Securing Data Transmission from Adversaries in Cybersecurity WSN Using Efficient Key Management Techniques

Kamlesh Kumar Yadav[1], Dhablia Dharmesh Kirit[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.*

KEYWORDS

Cyber Security, Health, Security, Privacy, WSN.

ABSTRACT

Concern over cyber security is becoming more and more prevalent in today's international politics. National security is now evaluated not only in terms of military might or economic might, but also in terms of technological innovation. The fact that today's society is heavily dependent on computer communication and control systems, which opens up infinite opportunities, shows how important technology is in the national security area. By effectively changing the keys, the suggested work aimed to provide WSN with complicated security solutions that would ensure data integrity, security, and genuine transmission for many additional network operations through structured cryptography approaches. The study's protective measures can be applied to a variety of WSN configurations, including heterogeneous WSNs with and without mobility aid and static homogeneous WSNs. Because WSN is more limited to hardware resources, not all applications can be protected using the same method.

1. Introduction

Cybersecurity pertains to the "technologies, processes, and policies that aid in preventing or mitigating the adverse effects of cyberspace events that may arise from intentional attacks on information technology by a hostile or malevolent actor." However, at the same time, cyber security concerns are regarded as one of the biggest hazards to public safety, economic growth, and national security facing all countries worldwide [1]. A multitude of incidents in recent years demonstrate how cyberspace has developed into an area of increased activity and conflict, where some countries and organisations operate for the purpose of stealing and espionaging intellectual property, while others obtain state support to act against other countries. However, cyberterrorists take advantage of the anonymity provided by this platform to further their own cause [9]. While numerous criminal groups and individuals engage in financial fraud, money theft, and blackmail online [2]. In the era of information, communication, and technology, cyber security has developed into a challenging and quickly evolving security issue [6]. With the increasing reliance of nations on ICT, there is a possibility that cyber threats are infiltrating every aspect of the country's infrastructure and economy. Furthermore, it now plays a crucial role in business and governance and is given consideration when it comes to issues of national security [13]. As the world's reliance on computers and internet-based networking grows, so does the frequency of cyberattacks [3]. Governments and internet users are more likely to become targets as a result of these attacks. Therefore, there could be grave consequences from any cyberattack that targets people, companies, or even governmental institutions. Furthermore, certain governments and nations are beginning to view it more and more as a strategic asset that can be used for national security objectives and even as a battlefield where strategic wars might be fought [12]. Examine the importance of cyber security in the current security discourse in this setting. Additionally, I would want to find out how cyber security fits into the national security narrative and why India's national security is becoming more concerned about it. Because cyber security encompasses a wide range of disciplines, it is a multifaceted issue that necessitates varied actions and responses. The endeavour becomes more challenging due to the dynamic and diffuse character of threats and the incapacity to formulate a suitable reaction when there are no physical perpetrators [4]. The technological dynamism of the ever-evolving ICT domain has made the cyber realm less predictable. Threats and the answers to them follow each other due to the rapid advancement of technology, which is also outside the purview of national governments. Furthermore, the implementation of traditional security techniques is further

complicated by deniability, anonymity, and occasional untraceability. In this particular setting, the study aims to investigate the evolution of the cyber security mechanism [5].

2. Methodology

Many small sensors with transducers are scattered throughout wireless sensor networks. They are used to track and monitor variables found in the actual environment, such as sound, temperature, and velocity. Any specified sink nodes receive data that have been combined by the sensor node's built-in transducers, either directly or via a series of hops via intermediary nodes. Transmission is insecure because of the ease with which attackers can take advantage of the wireless environment and the attributes of the sensor node. To safeguard and guarantee safe data transfer, security needs to be strengthened both inside the environment and within the nodes [11]. The main difficulty in implementing security in a wireless environment is the requirement for varying degrees of security, which must be granted to various application types while effectively utilising the available network resources. The security that is given to the applications must correspond with the different WSN features that need to be considered, such as node mobility, topology implementation, different security settings, etc. Efficient key management and encryption algorithms must be developed with these properties in mind [7].

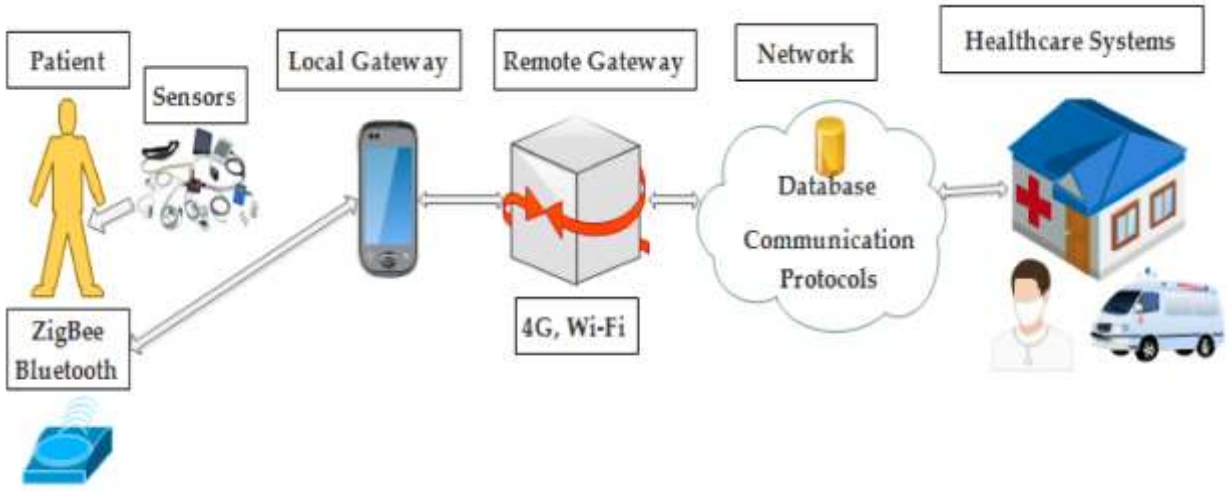

Figure 1. Proposed overflow

The suggested study focusses on applications that require differing degrees of security and come in a range of sizes. The outcomes of the suggested strategies successfully prevented a number of security assaults, including node capture and jammer attempts. The suggested security measures protect the devices communicating within the WSN and preserve the privacy, integrity, and confidentiality of the information that is transmitted. The freedom granted to nodes to join and leave the network at any time without prior notice is one of the main characteristics of WSN [8]. The original method that was put forth used the channel hopping methodology to perform dynamic key generation, which led to a dynamic key update for each conversation that was started over a new channel. Adversaries can simply infiltrate malicious nodes into the WSN and use them to launch a variety of assaults. A jamming attack involves the attacker jamming the transmission path, which causes the data to be transmitted corruptly. The suggested method uses dynamic key management, which causes data to hop across channels as it is being transmitted [14]. As a result, the amount of time data travels across any given channel is decreased. This reduces the likelihood that enemies will mount a successful attack because the transiting channels are constantly shifting. The suggested method's effectiveness was evaluated against the security framework protocol of the SNMP (Simple Network Management Protocol). Using the NS2 simulator, performance evaluation was conducted by taking into account the energy consumption, packet delivery ratio, delay, and network lifetime quality factors [10].

3. Results And Discussion

With the Network Simulator (NS2) tool, the recommended key management strategy for WSNs is simulated. In this experiment, different network layer attacks are employed on a network consisting of 300, 400, 500, 600, and 700 randomly placed sensor nodes spread throughout a 1000 × 1000 metre area. The radio transmission range of each node is roughly 250 meters, and the channel's capacity is 2 Mbits/sec. By changing the number of nodes with a defined number attack of 5 and the optimisation algorithm's iteration level of 100, the suggested system SNMP's efficiency is assessed [10]. Figure 2's delay efficiency for the various nodes and the delay of the put-forth OC-KMS are clearly visible as being less than those of the current SNMP system, although they have improved in relation to the increase in attack counts.

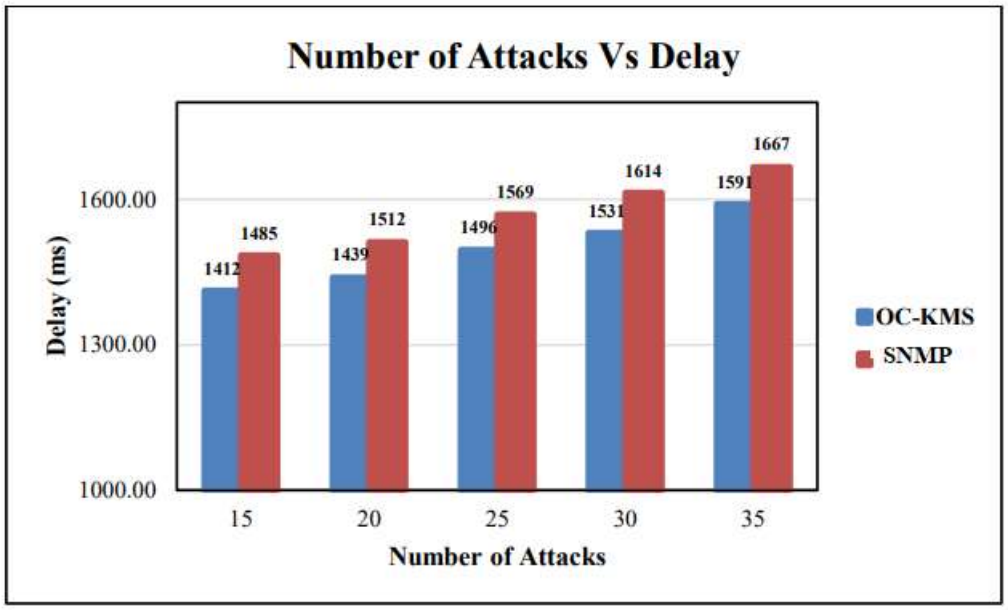

Figure 2. Number of attack Vs Delay

The efficiency of the distribution ratio with respect to the different nodes is mapped in Figure 3, where the distribution ratio of the proposed OC-KMS is evidently quite high in comparison to the current SNMP system, albeit slightly lower than the increase in attacks.

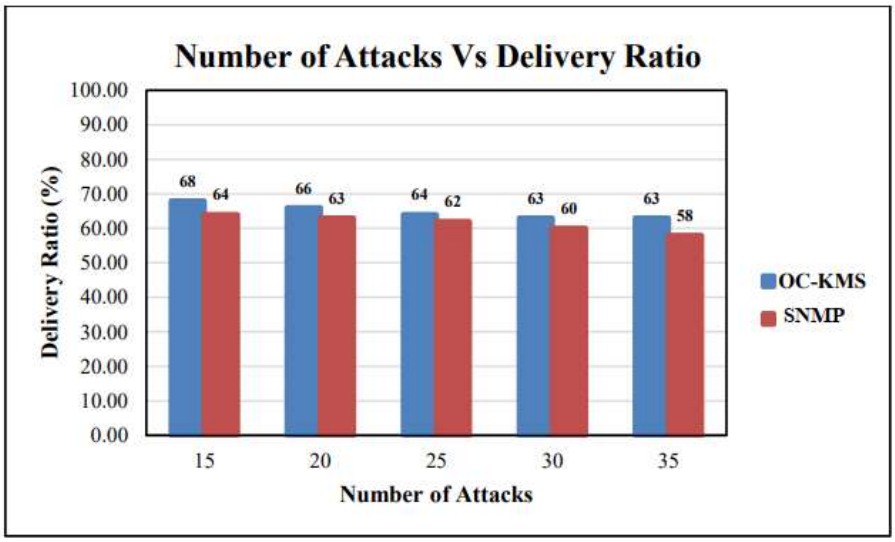

Figure 3. Number of attack Vs Delivery Ratio

Figure 4 maps the efficiency of energy consumption with regard to the different nodes. It is evident that the energy consumption of the proposed OC-KMS is significantly lower than that of the present

SNMP approach, but it is greater in terms of the increase in assaults.

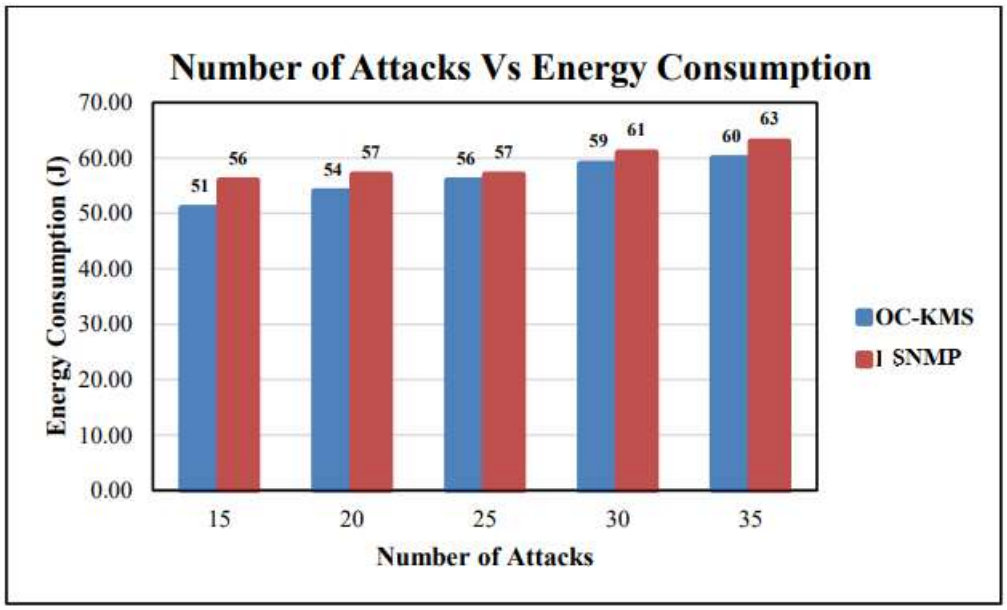

Figure 4. Number of attack Vs Energy Consumption

We plot the network lifetime in relation to the various attacks in Figure 5. The network lifetime of the suggested OCKMS is far longer than that of the existing SNMP system, and it is accurately shown.

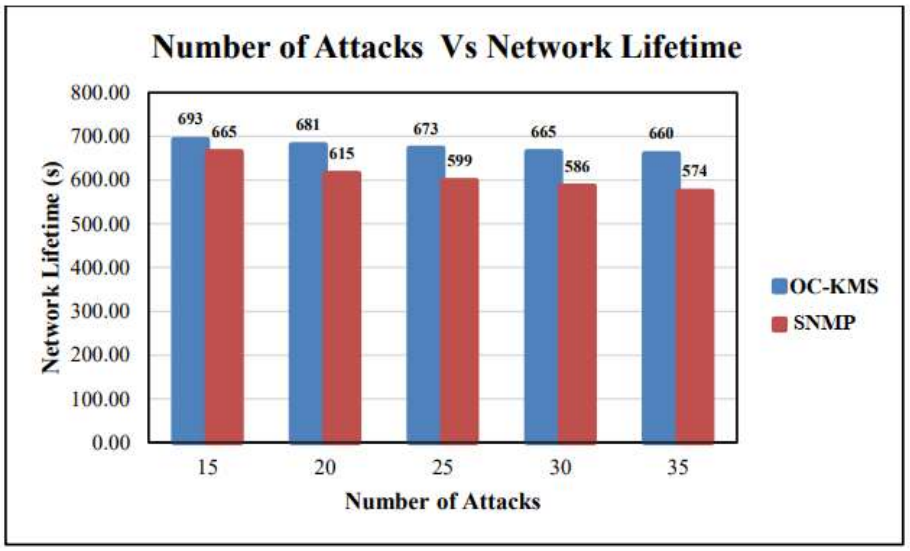

Figure 5. Number of attack Vs Network Lifetime

This study aims to investigate the nature and importance of cyber security in the context of the evolving global environment, as well as national and international responses to these threats. It lists the players, networks, and cooperative mechanisms that India's cyber security requires. The construction, identification of the study's characteristics, and development of the empirical mode of inquiry that characterises the phenomenon have all been done using a qualitative research methodology.

4. Conclusion

Systematic study has been done to clarify the foundations of dependable cryptographic algorithms and effective key management for WSN and its applications. It is well known that no single static or dynamic key management technique can be used to all three types of applications. For small-scale

installations, a basic protection strategy needs to be implemented in order to prolong the life of the network. The risks associated with the area where medium- and large-scale network applications have been deployed determine safety. Scalability is an important element to consider in medium- and large-scale systems. To ensure scalability, the nodes need to be organised into separate clusters. Depending on how the topology of the network changes, choosing the cluster head is one of the important tasks that needs to be done continuously and frequently. The vast majority of modern deployments need support with mobility. Dynamically generated node clustering is possible in the context of mobility assistance. Incorporating heterogeneous nodes capable of performing intricate tasks on a regular basis into the network might enhance its overall functionality.

Reference

[1] Busdicker, Mike, and Priyanka Upendra. "The role of healthcare technology management in facilitating medical device cybersecurity." *Biomedical Instrumentation & Technology* 51, no. s6 (2017): 19-25.

[2] Thomasian, Nicole M., and Eli Y. Adashi. "Cybersecurity in the internet of medical things." Health Policy and Technology 10, no. 3 (2021): 100549.

[3] Ammi, M., & Jama, Y. M. (2023). Cyber Threat Hunting Case Study using MISP. Journal of Internet Services and Information Security , 13(1), 1-29.

[4] Marotta, Angelica, and Stuart Madnick. "Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case." Issues in Information Systems 23, no. 1 (2022).

[5] Kwon, Juhee, and M. Eric Johnson. "Healthcare security strategies for regulatory compliance and data security." In 2013 46th Hawaii International Conference on System Sciences, pp. 3972-3981. IEEE, 2013.

[6] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[7] Lee, Chien-Ding, Kevin I-J. Ho, and Wei-Bin Lee. "A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations." IEEE Transactions on Information Technology in Biomedicine 15, no. 4 (2011): 550-556.

[8] Anderson, Scott, and Trish Williams. "Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge?" Computer Standards & Interfaces 56 (2018): 134-143.

[9] Komisarek, M., Pawlicki, M., Kozik, R., & Choras, M. (2021). Machine Learning Based Approach to Anomaly and Cyberattack Detection in Streamed Network Traffic Data. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 12(1), 3-19.

[10] Lechner, Nadica Hrgarek. "An overview of cybersecurity regulations and standards for medical device software." In Central European Conference on Information and Intelligent Systems, pp. 237-249. Faculty of Organization and Informatics Varazdin, 2017.

[11] Kelly, Brendan, Conor Quinn, Aonghus Lawlor, Ronan Killeen, and James Burrell. "Cybersecurity in Healthcare." Trends of Artificial Intelligence and Big Data for E-Health (2023): 213-231.

[12] Premakumari, R. N., et al. "Modeling the dynamics of a marine system using the fractional order approach to assess its susceptibility to global warming." Results in Nonlinear Analysis 7.1 (2024): 89-109.

[13] Nifakos, Sokratis, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina. "Influence of human factors on cyber security within healthcare organisations: A systematic review." Sensors 21, no. 15 (2021): 5119.

[14] Oleksandr, K., Viktoriya, G., Nataliia, A., Liliya, F., Oleh, O., Maksym, M. (2024). Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. Natural and Engineering Sciences, 9(1), 26-45.

[15] Abraham, Chon, Dave Chatterjee, and Ronald R. Sims. "Muddling through cybersecurity: Insights from the US healthcare industry." Business horizons 62, no. 4 (2019): 539-548.