk of WSN routing techniques were not designed with security in mind; rather, they were designed to make the most of WSN's limitations while ignoring security (Rathee et al., 2019).

Security is becoming more and more important because WSN technology is widely employed in security-conscious applications including warfare, target tracking, and other similar ones. Additionally, a WSN required the same level of importance for all security goals that can be met in a wireless or wired network, including verification, truthfulness, solitude, a state of non-control of access, and anti-replay attack. To accomplish these security objectives, steganography, a technique for hiding the presence of data, is frequently employed. The wavelength of the carrier is changed to hide the covert channel when

Correspondence: Muhammad Muntasir Yakubu. Department of Information Technology, Federal University Dutsin-Ma, PMB 5001, Katsina, Nigeria. ✉ ymmuhammad@fudutsinma.edu.ng. Phone Number: +234 803 293 2373
How to cite: Muhammad M. Y. and Umar D. M. (2023). Resource Limitations for Wireless Sensor Networks to Establish a Comprehensive Security System in the 5G Network. *UMYU Scientifica*, 2(2), 44 – 52. https://doi.org/10.56919/usci.2322.007

sending digital data. Due to the nature of wireless sensor networks' ability to stream multimedia content and the amount of energy needed, this type of a technique called however, cannot be utilized to directly secure data in a WSN. Another restriction on WSN is bandwidth and the processing of data that is multimedia (such as movie and audio). Additionally, all WSN security services can be used to fix the problem using cryptography (encryption and decryption) (Prakasan et al., 2022). On the other hand, the encryption and decryption methods used to secure conventional cable and wireless communications might not be expensive to deploy in a WSN. Due to the resource-constrained nature of sensor networks and the computational expense of asymmetric cryptographic algorithms, this creates significant security concerns in WSN. Limitations on WSN processing power, memory, and battery capacity, for instance, are common, particularly when many sensors are active and nodes are dispersed across a large area. Furthermore, an open-source crypto system cannot be used in WSN due to the unbalanced cryptographic technology's high cost and energy requirements. Even if the protection strategies used in ad hoc networks might not be totally applicable to WSNs, ad hoc systems and WSNs face similar security concerns (Singh et al., 2021).

This is because in a network operated in ad-hoc mode; every device is directly connected using a peer-to-peer networking paradigm, necessitating the use of an Integrated Basic Function Set (IBSS) for initiating communication between network devices (Nazir et al., 2021). For instance, several security protocols might be employed in a mobile network, including SSL and encryption at the end (IPsec). The WLAN architecture used by WSN, on the reverse hand, consists of a node or due to differences in design and implementation; security methods that can be used on peers in an ad hoc network may not be immediately relevant to a wireless sensor network (WSN) in practice wireless sensor network (WSN) in practice due to differences in design and implementation. Since WSN signals are transmitted across an unguided channel, they are more vulnerable to monitoring, Sybil assaults, worm hole assaults sinkhole assaults, denial of service assaults, Hello flood attacks, confirmation spoofing assaults, selective relaying assaults, and other security issues. A specialized security solution that provides security at both the initial and second OSI layers will not be sufficient since WSN radius broadcasts are more vulnerable. Instead, using a holistic security strategy that includes each of the seven OSI layers will be sufficient to provide overall security from the software layer all the way through to the physical one (Majid et al., 2022).

There have been numerous attempts to resolve the issue of WSN security issues in general and to find a compromise between encryption methods and WSN resource limitations. The adoption of the IEEE 802.11i specification wireless network is one of the adopted techniques to address the issue, while other methods attempt to improve on existing solutions. For wireless networks with media access control (MAC) and physical layer (PHY), IEEE 802.11i is a security standard (Olakanmi & Dada, 2020).

The 802.11i standard can be applied in both infrastructure mode and ad hoc mode. The standard uses the AES (Advanced Encryption Standard) encryption technique, which works better than the WEP (wireless comparable privacy) algorithm used by the earlier 802.11 standard. Three data privacy protocols are also introduced by the system to solve the issue of data privacy: CCMP (Counter-Mode/CBC-MAC protocol), WRAP (Wireless Robust Authenticated Protocol), and TKIP (Transport Key Integrity Protocol) (Temporal Key Integrity Protocol). The system also intensifies the identification, verification, and authorization processes to assure WLAN security (Feng et al., 2019).

On the other hand, the 802.11i CCMP protocol was discovered to be susceptible to a time storage trade off (TMTO) pre-computation assault in (Haq et al., 2023). It was found that the nonce production and transmission method of the CCMP protocol was subpar. The CCMP protocol also consumes a lot of processing power and relies on the Advanced Encryption Standard, also known as AES, and CBC-MAC (CCM) for authentication and data integrity (Kumar et al., 2021). If the amount of the content is known, such as content size long (2296) bytes, complete payload duration (2312) bytes, or whole payload duration 8bytes MIC 8bytes, the nonce number can also be precomputed. The initial counter amount used in the CCMP of 802.11i has been revealed to be forecastable thanks to the fact that the nonce value can also be precomputed by knowing the measured length of the payload from certain information, including maximum payload. This flaw in the counter block value makes a time memorization trade off (TMTO) pre-computation assault on the 802.11i CCMP feasible (Li & Fan, 2020).

(Sornalatha et al., 2021), recommendations for improving AES' processing capacity and memory limitations in the embedded processors of WSN. The study introduced LMEP-S-AES, a shortened form of AES that executes all of AES' functionalities while being memory-intensive and well suited for embedded systems. The new system uses five subfunction keys. Functions that can be employed include expansion, flattening the key, substitution, row transformation, and mix column. The new method uses the same block size of 128 as AES, but instead of using AES's 16x16 matrix, the 128 bits are stored in a single State Box of 4x4 bytes, which reduces the number of rounds to three. Additionally, with AES, a single key is used during all rounds, which reduces the extended key's memory requirements.

IEEE 802.11i has proven to be sufficiently secure in regard to privacy and integrity of data when the CCMP mechanism is used (Kumar & Paul, 2019). All WEP users will, however, need to upgrade their hardware. However, other flaws could emerge in the mutual authentication

process as it is implemented in the real world. The shared secret key may be revealed, for instance, by a man-in-the-middle assault. A dictionary assault can also be used to locate a password in a scenario where passphrases are employed to construct a 256-bit PSK. In an associated finding, (Bennett & Brassard, 2020) suggested an improved quantum handshake; a method intended to reinforce the 4-way contact in the BB84 protocol to overcome mutual authentication difficulties such as the man-in-the-middle assault in 802.11i. Quantum encryption depends on physics' quantum laws, as opposed to conventional cryptography, that is based on computation using mathematics. This ensures that no one can determine the state of an unjust divisive photon carrying knowledge without creating an issue that will be noticed by legitimate users.

Quantum cryptography is the most secure technique of key distribution since it can detect passive assaults like man-in-the-middle (eavesdropping). However, some WSN installation systems, such underwater and underground WSN, call for the installation of a high level of quantum instrument as a different line of sight channel. This obviously calls for greater computing power than a normal WSN has available. Quantum security won't work in a situation where lowering the energy consumption of WSNs is a top concern (Vazirani & Vidick, 2019).

(Hamann et al., 2022) suggested a security framework for three-party verification and distribution of keys using the Longer CK gateway of the 802.11i specification broadcast frame. The suggested approach, however, did not outline the proper definition for the access point's sessions identifier (SID). The proposed model won't be able to offer an ongoing remedy to the issue, for instance, if someone tries to mimic AP and the system has no way to handle the situation.

(Ostad-Sharif et al., 2019) compares two BR extended CK models, which are current security frameworks for the 802.11i three-party identification and key distribution protocol. The paper leverages the characteristics of AP within the framework of the 802.11i guideline to explain the idea of "Efficient AP." The article also suggested two more security simulations, both of which are suitable for WLAN, but it omitted any detailed information regarding the application of the novel three-party authentication model that was suggested.

(Dehraj & Sharma, 2021) The framework for implementation independent safety principles was introduced in wireless sensor networks. The proposed design sought to simplify accessibility, interoperability, and security of WSNs. With hesitation, one of the latest areas of scientific interest is autonomous computing. The suggested architecture integrates thermostatic features into the system for WSN to enable safety mechanisms in the event of unlawful, unintentional, or intentional modifications to security parameters.

The framework for implementation independent safety principles was introduced in wireless sensor networks. The proposed design sought to simplify accessibility, interoperability, and security of WSNs. With hesitation, one of the latest areas of scientific interest is autonomous computing. The suggested architecture integrates thermostatic features into the system for WSN to enable safety mechanisms in the event of unlawful, unintentional, or intentional modifications to security parameters (Orogun et al., 2020). Based on the preceding, WSN technology offers degrees of confidentiality and authentication capability that are effective and economical. However, there is need for a WSN system with good security and very low power consumption. In addition strong, comprehensive security measures are needed to address the WSN security conundrum permanently. Hence, the main objective of the present study is to provide an ongoing remedy to all or any of the afore-mentioned problems by creating a framework for security that strikes a balance between a thorough security mechanism and the resource limits of WSN(AlTawy et al., 2020). Therefore, the following goals are set forth:

1. Knowing that assaults in the WSN are frequently caused by the delivery of incorrect data into a hacked node across the network (Man-in-the-middle attack), it is important to use an effective diagnostic technique that is crucial for identifying any fraudulent report of attack in the WSN (Sharma & Verma, 2022).

2. There has been a lack of coordinated effort to take an approach that may address a holistic protection issue within WSN, as we observe in most of the today's WSN, so it's a need for an inexpensive and safe system that will guarantee a holistic protection service in every one of the layers of WSN (Cohen-Shacham et al., 2019).

3. To utilize the data-encryption and data-integrity capabilities of the PTK in 802.11i, which requires the application of several cryptographic algorithms to ensure information security and integrity? Furthermore, it might be necessary for every sensor network node to support a range of communication modes, such as unicast, multicast, multicast, and broadcast. The most used standard for data security, authentication, and authorization in WSN up to this point has been 802.11i (Kissi & Asante, 2020).

4. To be aware that a sensor device can be compromised by an attacker covertly since to the unsupervised nature of WSN. Therefore, a strong WSN safety system is needed to thwart a hacking attempt, and the impact of an attack should be minimized if it is successful. In terms of a security system that is tolerant of faults (Kissi & Asante, 2020).

RESEARCH DESIGN IN HOLISTIC SECURITY APPROACH IN WIRELESS SENSOR NETWORKS (WSNS)

Improving safety in terms of protection, long-term connection, and the ability to connect in a range of situations is the aim of implementing a comprehensive security strategy in WSNs. It has been found that using quantum technology, a holistic approach to the problems is more effective than a particular layer security strategy for protecting complete wireless sensor networks. To adopt an organized approach in a network, there are some requirements to meet (Lata et al., 2021).

While certain of the sensors on the nodes have been assaulted and interfered with, the safety precautions in place must allow for seamless decline; if nodes are taken by an intruder, the preventative evaluates in place must operate independently of one another within the network. Even when extra safety safeguards are in effect at the other layers, the complete network collapses when WSN protection isn't approached holistically, and an attacker obtains a node with sensors at the networks' physical layer. Security is implemented holistically across the entire network (Chiara, 2023).

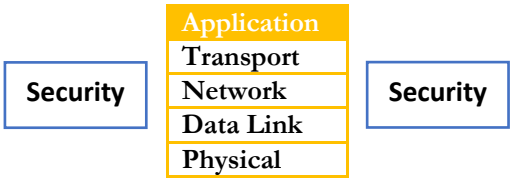

Figure 1: An in-depth analysis of privacy in wireless networks of sensors

QUANTUM CRYPTOGRAPHY TECHNIQUE

Quantum cryptography, also known as quantum key distribution (QKD), is a technique that uses principles of quantum mechanics to secure the transmission of information. Unlike classical cryptographic methods that rely on mathematical complexity, quantum cryptography is based on the fundamental laws of physics. The fundamental idea behind quantum cryptography is the use of quantum mechanics to the protection of data transmission. Quantum superposition, which asserts that a quantum system can exist in numerous states concurrently, is one of these characteristics. Another characteristic is quantum entanglement, where two or more particles link up in such a way that their states are interdependent, regardless of how far apart they are from one another (Prakasan et al., 2022).

The resulting shared secret key can be used for secure communication using symmetric encryption algorithms. The security of the key is based on the principles of quantum mechanics, making it resistant to eavesdropping attempts by attackers with classical computing power. It's important to note that while quantum cryptography provides a secure key distribution mechanism, it does not directly provide encryption of the actual data transmitted. The shared key obtained through QKD can be used in combination with classical cryptographic methods to achieve secure communication (Shamshad et al., 2022).

HERE'S A HIGH-LEVEL OVERVIEW OF HOW QUANTUM CRYPTOGRAPHY WORKS:

Quantum Key Distribution (QKD): The sender (often called Alice) and the receiver (often called Bob) establish a secure key over a public channel. They do this by using quantum properties to create a random string of bits, known as the quantum key (Cao et al., 2022).

Quantum Transmission: Alice prepares individual quantum particles (e.g., photons) with specific quantum states that represent the bits of the quantum key. She then sends these particles to Bob over a quantum channel, typically using fiber optic cables or free-space transmission (Simidzija et al., 2020).

Measurement and Detection: Bob receives the quantum particles from Alice and measures their quantum states. Due to the principles of quantum mechanics, any attempt to observe or measure the quantum particles will disturb their states. Therefore, if an eavesdropper (often called Eve) tries to intercept the quantum transmission, her measurements will introduce errors that Alice and Bob can detect (Fan et al., 2022).

Error Checking: Alice and Bob perform error-checking procedures on the quantum transmission. They compare a subset of their measurement results to check for discrepancies. If the error rate is within an acceptable range, they can proceed to the next step (Niemiec, 2019).

Key Distillation: Alice and Bob publicly communicate their measurement bases (the orientation in which they measured the quantum particles). By comparing their bases and discarding the measurement results where their bases do not match, they obtain a shared secret key (Vishal & Taruna, 2020).

Privacy Amplification: To further enhance the security of the shared key, Alice and Bob perform privacy amplification techniques. This involves applying a hash function or other mathematical operations on the shared key to eliminate any remaining information that an eavesdropper might have gained (Aldaghri & Mahdavifar, 2020).

CRITICAL DATA FOR EVALUATION REQUIREMENT FOR SECURITY

When evaluating the security requirements for critical data, it is essential to consider several factors to ensure the confidentiality, integrity, and availability of the data. Here are some key considerations:

Confidentiality: Critical data often requires strict confidentiality to prevent unauthorized access. Evaluate the sensitivity of the data and identify who should have access to it. Consider encryption techniques, access controls, and secure storage mechanisms to protect the data from unauthorized disclosure (Ahmad et al., 2022).

Integrity: Data integrity ensures that critical information remains unaltered and trustworthy. Implement measures

to detect and prevent unauthorized modifications, whether intentional or accidental. Use mechanisms such as checksums, digital signatures, and access controls to maintain the integrity of the data (Ahmad et al., 2022).

Availability: Critical data must be available when needed. Assess potential threats to data availability, such as system failures, network outages, or distributed denial-of-service (DDoS) attacks. Implement redundancy, backups, disaster recovery plans, and robust network infrastructure to ensure data availability (Ahmad et al., 2022).

Authentication and Authorization: Implement strong authentication mechanisms to ensure that only authorized individuals can access critical data. This may include multifactor authentication, biometrics, or secure login credentials. Use role-based access control (RBAC) or access control lists (ACLs) to enforce proper authorization levels for different users (Ahmad et al., 2022).

Auditability and Accountability: Maintain a robust audit trail to track access to critical data. Logging and monitoring mechanisms can help detect suspicious activities, identify potential breaches, and hold individuals accountable for their actions. Regularly review and analyze logs to ensure compliance and security (Power, 2021).

Secure Communication Channels: When transmitting critical data, ensure the use of secure communication channels. Encryption protocols such as SSL/TLS can provide secure transport of data over networks. Secure file transfer protocols (SFTP) or virtual private networks (VPNs) can also be employed for secure data exchange (Wagner et al., 2020).

Vulnerability Management: Regularly assess the security of systems and applications housing critical data. Conduct vulnerability scans, penetration tests, and security assessments to identify and remediate vulnerabilities promptly. Stay up to date with security patches, updates, and best practices to mitigate emerging threats (Fatima et al., 2023).

Employee Education and Awareness: Human factors play a crucial role in data security. Provide ongoing training and awareness programs for employees to educate them about security practices, social engineering risks, and the importance of handling critical data securely. Foster a security-conscious culture within the organization (Aldawood & Skinner, 2019).

Compliance with Regulations: Evaluate legal and regulatory requirements specific to your industry or geographical location. Ensure compliance with relevant data protection regulations, such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act), to avoid legal consequences and protect critical data (Aldawood & Skinner, 2019).

Incident Response and Recovery: Develop an incident response plan to handle security incidents promptly and effectively. Establish procedures for reporting, investigating, and containing breaches. Have a recovery plan in place to restore critical data and resume operations in the event of a security incident (Fatima et al., 2023).

SECURITY GOAL

Remember that security is an ongoing process, and it's essential to regularly review and update security measures as threats evolve. Consider engaging security professionals or consultants to perform audits and provide expertise in securing critical data.

The overarching goal of security is to protect assets, whether they are data, systems, infrastructure, or people, from unauthorized access, misuse, disclosure, alteration, or destruction. Those security objectives are interrelated and frequently call for a tiered strategy to achieve complete asset protection and reduce potential threats. Based on their objectives, industry standards, and legal and regulatory constraints, organizations should identify their specific security goals (Bock et al., 2020).

INTEGRATED SECURITY SOLUTION IN WSN

An integrated security solution in Wireless Sensor Networks (WSNs) refers to a comprehensive approach that combines multiple security measures and mechanisms to protect the network and its assets from various threats. WSNs typically consist of numerous low-power sensor nodes that communicate wirelessly to collect and transmit data. Due to the resource-constrained nature of sensor nodes and the wireless communication medium, security in WSNs poses unique challenges (Sharma & Verma, 2022). An integrated security solution in WSNs should address the following aspects:

Secure Communication: WSNs require secure communication channels to protect data transmission from eavesdropping, tampering, or interception. Encryption techniques such as symmetric key cryptography or lightweight cryptographic algorithms can be employed to ensure confidentiality and integrity during data exchange (Aldawood & Skinner, 2019).

Node Authentication: Verify the authenticity and trustworthiness of sensor nodes to prevent unauthorized nodes from joining the network. Public key cryptography, digital certificates, or shared secrets can be used for node authentication during the network initialization phase (Kumar & Paul, 2019).

Data Integrity and Validation: Ensure the integrity and validity of data collected by sensor nodes. Techniques such as message authentication codes (MACs), digital signatures, or hash functions can be used to verify the integrity of data packets and detect any tampering or modifications (Shamshad et al., 2022).

Access Control: Establish access control mechanisms to restrict unauthorized access to sensor nodes and network resources. Role-based access control (RBAC) or access control lists (ACLs) can be employed to define and enforce access privileges for different entities in the network (Lata et al., 2021).

Intrusion Detection and Prevention: Implement mechanisms to detect and mitigate potential attacks or intrusions in the WSN. Intrusion detection systems (IDS) or anomaly detection algorithms can be used to identify abnormal behaviors or patterns that may indicate malicious activity. Intrusion prevention mechanisms, such as packet filtering or anomaly-based intrusion prevention systems (IPS), can help block or mitigate attacks (Keerthika & Shanmugapriya, 2022).

Key Management: Efficient and secure key management is crucial in WSNs to ensure the confidentiality and integrity of data transmissions. Key establishment, distribution, revocation, and updating mechanisms should be designed to minimize overhead while maintaining security (Rathee et al., 2019).

Energy-Efficient Security: Due to the limited energy resources of sensor nodes, security solutions in WSNs should be energy-efficient. Lightweight cryptographic algorithms, energy-aware key management protocols, and optimized security mechanisms can be employed to minimize energy consumption while providing the necessary security (Nazir et al., 2021).

Secure Localization: Localization is essential in WSNs for various applications. Secure localization techniques can ensure the accuracy and reliability of location information by preventing malicious nodes from manipulating or tampering with localization data (Chiara, 2023).

Secure Over-the-Air Programming: Over-the-Air Programming (OTAP) allows remote updates and reprogramming of sensor nodes. Secure OTAP mechanisms ensure that only authorized and authenticated updates are installed on the nodes to prevent unauthorized code execution or tampering (Bock et al., 2020).

Security Monitoring and Management: Implement monitoring and management systems to oversee the security of the WSN. Centralized or distributed management systems can provide real-time monitoring, logging, and auditing capabilities to detect security incidents and manage security policies (Olakanmi & Dada, 2020).

HOLISTIC SECURITY APPROACH ON WSN

A holistic security approach in Wireless Sensor Networks (WSNs) involves considering all aspects of security, from design and implementation to monitoring and response, in a comprehensive and integrated manner. It focuses on addressing the security challenges and requirements of WSNs through a systematic and multi-layered approach (Maiwada et al., 2022). Here are key components of a holistic security approach for WSNs:

Secure Network Architecture: Design a secure network architecture that considers the specific requirements and constraints of the WSN. This includes defining network boundaries, establishing secure communication channels, and designing the placement and deployment of sensor nodes to minimize vulnerabilities (Shamshad et al., 2022).

Threat Modeling and Risk Assessment: Conduct a thorough analysis of potential threats and vulnerabilities specific to the WSN application. Identify potential attack vectors and assess the impact and likelihood of security incidents. This helps in prioritizing security measures and allocating resources effectively (Fatima et al., 2023).

Robust Cryptographic Mechanisms: Implement strong and lightweight cryptographic mechanisms to ensure secure communication and data protection. This includes encryption algorithms, message authentication codes, and secure key management protocols suitable for resource-constrained sensor nodes (Li & Fan, 2020).

Authentication and Access Control: Employ mechanisms for node authentication and access control to prevent unauthorized nodes from joining the network and accessing sensitive resources. This involves techniques such as mutual authentication, digital certificates, and access control policies to enforce authentication and authorization (Kumar & Paul, 2019).

Data Confidentiality and Integrity: Ensure the confidentiality and integrity of data collected and transmitted by sensor nodes. Apply encryption techniques to protect data confidentiality, and employ integrity checks, such as checksums or digital signatures, to ensure data integrity throughout the network (Chiara, 2023).

Intrusion Detection and Prevention: Deploy intrusion detection and prevention mechanisms to identify and mitigate potential attacks or anomalies in the network. This includes anomaly-based detection algorithms, intrusion prevention systems, and real-time monitoring to detect and respond to security incidents (Keerthika & Shanmugapriya, 2022).

Physical Security Measures: Implement physical security measures to protect sensor nodes and the WSN infrastructure from physical tampering, theft, or unauthorized access. This can include secure enclosures, tamper-evident seals, and surveillance systems to ensure the physical integrity and protection of the WSN (Lata et al., 2021).

Secure Over-the-Air Updates: Implement secure mechanisms for over-the-air updates and reprogramming of sensor nodes. Ensure that only authenticated and authorized updates are installed to prevent unauthorized code execution or malicious updates compromising the network (Rathee et al., 2019).

Security Awareness and Training: Foster a culture of security awareness among WSN stakeholders, including network administrators, developers, and end-users. Conduct regular training and awareness programs to educate them about potential risks, best practices, and their roles in maintaining the security of the WSN (Maiwada et al., 2022).

Continuous Monitoring and Response: Establish mechanisms for continuous monitoring and response to security events. This includes real-time monitoring of network activity, logging and auditing of security events, and timely incident response procedures to detect, investigate, and mitigate security breaches or anomalies (Olakanmi & Dada, 2020).

Regular Security Assessments: Conduct regular security assessments and audits to identify potential vulnerabilities, gaps in security measures, or compliance issues. Periodic assessments help ensure that the WSN's security posture remains robust and up to date in the face of evolving threats (Singh et al., 2021).

CONCLUSION AND FUTURE WORK

The security goals are interconnected and often require a layered approach to ensure comprehensive protection of assets and mitigate potential risks. Organizations should define their specific security goals based on their unique requirements, industry standards, and regulatory obligations. An integrated security solution in WSNs should consider the specific requirements, constraints, and characteristics of the network. It should strike a balance between security requirements, resource limitations, and the unique operational needs of the WSN application. By adopting a holistic security approach, WSNs can benefit from a comprehensive and integrated security framework that addresses various aspects of security, mitigates risks, and ensures the confidentiality, integrity, and availability of data and resources within the network.

As the rising usage of WSNs becomes more viable, improved methodologies are urgently required for security, privacy, power, computing capability, and scalability are all requirements. Industries and organizations are asking for a full-proof WSN system that assures data privacy, integrity, freshness, identity verification, and reliability, as well as WSNs that can meet Quality of Service, security needs, attack vulnerability, and encryption algorithms. Some may claim that this is since WSNs were in their infancy, therefore current plans are attack oriented. When security-related difficulties arise, researchers only improve security protocols, recommend new ones, or fix issues. Because existing models were created specifically to tackle specific assaults, they may fail if unanticipated attacks occur. Nonetheless, the security of WSNs has gained in importance as a study topic, and much work must be done by researchers to focus on and develop a holistic integrated system that would handle the entire security concerns of WSNs.

REFERENCES

Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. Computer Science Review, 43, 100452. **[Crossref]**

Aldaghri, N., & Mahdavifar, H. (2020). Physical layer secret key generation in static environments. IEEE Transactions on Information Forensics and Security, 15, 2692-2705. **[Crossref]**

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), 73. **[Crossref]**

AlTawy, R., Gong, G., Mandal, K., & Rohit, R. (2020). Wage: An authenticated encryption with a twist. IACR Transactions on Symmetric Cryptology, 132-159. **[Crossref]**

Bennett, C. H., & Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:2003.06557.

Bock, E. A., Amadori, A., Brzuska, C., & Michiels, W. (2020). On the security goals of white-box cryptography. IACR transactions on cryptographic hardware and embedded systems, 327-357. **[Crossref]**

Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys & Tutorials, 24(2), 839-894. **[Crossref]**

Chiara, P. G. (2023). Security and Privacy of Resource Constrained Devices University of Luxembourg, Luxembourg, Luxembourg].

Cohen-Shacham, E., Andrade, A., Dalton, J., Dudley, N., Jones, M., Kumar, C., Maginnis, S., Maynard, S., Nelson, C. R., & Renaud, F. G. (2019). Core principles for successfully implementing and upscaling Nature-based Solutions. Environmental Science & Policy, 98, 20-29. **[Crossref]**

Dehraj, P., & Sharma, A. (2021). A review on architecture and models for autonomic software systems. The Journal of Supercomputing, 77, 388-417. **[Crossref]**

Fan, P., Rahman, A. U., Ji, Z., Ji, X., Hao, Z., & Zhang, H. (2022). Two-party quantum private comparison based on eight-qubit entangled state. Modern Physics Letters A, 37(05), 2250026. **[Crossref]**

Fatima, A., Khan, T. A., Abdellatif, T. M., Zulfiqar, S., Asif, M., Safi, W., Al Hamadi, H., & Al-Kassem, A. H. (2023). Impact and Research Challenges of Penetrating Testing and Vulnerability

Assessment on Network Threat. 2023 International Conference on Business Analytics for Technology and Security (ICBATS), [Crossref]

Feng, Y., Jayasundara, C., Nirmalathas, A., & Wong, E. (2019). A feasibility study of IEEE 802.11 HCCA for low-latency applications. IEEE Transactions on Communications, 67(7), 4928-4938. [Crossref]

Hamann, M., Moch, A., Krause, M., & Mikhalev, V. (2022). The DRACO stream cipher: A power-efficient small-state stream cipher with full provable security against TMDTO attacks. IACR Transactions on Symmetric Cryptology, 1-42. [Crossref]

Haq, I. U., Ramzan, S., Ahmad, N., Ahmad, Y., & Nadeem, A. (2023). Towards Robust and Low Latency Security Framework for IEEE 802.11 Wireless Networks. International Journal of Computing and Digital Systems, 14(1), 1-xx.

Keerthika, M., & Shanmugapriya, D. (2022). A Systematic Survey on Various Distributed Denial of Service (DDoS) Attacks in Wireless Sensor Networks (WSN). 2022 IEEE 7th International Conference on Recent Advances and Innovations in Engineering (ICRAIE), [Crossref]

Kissi, M. K., & Asante, M. (2020). Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools. International Journal of Computer Applications, 975, 8887.

Kumar, A., & Paul, P. (2019). A Secure Three-Way Handshake Authentication Process in IEEE 802.11 i. Proceeding of the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017), [Crossref]

Kumar, T. M., Reddy, K. S., Rinaldi, S., Parameshachari, B. D., & Arunachalam, K. (2021). A low area high speed FPGA implementation of AES architecture for cryptography application. Electronics, 10(16), 2023. [Crossref]

Lata, S., Mehfuz, S., & Urooj, S. (2021). Secure and reliable wsn for internet of things: Challenges and enabling technologies. IEEE Access, 9, 161103-161128. [Crossref]

Li, J.-D., & Fan, C.-P. (2020). Design and VLSI Implementation of Low Latency IEEE 802.11 i Cryptography Processing Unit. Journal of Advances in Computer Networks, 8(1). [Crossref]

Maiwada, U. D., Muazu, A. A., & Noor, N. (2022). The Security Paradigm That Strikes a Balance Between a Holistic Security Mechanism and The WSN's Resource Constraints. East Asian Journal of Multidisciplinary Research, 1(3), 343-352. [Crossref]

Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C.-W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6), 2087. [Crossref]

Nazir, R., Laghari, A. A., Kumar, K., David, S., & Ali, M. (2021). Survey on wireless network security. Archives of Computational Methods in Engineering, 1-20.

Niemiec, M. (2019). Error correction in quantum cryptography based on artificial neural networks. Quantum Information Processing, 18(6), 174. [Crossref]

Olakanmi, O. O., & Dada, A. (2020). Wireless sensor networks (WSNs): Security and privacy issues and solutions. Wireless mesh networks-security, architectures and protocols, 13, 1-16. [Crossref]

Orogun, E., Erivwo, O., Ideh, M., Okon, W., & Ageh, E. (2020). Optimizing Technology Applications with Compatibility Challenges in Remote Operating Environments–A Niger Delta Case Study. SPE Nigeria Annual International Conference and Exhibition, [Crossref]

Ostad-Sharif, A., Arshad, H., Nikooghadam, M., & Abbasinezhad-Mood, D. (2019). Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. Future Generation Computer Systems, 100, 882-892. [Crossref]

Power, M. (2021). Modelling the micro-foundations of the audit society: Organizations and the logic of the audit trail. Academy of management review, 46(1), 6-32. [Crossref]

Prakasan, A., Jain, K., & Krishnan, P. (2022). Authenticated-encryption in the quantum key distribution classical channel using post-quantum cryptography. 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), [Crossref]

Rathee, M., Kumar, S., Gandomi, A. H., Dilip, K., Balusamy, B., & Patan, R. (2019). Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. IEEE Transactions on Engineering Management, 68(1), 170-182. [Crossref]

Shamshad, S., Riaz, F., Riaz, R., Rizvi, S. S., & Abdulla, S. (2022). An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), Employing quantum computing supremacy. Sensors, 22(21), 8151. [Crossref]

Sharma, S., & Verma, V. K. (2022). An integrated exploration on internet of things and wireless sensor networks. Wireless Personal Communications, 124(3), 2735-2770. [Crossref]

Simidzija, P., Ahmadzadegan, A., Kempf, A., & Martín-Martínez, E. (2020). Transmission of quantum

information through quantum fields. Physical Review D, 101(3), 036014. **[Crossref]**

Singh, P., Acharya, B., & Chaurasiya, R. K. (2021). Lightweight cryptographic algorithms for resource-constrained IoT devices and sensor networks. In Security and Privacy Issues in IoT Devices and Sensor Networks (pp. 153-185). Elsevier. **[Crossref]**

Sornalatha, R., Janakiraman, N., Balamurugan, K., Sivaraman, A. K., Vincent, R., & Muralidhar, A. (2021). FPGA Implementation of Protected Compact AES S–Box Using CQCG for Embedded Applications. Smart Intell. Comput. Commun. Technol., 38, 396-401. **[Crossref]**

Strumberger, I., Minovic, M., Tuba, M., & Bacanin, N. (2019). Performance of elephant herding optimization and tree growth algorithm adapted for node localization in wireless sensor networks. Sensors, 19(11), 2515. **[Crossref]**

Vazirani, U., & Vidick, T. (2019). Fully device independent quantum key distribution. Communications of the ACM, 62(4), 133-133. **[Crossref]**

Vishal, & Taruna, S. (2020). An Efficient Quantum Key Management Scheme. 4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2019: Internet of Things and Connected Technologies, **[Crossref]**

Wagner, P. G., Birnstill, P., & Beyerer, J. (2020). Establishing secure communication channels using remote attestation with TPM 2.0. Security and Trust Management: 16th International Workshop, STM 2020, Guildford, UK, September 17–18, 2020, Proceedings 16, **[Crossref]**