ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

IMPROVING SECURITY IN WIRELESS SENSOR NETWORK USING ENCRYPTION AND DECRYPTION WITH CETSAD

T.Nirmalraj [a], Dr.J.Jebathangam [b]

[a] Research Scholar, Department of Computer Science, School of Computing Science, VISTAS, Chennai

[b] Associate Professor, Department of Information Technology, School of Computing Science, VISTAS, Chennai

ABSTRACT: As WSN networks expand, they become more vulnerable to assaults, necessitating the use of effective security procedures. The identification of acceptable cryptography for wireless sensor networks is a significant difficulty due to the sensor nodes' limited energy, processing power, and storage resources, which is referred to as dependable Crypto Encryption Trust Secure Attacker Detection. CETSAD fulfills critical WSN requirements such as energy efficiency, dependability, data aggregation, and attacker detection. CETSAD is an energy-efficient routing method that identifies routes that use the least amount of energy for end-to-end packet traversal while also improving malicious node detection. To implement the Encryption approach in WSN, we suggested a cryptography-based security mechanism. Improving the encryption and decryption components of an existing method, paving the path for superior security.

Keyword: CETSAD, WSN networks, cryptography, encryption, decryption

I. INTRODUCTION

Wireless communication technology, along with power-saving design alternatives, has provided a new frontier for WSN, which has expertly pertained to another parallel expanding sphere of big data prediction, learning, and analysis. With the goal of automating industrial and manufacturing units, as well as the acceleration of MEMS and sensor technologies, the potential of WSNs is fast expanding [1]. Wireless sensor networks (WSNs) are becoming more essential as a platform for acquiring and processing data in the physical environment. The application determines the security level. Data confidentiality and integrity are essential needs in most applications. Cryptography methods must be implemented on sensor nodes to meet these criteria [2].

Trust may be defined as the notion that something is trustworthy enough to not harm or disrupt the smooth operation of real-time applications. It is extremely important in everyday life as well as when dealing with sensitive data [3]. Trust models are the procedures for getting trust information and determining the trustworthiness of each node. A trust model is employed not just for higher-layer choices like routing and data aggregation, but also for cluster head election and data aggregation, perhaps shockingly, key distribution. Its goal is to improve security and, as a result, boost the throughput, longevity, and resilience of a sensor network [4].

Wireless Sensor Networks' security has become an issue (WSNs). To accomplish security services such as Authentication, Confidentiality, and Integrity, several cryptographic algorithms have been developed. In WSNs, there are two major issues with security standards. To begin, the overload that security methods impose in messages should be kept to a minimum; every bit the sensor sends consumes energy and, as a result, diminishes the device's life. Second, the memory size, which relates to the size of the encrypted message as well as the key size, should be lowered [5]. The use of well-known symmetric-key cryptography is a simple yet effective solution. Symmetric-key approaches, on the other hand, offer a variety of disadvantages. It has limited scalability, requires a lot of memory to store key materials, is difficult to add or remove keys, and requires a complex key pre-distribution method [6]. CETSAD is an energy-efficient routing method that identifies routes that use the least amount of total energy for end-to-end packet traversal while also improving malicious node detection. In this research, we propose a cryptography-based security strategy for use in WSN encryption.

II. RELATED WORKS

Wander et al. [7] have attempted to evaluate well-known security problems in WSNs and to investigate the behavior of WSN nodes performing public key cryptographic operations. Simulation is used to assess the time and power consumption of a public key cryptography method for signature and key management. According to their estimations, RSA is not well suited for WSNs. When comparing ECC-160 with RSA-1024, it becomes clear that the work required for RSA cryptography is excessive. While using the even more powerful ECC-224 appears to be possible, the time and power consumption of the comparable RSA-2048 is considerably above what is tolerable. Public-key cryptography, in addition to key management and secure communication, may be used to enable a variety of additional WSN applications, such as securely connecting ubiquitous

devices to the Internet and disseminating signed software patches.

Großschädl et al. [9] They examine and evaluate the energy costs of two distinct techniques for establishing authenticated keys. The first protocol uses 128-bit AES encryption and a lightweight implementation of the Kerberos key transit mechanism. The second protocol is based on ECMQV, an authenticated variant of the Diffie-Hellman key exchange for elliptic curves, and employs a 256-bit prime field GF(p) as the underlying algebraic structure. On a Rockwell WINS node with a 133 MHz Strong ARM CPU and a 100 kbit/s radio module, the energy consumption of both protocols was examined. The evaluation takes into account both the energy used by the CPU to calculate cryptographic primitives and the energy cost of radio transmission at various transmit power levels. The ECMQV key exchange uses up to twice as much energy than Kerberos-like key transmission, according to our simulation results.

Chien-Erh Weng et al. [10] They created a routing method that use the proximity technique to choose the best group of nodes for transmission, hence enhancing lifespan and addressing routing loop concerns. The usefulness of the proposed Proximity Based Energy Efficient Routing (PEER) is evidenced by the improvements in lifetime and energy usage.

Deepak C. Mehetre et al. [11] Their research offered a dependable and secure WSN routing system that employs a two-stage security mechanism and a dual assurance approach to choose the node and protect the data packet. Active Trust is used by both systems to fight against various forms of routing attacks, such as black hole attacks and selective forwarding attacks. As a result, this research uses trust and the Cuckoo search algorithm to find the trusted path and provide secure routing pathways. In the suggested technique, energy is employed as a performance metric.

III. PROPOSED METHOD

The wireless sensor network is the most often used network presently (WSN). WSN sensors, on the other hand, are restricted in terms of energy and transmission range, necessitating the use of a number of intermediary sensor nodes to perform cooperative transmission. The WSN, like any other network, is vulnerable to a number of adversarial assaults. Data transmission is often achieved by selecting the optimum path between any two geographically separated nodes. The broadcast mechanism, which can manage route selection, handles route discovery and any protocol, such as shortest path, energy efficient routing, and so on. WSN networks become more vulnerable to attacks as they grow in size, necessitating the implementation of appropriate security mechanisms. Identifying appropriate cryptography for wireless sensor networks is a critical challenge termed reliable Crypto Encryption Trust Secure Attacker Detection due to the limited energy, computing capabilities, and storage capacities of sensor nodes. CETSAD fulfils several key WSN criteria, including energy efficiency, dependability, data aggregation, and detection of attackers. CETSAD is an energy-efficient routing method that identifies routes that use the least amount of total energy for end-to-end packet traversal while also improving malicious node detection.

i. Energy efficiency

With the rapid advancement of hardware technology, CPUs and flash memory are getting smaller, more powerful, and more affordable. As a result, the memory and processing capabilities of sensor nodes will no longer be the most significant barrier to WSN implementation. However, battery technology has yet to achieve a breakthrough. Clearly, the energy capacity of sensor nodes will be the primary obstacles for the long-term development of WSNs. As a result, research into increasing the energy efficiency of WSNs in order to extend network lifetime remains a priority for the time being and in the future. The energy efficient routing algorithms and clustering algorithms are the key technological strategies and methods for enhancing the energy efficiency of WSNs. CETSAD method developed an improved energy-efficient routing method for WSNs.

ii. Reliability

In the context of industrial applications, safe and dependable communications are crucial in IWSNs, because a lack of data security and dependability might lead to a production line shutdown, manufacturing equipment damage, or even worker fatality. If a sensor detects an abnormally high temperature (or pressure) in a machine engine, the machine will shut down, for example, a failing transmission of this critical information obstructs an emergency reaction and may cause engine damage. A rogue sensor might potentially cause false alerts to interrupt the manufacturing process. As a result, it is critical to ensure the security and reliability of data connections in IWSNs.

Method CETSAD In IWSNs, maintain extremely dependable data connections. In industrial applications, establishing highly reliable data communications in IWSNs is crucial because wireless sensors may generate safety-critical data that must be communicated consistently and swiftly to the sink.

iii. Data Aggregation

Any procedure that gathers data and summarises it is referred to as data aggregation. When data is aggregated, individual data rows are replaced with totals or summary statistics, which are usually acquired from numerous sources. Summary statistics based on those observations are used to replace groups of observed aggregates. Aggregate data is commonly found in a data warehouse since it can answer analytical queries while also drastically reducing the time it takes to query big amounts of data.

Individual data pieces with individually identifiable features are aggregated and replaced with a summary reflecting a group as a whole in data aggregation, which has a similar effect to data anonymization. Rather than searching through individual employee records containing pay data, create a summary that provides the aggregate average wage for employees by department.

Numeric data isn't required for aggregate data. You may count the number of any non-numeric data element, for example.

iv. Attacker's detection

In general, there are two types of network security solutions: prevention-based tactics and detection-based procedures. Encryption and authentication are commonly employed as the first line of defense against cyber-attacks. Detection-based tactics aim to identify and exclude the attacker once prevention-based measures have failed. Signature detection and anomaly detection are the two sorts of detection procedures.

Anomaly detection compares established normal profiles to strange deviations from this normal behavior, whereas signature detection compares known attack patterns to current alterations.

The next crucial step is to select a detection algorithm that uses the criteria to identify infiltration trends.

v. Cryptography

The planned CETSAD is presented in this section. Today, several cryptographic approaches are popular. Some of them were created during the dawn of contemporary cryptography technology in the late twentieth century. Later, several of the strategies were instilled with further changes and refinements of their predecessors. To be familiar with this particular issue statement of boosting the security level of the WSN without sacrificing the performance metrics of its intrinsic parameters, a fundamental comprehension of cryptographic algorithms is required. To ensure secrecy, integrity, availability, data authenticity, data freshness, and non-repudiation, all feasible cryptographic approaches must meet the quality criteria of a secure WSN.

a. Encryption

The first step in offering extra security services like encryption is to create shared secret keys across nodes in a WSN. This could be done with pre-deployed shared keys, but it poses important storage considerations as well as node compromise resilience in big networks. As a result, key distribution or key agreement protocols are employed as a solution when the nodes are deployed.

Table I. Comparison on existing algorithms

Reference	Authors	Algorithm	advantages
[13]	Simarmata	AES	AES is most efficient in speed, throughput
[14]	Fuertes	RSA	Found that RSA is widely used
[15]	Vasantha	Blowfish	Blowfish - greater than all, better in performance. Blowfish power consumption value is least
[16]	KAMEPALLI	SHA	SHA provided better security and less

Energy consumption overhead

Table II shows the energy usage of each algorithm. This is assessed using power consumption statistics collected from Micaz nodes. When operating in busy mode at 7.37MHz, the average current of the ATmega128L is around 8.7mA. We utilise mAh as a unit to remove the influence of voltage variation.

Table I. Energy consumption rate on each algorithm

Algorithm	Encryption time for 1Mb file in (s)	Energy consumption (10^{-6} mAh)	
		Encryption	Decryption
AES	0.483	1.25	1.37
RSA	0.825	1.12	1.22
Blowfish	0.290	0.918	1.09
SHA	0.250	0.865	0.923
CETSAD	0.185	0.578	0.61

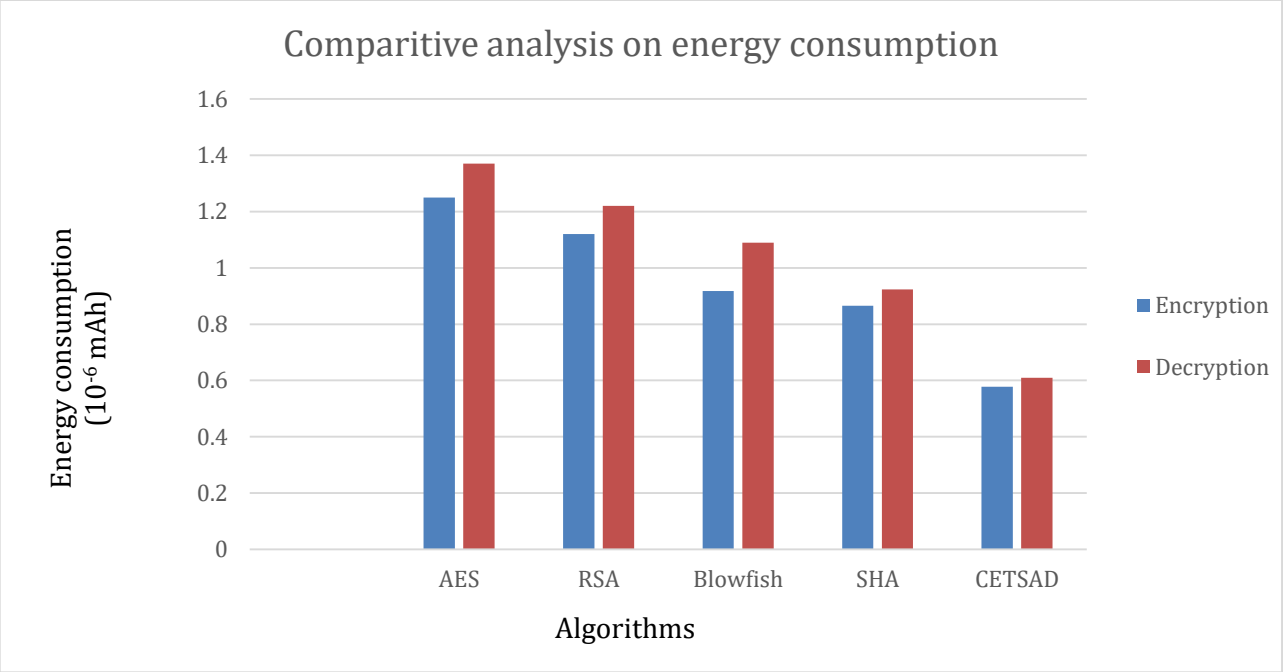

Figure1. Comparison of Energy consumption on Encryption and Decryption

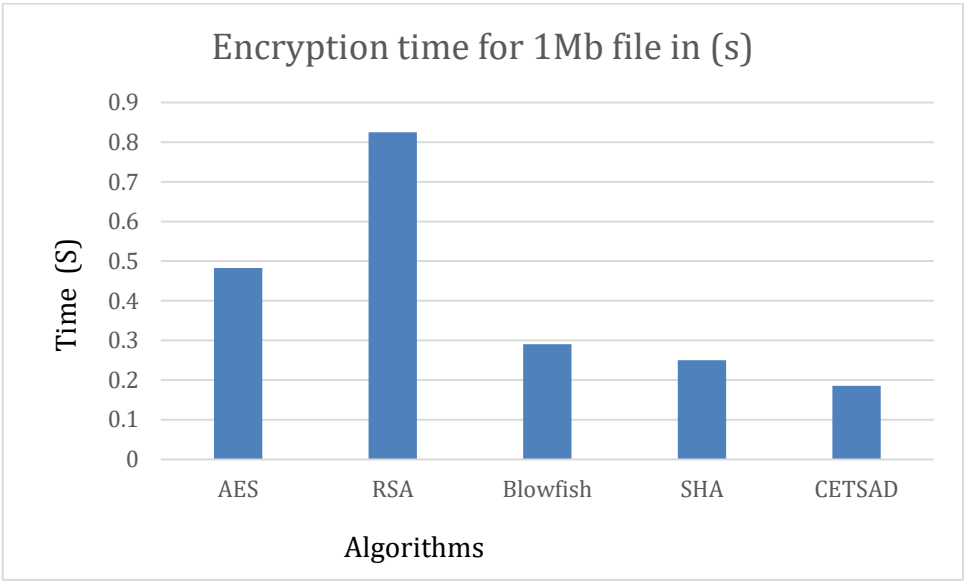

Figure2. Comparison of encryption time

The CETSAD cryptography technology was used to accelerate the encryption and decryption processes. This will eliminate any overhead delay while maintaining security. When we compare and assess the performance of the symmetric and asymmetric key cryptography approaches employed in the various studies, we can infer that the former greatly decreases the cryptosystem's calculation time.

IV. CONCLUSION

As WSN networks expand, they become more vulnerable to assaults, necessitating the use of effective security procedures. Due to the limited energy, compute capabilities, and storage resources of sensor nodes, identifying adequate cryptography for wireless sensor networks is a significant problem called dependable Crypto Encryption Trust Secure Attacker Detection. CETSAD fulfils several key WSN criteria, including energy efficiency, dependability, data aggregation, and detection of attackers. CETSAD is an energy-efficient routing method that identifies routes that use the least amount of total energy for end-to-end packet traversal while also improving malicious node detection. In this research, we propose a cryptography-based security strategy for use in WSN encryption. We get excellent security by improved encryption and decryption aspects of the WSN networks.

V. REFERENCES

1) Mallick, B. B., & Bhatia, A. (2021). Comparative Analysis of Impact of Cryptography Algorithms on Wireless Sensor Networks. *arXiv preprint arXiv:2107.01810*.

2) Liu, W., Luo, R., & Yang, H. (2009, January). Cryptography overhead evaluation and analysis for wireless sensor networks. In *2009 WRI International Conference on Communications and Mobile Computing* (Vol. 3, pp. 496-501). IEEE.

3) Mehmood, G., Khan, M. Z., Waheed, A., Zareei, M., & Mohamed, E. M. (2020). A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks. *IEEE Access*, *8*, 131397-131413.

4) Zahariadis, T., Leligou, H. C., Trakadas, P., & Voliotis, S. (2010). Trust management in wireless sensor networks. *European Transactions on Telecommunications*, *21*(4), 386-395.

5) Alkady, Y., Habib, M. I., & Rizk, R. Y. (2013, December). A new security protocol using hybrid cryptography algorithms. In *2013 9th International Computer Engineering Conference (ICENCO)* (pp. 109-115). IEEE.

6) Le, X. H., Lee, S., Butun, I., Khalid, M., Sankar, R., Kim, M., ... & Lee, H. (2009). An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography. *Journal of Communications and Networks*, *11*(6), 599-606.

7) Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005, March). Energy analysis of public-key cryptography for wireless sensor networks. In *Third IEEE international conference on pervasive computing and communications* (pp. 324-328). IEEE.

8) Yin, G., Yang, G., Yang, W., Zhang, B., & Jin, W. (2008, January). An energy-efficient routing algorithm for wireless sensor networks. In *2008 International Conference on Internet Computing in Science and Engineering* (pp. 181-186). IEEE.

9) Großschädl, J., Szekely, A., & Tillich, S. (2007, March). The energy cost of cryptographic key establishment in wireless sensor networks. In *Proceedings of the 2nd ACM symposium on Information, computer and communications security* (pp. 380-382).

10) Weng, C. E., Sharma, V., Chen, H. C., & Mao, C. H. (2016). PEER: Proximity-Based Energy-Efficient Routing Algorithm for Wireless Sensor Networks. *J. Internet Serv. Inf. Secur.*, *6*(1), 47-56.

11) Mehetre, D. C., Roslin, S. E., & Wagh, S. J. (2019). Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. *Cluster Computing*, *22*(1), 1313-1328.

12) Kumar, M. H., Mohanraj, V., Suresh, Y., Senthilkumar, J., & Nagalalli, G. (2021). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. *Journal of Ambient Intelligence and Humanized Computing*, *12*(5), 5287-5295.

13) Simarmata, J., Limbong, T., Ginting, M. B., Damanik, R., Padli, M. I., Nasution, A. H. H., ... & Sinambela, M. (2018). Implementation of AES Algorithm for information security of web-based application. *Int. J. Eng. Technol*, *7*(3.4), 318-320.

14) Fuertes, W., Meneses, F., Hidalgo, L., & Torres, J. RSA OVER-ENCRYPTION IMPLEMENTATION FOR NETWORKING: A PROOF OF CONCEPT USING MOBILE DEVICES.

15) Vasantha, R., & Prasad, R. S. (2017). An advanced security analysis by using blowfish algorithm. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *2*(5), 1031-1036.

16) KAMEPALLI, S., & REDDY, A. S. (2020). Analysis of Secure Hash Algorithm (SHA-512) For Encryption Process on College Web Based Application.