East Asian Journal of Multidisciplinary Research (EAJMR)
Vol.1, No.3 2022: 343-352

The Security Paradigm That Strikes a Balance Between a Holistic Security Mechanism and The WSN's Resource Constraints

Umar Danjuma Maiwada[1], Aminu Aminu Muazu[2], Nadzira Noor[3]

[1,2]Umaru Musa Yaradua University Katsina
[3]Universiti Teknologi Petronas

ABSTRACT: There is a need for comprehensive holistic security methods that can provide a long-term response to the challenge of security in Wireless Sensor Networks (WSNs). Due to the widespread use of WSN around the world, particularly the Internet of Things (IoTs), quantum security is predicted to aid in the comprehensive security strategy for WSN environments. These quantum securities can be used in conjunction with WSN to provide data security anywhere and at any time. The goal of this study is to examine the security constraints of WSNs and provide a holistic strategy across all network tiers that will serve as a balanced security mechanism solution, as well as a solution to protect nodes from vital data attack, eavesdropping, disruption, destruction as well as alteration and other threats. WSNs are utilized for monitoring, tracking, and controlling applications in a variety of operations, including military, ecological, and health. However, the nature of their resource constraints causes difficulties. Low compute capabilities, tiny memory, limited energy resources, and unreliable communications are just a few of the factors that make data and node security problematic when employing WSN. As a result, as the need for WSNs grows, so does the requirement for improved security methods.

Keywords*: Wireless, Sensor, Network, Holistic, Quantum*

Submitted: ***07.04.2022****; Revised:* ***16.04.2022****; Accepted:****27.04.2022***

DOI prefik: 10.55927
ISSN-E: 2828-1519
https://journal.formosapublisher.org/index.php/eajmr

INTRODUCTION

The topic of WSN is one of the rising fields that attracts the scholars in the area of information technology's focus (Wireless Sensor Network). Hardware, software, self-localization algorithms, energy and memory limits, deployment procedures, navigation systems, security, and data management are all factors to consider all topics of ongoing study in this domain **[1].** WSN's main goal is to use small, tiny devices capable of sensing, processing, communicating, and storing information from a physical location for various purposes such as security surveillance, military operations, pipeline monitoring, weather forecast, habitat monitoring, traffic avoidance, control systems, and target tracking **[2],** among others.

Though several aspects of WSN are gaining a lot of attention, such as routing methods, communication protocols, energy saving approaches, and wireless sensor modelling, the security element of WSN has yet to be prioritized. As a result, WSN security difficulties are a severe problem that necessitates the consideration of several parameters, including energy, processing power, WSN selection/election algorithms, memory, and WSN self-organizing capabilities, all of which are constraints to WSN implementation. WSNs are made up of extremely small sensor devices with integrated sensors, a data processing unit, a small memory for storage, and radio communication signals with a short range. Typically, WSN nodes are installed in the field to gather data from the field in an unattended wireless network, aggregate the data, and then deliver it to a sink. The majority of WSN routing protocols were created to maximize WSN's limited capabilities while ignoring the issue of security **[3],** even though these protocols were not created with security in mind.

Because WSN technology is widely used in security-conscious applications such as military operations, target tracking, and so on, security becomes increasingly crucial. In addition, all security objectives that may be satisfied in a wired or wireless network, such as authentication, integrity, privacy, nonrepudiation, access control, and anti-replay attack, were equally critical in a WSN. However, steganography, a method for disguising the existence of data, is commonly used to achieve these security aims. When transferring digital data, the carrier frequency is altered so that the covert channel is concealed. This sort of steganography, however, cannot be directly used to safeguarding data in a wireless sensor network due to the nature of WSN's multimedia streaming abilities and the quantity of energy required. Furthermore, bandwidth and processing of multimedia data (such as video and audio) is another constraint to WSN. Also, the use of cryptography (encryption and decryption) can be used to solve the problem of all WSN security services. The encryption / decryption techniques used to protect traditional cable & wireless communications, on the other hand, may not be expense for use in a WSN. This is due to the computational cost of asymmetric crypto schemes, as well as the resource-constrained nature for sensor networks raises substantial security challenges in WSN. WSN processing power limits, memory limitations, and poor battery capacity, for example, especially when the majority of sensors are all active & nodes are spread out across a vast region. Furthermore, due to the cost and energy

demands of the asymmetric cryptographic method, a public key cryptography system cannot be implemented in WSN. Ad-hoc networks and WSNs have comparable security challenges, albeit the defense methods utilized in ad-hoc networks may not be entirely relevant to WSNs.

This is due to the fact that in an ad-hoc network mode, all devices are directly connected in a peer-to-peer network paradigm, requiring network devices to initiate communication in an Independent Basic Service Set (IBSS) [4]. In an ad hoc network, for example, multiple security protocols such as SSL and end-to-end encryption (IPsec) might be used. WSN, on the other hand, employs a WLAN infrastructure that includes a node/station (STA), an access point (AP), and a server or controlling centre (sink). In practice, due to the design and deployment differences between WSN and ad hoc network, security protocols that can be applied to peers (adhoc network) may not be directly applicable to WSN. WSN signals are more prone to eavesdropping, sybil attacks, worm hole attacks, sinkhole attacks, denial of service attacks, Hello flood assaults, acknowledgement spoofing attacks, selective forwarding attacks, and other security problems since they are delivered across an unguided channel. Because WSN radius signals are more susceptible, a specific security solution that offers security with the first and second OSI levels will not adequate. Instead, employing a holistic approach to security that involves all seven OSI layers for ensuring a general security from the application layer down to the physical layer **[5]** will suffice.

STATEMENT OF THE PROBLEM

WSN technology provides levels of capability for data privacy and authentication that are both efficient and cost-effective, possibility of presenting a WSN solution with very low power consumption having well energy efficiency and strong security is required. There are demands for robust comprehensive security methods that can provide a long-term solution to the WSN security dilemma. There are many security-related difficulties that may arises in WSN, researchers only improve the security protocols, recommend new ones, or fix issues forgetting that other layers of the network needs to be looked upon. Another problem is how to detect passive attack and fault tolerance.

AIM AND OBJECTIVES

At its core, the research study aims to give a long-term solution to some or all of the difficulties by developing a security model that balances a comprehensive security mechanism with the resource's constraints of WSN. The following are the objectives:

1. To employ an effective detection technique that is essential for detecting any false report attack in the WSN, knowing that attacks in the WSN are commonly generated by the injection of fake information into a compromised node inside the network (Man-in-the middle attack).
2. To employ a security scheme that is based on a specific network model, there is a need for a cost-effective and security model that can ensure a holistic security service in all seven layers of WSN, because there is a lack of combined effort to take a common

model that can solve a holistic security problem in WSN, as we can see in most of today's WSN.
3. To employ the PTK's data-encryption and data-integrity features in 802.11i, which entails the use of various cryptographic algorithms to achieve data confidentiality and integrity. Additionally, each sensor network node may be required to support a variety of communication models, including unicast, multicast, and broadcast. So far, 802.11i has been the most widely used standard in WSN for data privacy, authentication, and authorization. As a result of the limited battery life and the large amount of energy required by various cryptographic algorithms and authentication processes in WSN, a new security mechanism is needed to balance the energy constraints of WSN devices, the energy required for encryption algorithms, and the communication mechanisms in WSN.
4. To know that an attacker can compromise a sensor device without being discovered because to the unattended nature of WSN. As a result, a powerful WSN security mechanism is required to defend against an attack, and the consequence of an assault should be reduced if it succeeds. In other words, a fault-tolerant security system.

HOLISTIC SECURITY APPROACH IN WIRELESS SENSOR NETWORKS (WSNS)

The goal of using a holistic security strategy in WSNs is to improve security performance in terms of security, long-term connectivity, and the capacity to connect in a variety of environments. Using the quantum technique, in ensuring protection in entire wireless sensor networks, it has been observed that a holistic view in its difficulties is more effective than individual layer security strategy. There are certain criteria to follow in order to adopt a systematic view in a network.

While some of the sensor nodes have been threatened and tampered with, the measures in place must allow for smooth degradation; if nodes have been captured by an attacker, the precautionary measures in place must work independently of each other within the network; and if nodes have been captured by an attacker, the precautionary measures in place must work independently of each other within the network. When WSN security is not approached holistically, and an intruder captures a sensor node at the network's physical layer, the overall network collapses, even if extra security measures are in place in the other layers. Security is applied across the whole network in a holistic perspective.

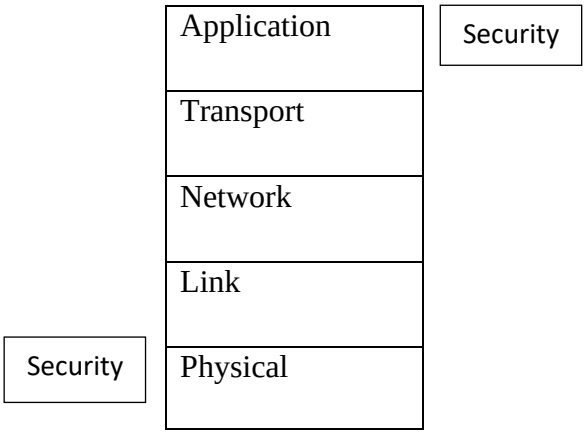

Figure 1: A Comprehensive View on Privacy within Wireless Sensor Networks

QUANTUM CRYPTOGRAPHY TECHNIQUE

Physics knowledge was utilized to build a cryptosystem which is believed to be completely secured and impervious to tampering without the approval of the client receiving and sending the signal to data sniff or eavesdropping. The regular encryption system and quantum cryptography are vastly different. Quantum cryptography uses physics as the backbone of its security paradigm, rather than computational mathematics. Quantum cryptography is the application of quantum mechanical processes to cryptographic functions to build a secure path between sender and recipient during message transmission. The supply of an information-theoretically secure solution to the handshake problem via quantum key distribution is a well-known example of quantum cryptography.

Another significant advantage of quantum cryptography over traditional encryption is its capacity to complete a variety of cryptographic tasks that have been proved to be nearly impossible to do using classical communication. If an unauthorized user tries to read, store, or sniff the quantum encryption, for example, the quantum code will be modified as well.

CRITICAL DATA FOR EVALUATION REQUIREMENT FOR SECURITY

The vulnerability of WSN nodes to danger and harsh settings necessitates special security considerations when developing WSN security protocols. As a result, a variety of security services were evaluated, including confidentiality, authenticity, integrity, availability, nonrepudiation, freshness, forward secrecy, and backward secrecy.

CONFIDENTIALITY

When sending data across sensor nodes, the necessity for secrecy in security services is crucial, since it ensures that data is kept private. Packets are successfully received in the first occurrence of file transfer between two nodes. However, to prevent attackers from gaining access to sensitive data, successive packets are encrypted at the receiving end, ensuring secrecy between sensor nodes that do not share the same decryption keys.

AUTHENTICITY

Authenticity is essential for ensuring the security of node identities when communicating. Even if the message was transmitted by a genuine sender, any transmitting node must be checked before being acknowledged. It would be easy for attackers to introduce bogus data onto wireless sensor networks if there was no authentication.

INTEGRITY

By generating packet interruption and a rogue routing node that may modify the priority of data packets, attackers can control polarity. As a result, to ensure integrity, it is vital to ensure that sent messages are not modified or changed in any manner by attackers.

AVAILABILITY

The ability to supply data when it is needed is a significant feature of Wireless Sensor Networks. Attackers frequently sabotage the availability of nodes inside the network by launching attacks that degrade the network's performance, thereby jeopardizing the network's capacity.

SECURITY GOAL

Even if standard security protocols are implemented to WSNs as well as other communication systems, sensor nodes are susceptible to and vulnerable to attacks owing to their nature, that includes being discarded without monitoring in an uncontrolled environment limited resources. In the case of secrecy, information is only available to authorized individuals. The identification of data that has been changed from sender to the receiver is done in integrity since the sender andrecipient of the conveyed message do not have the authority to deny the transmission in non-repudiation. As a result, access control resources are only available to qualified parties.

INTEGRATED SECURITY SOLUTION IN WSN

Due to the lack of a visible line of defense for WSNs, a complete security solution should include three major elements: eavesdropping avoidance, detection, and reaction. The preventive component would increase the system's quality by preventing sniff infiltration. As history has often proved, a complete proof invasion free system is impossible for eavesdroppers, regardless of how excellent the preventative techniques in

WSNs are. WSNs relying on a holistic approach or quantum mechanism have been discovered to be vulnerable to manipulation or physical slavery.

Because quantum encryption requires a comprehensive approach, detection and response components that help in detecting uncommon intrusions and taking measures to prevent ongoing negative consequences which are crucial for security systems to work in the presence of limited resources. Keys, quantum security, as well as a holistic strategy have all been recognized as parts of prevention that stop attackers from keeping and sniffing nodes communications inside a network in the context of WSN. The detecting part is what discovers the ongoing sniffs. On sensor nodes, sniffs were recognized using a holistic approach technique or quantum security. When the security mechanism detects an attacked node trying to store and sniff, the response building block portion of the security mechanism adapts to prohibit the targeted node from the network.

HOLISTIC SECURITY APPROACH ON WSN

Because each entity inside the network layer seeks to defend its system by identifying the layer it serves, the first step is to define the structure of the WSN holistic security method as a potential deployment of quantum cryptography structure whose defense system was studied and has focused on delivering a core framework quantum encryption for security perspective strategy implementation. There are three primary steps to the creation, execution, and assessment of these initiatives. To avoid eavesdropping, quantum cryptography was encoded, and the strategic planning technique was changed holistically.

The holistic approach seems to have three main goals: first, to guarantee that probable threats relating to information systems and crucial message passing are discovered and risks have been mitigated slightly earlier; second, workplace and business such as private corporations, government agencies, and citizens to implementing the security remedies that will protect eaves droppers from sniffing vital information; and third, to identify such as private corporations, government entities, and residents to implementing the security solutions which will protect eaves droppers from sniffing vital information that are intended for interested parties such as private corporations or government agencies.

CONCLUSION AND RECOMMENDATION

Finally, as WSNs are subject to a vast range of vulnerabilities and obstacles, Eavesdropping, man-in-the-middle attacks, manipulation of data, data distortions, phishing, due to data loss, and theft of data have all become typical security concerns. Data on WSNs must be protected from all forms of attack, as failing to do so will have serious implications. Certain researchers have employed a monolithic solution framework to prevent various WSN security concerns, however, to effectively safeguard the network, a comprehensive security solution is required.

This study proposes layer-by-layer protection, quantum security, permission, authentication, or other measures to address WSN security problems. Starting with layer-by-layer protection, so using quantum protection, and eventually avoiding eavesdroppers from obtaining the corporate network that used a range of approaches, such as layer-by-layer protection, quantum security, permission, authentication, or other measures. The insertion of fake information, sniffing, and storage of messages by tampered nodes inside the network is one of the most prevalent security threats in wireless sensor networks. These attacks have the same objective to compromise the network's integrity, availability, and secrecy, and these challenges have been handled through a holistic strategy that uses the network's levels.

Unauthorized access and data modification during transmission should be prevented via encryption or client and server authentication are not implemented, it will become a major area of research in WSNs. Because most current research focuses on specialized network models, there is a dearth of effort put together done by researchers to create a recognized design approach for wireless sensor networks. It uses a holistic approach to assure security for all network levels. Future research should hopefully result in the development of a very well security for each WSN network level, which will integrate the security features and function holistically inside a single system, collaborating among them. Even if comprehensive security is penetrated, researchers would have substantial hurdles in adopting such a strategy owing to a shortage of resources for sensor nodes, cost benefits, and energy efficiency. Demonstrating resilience on an attacked node, for example, is currently impossible. As a result, a method for detecting false reports and preventing attackers from injecting false reports through compromised nodes must be established. Building such an effective and efficient detection and prevention security mechanism, on the other hand, is a major research challenge.

As the rising usage of WSNs becomes more viable, improved methodologies are urgently required for security, privacy, power, computing capability, and scalability are all the 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 due to the fact that WSNs were in their infancy, therefore current plans are attack oriented. When security-related difficulties arises, 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 an 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.

ACKNOWLEDGMENT

We will like to thank and appreciate the efforts made by Dr. Abubakr Aminu Muazu and Dr. Kamaluddeen Usman Danyaro for their tremendous help, advice and guidance in the success of this research.

REFERENCES

[1] Amitangshu Pal, "Localization Algorithms in Wireless Sensor Networks," *Network Protocols and Algorithms,* Vols. Vol. 2, No. 1, pp. 45-48, 2010.
[2] F. Idachaba, "Remote Operation of Oil and Gas production installations in the Niger Delta," *Asian Transactions on Engineering,* vol. Volume 01, no. Issue 03, pp. 45-59, 2011.
[3] D. W. Chris Karlof, "Secure routing in wireless sensor networks: attacks," *Elsevier,* vol. 1, pp. 293-315, 2003.
[4] T. Hollingshead, "802.11 Wireless Security vs. Basic Network Security Principles," Global Information Assurance Certification, 2003.
[5] Al-Sakib Khan Pathan, "Security in Wireless Sensor Networks: Issues and challenges," 2006, 2006.
[6] I. M. Junaid, "Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol," *World Academy of Science, Engineering and Technology 11 2007,* vol. II, pp. 910-915, 2007.
[7] Suhas J Manangi, "Simplified AES for Low Memory Embedded," *Global Journal of Computer Science and Technology Processors,* vol. Vol. 10 14, no. 14, pp. 7-11, 2010.
[8] J. C. M. Changhua He, "Security Analysis and Improvements for IEEE 802.11i". Electrical *Engineering and Computer Science Departments, Stanford University, Stanford CA 94305.*
[9] M. A. S. a. S. G.-H. Thi Mai Trang Nguyen, "802.11i Encryption Key Distribution Using Quantum Cryptography," *JOURNAL OF NETWORKS,* vol. 1, no. 5, pp. 9-20, SEPTEMBER/OCTOBER 2006.
[10] H. A. a. Y. B. S. Yubo, "The provable security formal analysis of 802.11i authentication scheme," *Engineering Sciences,* vol. 1, no. 12, pp. 67-73, 2010.
[11] T. W. a. H. Bin, "A Stronger Formal Security Model of Three-party Authentication and Key Distribution Protocol for 802.11i," *International Journal of Security and Its Applications,* vol. 6, no. 4, pp. 163-174, 2012.
[12] A. P. Hosam Soleman, "Architecture for Application Autonomic Protection Principles in Wireless Sensor Network," *International Journal of Computer Applications,* vol. 64, no. 6,pp. 39-42, 2013.