SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549 / https://doi.org/10.14445/23488549/IJECE-V10I4P105

Volume 10 Issue 4, 41-50, April 2023
© 2023 Seventh Sense Research Group®

Original Article

Data Security in Wireless Sensor Networks using an Efficient Cryptographic Technique to Protect Against Intrusion

S. Suma Christal Mary[1], S. Jothi Shri[2], E. Thenmozhi[3], K. Murugeswari[4]

[1,3]*Department of Information Technology, Panimalar Engineering College, India*
[2]*Department of Artificial Intelligence &Data Science, Panimalar Engineering College, India*
[4]*Department of Computer Science and Engineering, Panimalar Engineering College, India*

[1]*Corresponding Author : professorsumachristalmary@gmail.com*

Received: 28 February 2023 Revised: 03 April 2023 Accepted: 14 April 2023 Published: 30 April 2023

Abstract *- The ubiquitous nature of wireless sensor networks (WSNs) means that their underlying network architecture may be used to serve a broad range of use cases, from "smart cities" to "smart homes" and beyond. Other serious problems, such as energy use and security, have persisted. When it comes to WSN security, the blockchain might be the answer. Traditional blockchains have limitations, such as inefficient transaction processing and limited scalability. When Wireless Sensor Networks (WSNs) are deployed, most of the time, the nodes are left unmanaged and vulnerable to various security threats. Reliable data distribution in WSNs is nontrivial because of the limited resources and dynamic behavior of sensor nodes. Traditional cryptography and authentication-based methods have been shown to be unsuitable for countering node misbehavior attacks due to their high cost and incapability. The lightweight authentication encryption system was developed to solve the problems of sensor resource scarcity and data security (data integrity and secrecy). Current trust-based solutions, on the other hand, increase traffic congestion and decrease the network's lifespan due to the high costs associated with trust estimates and network-wide dissemination. As a result, the objective of this study is to present an intrusion prevention architecture for mobile Internet of Things devices, along with its integration into WSN, to ensure data security while simultaneously improving the network delivery ratio. The architecture that has been suggested is made up of two different discrete components. To begin, the ambiguity principle is used to construct non-overlapping and independently structured clusters, which are then used to preserve the clusters' stability. Second, based on the architecture of the blockchain, encrypted multi-hop routing pathways with end-to-end coverage are being established. By reducing end-to-end latency, time consumption, packet loss rate, and energy usage while increasing throughput, our recommended model's simulation results reveal good results and security gains.*

Keywords *- Data security, WSN, Encryption, Cluster, Intrusion prevention.*

1. Introduction

Mobile nodes, the small, low-cost sensor nodes that make up WSNs, are subject to severe resource constraints. The sensors are placed around the study area, allowing for collecting and analysing environmental data (e.g., mechanical, thermal, biological, chemical, and optical readings). Environment monitoring (including the monitoring of atmosphere, soil, and moisture), condition-based maintenance, ecosystems monitoring (including the determination of the population and behaviour of plant and animal species), seismic recognition, surveillance systems, stock management, smart spaces, and assembling sensed data in uninhabitable locations, healthcare and home protection, machine diagnosis, contaminant detection, etc. are just some of the many areas in which they can be used. Since most sensors on board are battery-operated, a lot of work has been done to build energy-aware protocols, particularly at the data connection layer. One of the primary motivations for creating such schemes is the need to maximise energy efficiency in network interaction to lengthen the service life of the network.

Densely distributed sensor nodes, each equipped with sensing and computing capabilities and linked through wireless connections, constitute a sensor network as shown in fig.1. Each sensor node is a self-contained, low-power, intelligent device that can sense its environment, do basic processing, and communicate wirelessly with other nodes. The data produced by sensor networks are uncontrolled, each with its own format and standards, and may be used for everything from national security to medical applications to environmental monitoring. With the use of sensor networks, researchers worldwide may access data in near real-time. One of the greatest obstacles in the modern world is extracting this data to study and comprehend.

WSNs are often required to function autonomously and unsupervised, making the nodes vulnerable to a wide range of assaults. Safe routing techniques [1-5] have been

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

designed to prevent these kinds of assaults on WSNs. These methods rely on encryption and authentication, two standard security techniques. However, they aren't well suited for use in WSNs to prevent malicious activity on individual nodes. Most cryptographic, authentication and encryption systems and algorithms work under the assumption that all nodes involved are reliable and trustworthy. On the contrary, insider or node misbehaviour attacks [6] prove this assumption is unrealistic. The sensor nodes' limited access to memory, computing power, and other vital resources hinders their ability to deploy sophisticated security measures.

On the other hand, most cryptographic methods have prohibitively high resource requirements [7] in the areas of computing, memory, and energy. Most cryptography and authentication-based techniques need centralised agents for security management, which is often not viable in WSN [8]. Typical security techniques are deemed useless in an unattended setting, where sensor nodes are susceptible to manipulation by an adversarial force with simple access to valid keys and memory contents [10]. The trust and reputation-based techniques implemented with the intention of protecting WSNs have been shown to be more resistant to node misbehavior attacks. A recent development in the realm of security provision, trust-based security [7], does away with the need for cryptographic methods.

While routing protocols are used to determine the best way between nodes, their function does not extend to selecting the monitor nodes in multi-path setups. Considering the aforementioned goals, we've created these hybrid networking and monitoring techniques to bolster protection across all available channels. When determining which nodes will provide monitoring, the procedure is performed effectively at the time of routing. Combining routing characteristics and properties with sensor monitor different levels that encrypt the different channels with a two-fish cryptographic system with the unexpected key-share origin of the word allows data to travel efficiently among both Ad hoc sensor nodes despite their definition being instantaneously challenged by numerous international opponents.

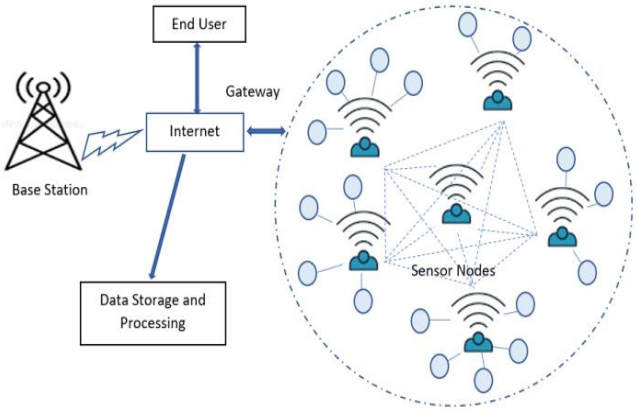

Fig. 1 Typical wireless sensor network structure

Since internet-based multimedia processing technologies have rapidly evolved, so too have data masking techniques for protecting 3D models [11-13]. Integrity identification and copyright protection may be accomplished with the use of data concealing techniques [14,16] by embedding secret data within the original carrier's content. Nevertheless, no alterations to the original carrier are permitted for situations with high data security protocols, such as transmitting medical photographs or certifying documents for use in the court system. Since then, additional people have looked at reversible data hiding (RDH) to see if it has any useful uses [17,18,20]. Difference expansion (DE), histogram shifting (HS), and compression ratio are the three main types of conventional RDH techniques (LC). Methods using differential evolution (DE) to implement RDH embed hidden data into a carrier picture by increasing the dissimilarity between neighbouring pixels [21, 22]. By raising the delta between the actual and anticipated pixel values, prediction error expansion (PEE)[23] is a sort of difference enlargement used for concealment[25-27]. In order to conceal sensitive information, HS-based RDH techniques create a feature histogram from the original picture and insert it into its smallest point. LS-based RDH techniques incorporate hidden data into a compressed region of the carrier image.
As a result, we create a data security paradigm that employs encryption, electronic envelopes, digital certificates, and public key infrastructure to safeguard information throughout its entire lifecycle, from the sensors to the wifi communication to the apps that handle it (PKI). In addition, the model may be applied in sensor networks and other human activities requiring data security for management objectives. It does so without depending on the underlying communications infrastructure. Additionally, it satisfies a distributed system's identification, authorisation, data security, dependability, dependability, non-repudiation, confidence, and confidentiality criteria.

This study introduces an intrusion prevention architecture for WSN-based mobile IoT networks, aiming to extend the network's lifetime through lightweight, secure data routing amongst the network's mobile nodes. Our suggested system uses the uncertainty principle to divide the mobile IoT objects into distinct clusters and pick cluster leaders. In addition, the most recent location of mobile cluster heads is established based on network monitoring and analysis. Furthermore, due to their limitations, most existing solutions cannot easily provide safe and reliable end-to-end data exchanges between mobile IoT gadgets. Compared to existing options, our suggested framework provides an end-to-end safe method that is both efficient and dependable, all thanks to blockchain architecture. Because of this, the proposed architecture enhances mobile IoT devices' routing performance regarding data security and energy consumption. The goal of this paper is to create a framework for a secure sensor network that is decoupled from the underlying communications infrastructure and can be applied to sensor networks in other domains where people engage in activities that necessitate safeguarding collected data for administrative purposes.

The following sections outline the paper's structure. In Part 2, we talk about the problem formulation and background research. The suggested intrusion avoidance system for safe routing in WSN is introduced in Section 3. The standard simulation scenario is outlined in Section 4 and also discusses the performance of the suggested framework. The final section of the research article is the conclusions.

2. Related Works

A number of security concerns have been raised with WSNs, and several models and methods have been proposed to solve them in the existing literature. Sensor network attacks, defences against them, and the way forward are all explored in [28]. With the goal of protecting WSNs from common assaults, Roberto et al. [29] offered a useful solution. It focuses mostly on UWSNs, or unattended WSNs, in which the central authority is not present for extended periods of time. It was proposed by Laurent and Virgil [31] that the key be given out randomly. Two techniques proposed by Song et al. for protecting WSNs from delay attacks are discussed. The Generalised Extreme Studentised Deviate (GESD) method and a present value-based filter are used in [32]; the former is used to identify malicious nodes. Tao et al. [33] describe a solution that prioritises the compromised node and DoS attack using a multi-path random routing technique. In their paper, Xiaojiang et al. [34] offer a method for ensuring the safety of networks of cooperative sensors based on the time-synchronisation of their sensors. Yet, decentralisation might make it challenging for nodes to work together. To create a communication session in the network and to prevent complications caused by the compromised node, the authors of [35] explore secret key-sharing approaches.

Nevertheless, much WSN security research and development is focused on finding and improving viable substitutes for traditional public-key algorithms and PKIs. New research disproves the idea that public key and Diffie-Hellman-based techniques are impractical for use in WSNs. Sensor nodes have been shown to be capable of basic ECC key generation in a feasible timeframe with enhanced performance that can be predicted. In light of this, ECC has emerged as a viable public key cryptographic basis, offering good security for relatively modest key sizes. Both RSA and elliptic curve cryptography (ECC) is viable on 8-bit Processors, as reported by Gura et al. in [36], albeit ECC has been shown to be more efficient. In addition to being more secure, communications encrypted using ECC's 160-bit keys are shorter than those encrypted with RSA's 1024-bit keys when being sent. In particular, Gura et al. [36] show that ECC's point multiplication operations are an order of magnitude quicker than the private-key operations inside RSA and are on par with the RSA public-key operation. Watro et al. [37] demonstrate that the RSA cryptosystem may be partly deployed on real-world wireless sensors, such as the UC Berkeley MICA2 motes. In this case, they used the sensors to handle the public operations while sending the private ones to other machines better suited to heavier computations.

The authors provided a generic architecture in [38]; in this design, the sink node is located in the centre of the surroundings. The remaining sensor nodes are virtually separated into several coronas. In multi-hop transmission, the data packets are sent to the innermost corona, where they are relayed to the sink node. The proposed technique reduced power consumption at the sink node and increased the lifetime of MWSN networks. Still, it did not consider the possibility of data breaches due to hostile threats. To ensure reliability and low power consumption, the developers of [39] designed a novel that includes protective measures for WSNs. The suggested approach has been subjected to both official and unofficial security examinations, and it has been shown to increase network performance when facing hostile attacks. Furthermore, in [41], a lightweight security solution is given employing a one-way hash function, a bitwise exclusive operation, and a physical burning anthracite or bituminous coal function, which enhances data security compared to existing techniques across a range of parameters. However, such systems have not been tested on various network sizes to ascertain the routing price.

We can detect any unusual activity by keeping an eye on the network's nodes. In most cases, the nodes closest to each other are used for the monitoring process. To efficiently create the construction of trustworthy clusters using pre-distributed keys, a safe cluster formation method [45] would be useful. By negative information exchange and independent trust-based decision-making, this method equips a node with the reputation and trust it needs to ascertain whether or not another node has been hacked and take any remedial action that may be required. Even in the presence of cooperating nodes, the information reported is confirmed using a straightforward location verification method based on the received signal strength attribute. Secured routing with intrusion detection has been suggested by Tao Shu et al. [33] using a WSN clustering architecture. To guarantee the safety of the nodes throughout the cluster formation phase, they projected an energy model for nodes, which can be utilised to detect assaults during the election process of the cluster head and then selected for a key management strategy. The flow prediction model also thwarts attacks that leverage the network's routing infrastructure.

With regard to wireless sensor networks, routing methods [47] are crucial. In the event that an adversary obtains the routing protocol algorithm, they will be able to quickly traverse the network and pose risks to all data packets transmitted along the route. Multi-path routing [46] is one solution to thwart these assaults. When the data packets are sent over varying channels over time, it becomes more challenging for an opponent to deduce their order. Simulation results show that, in addition to being random, multi-path routing is also very dispersed and low-power.

Hybrid Encryption Technique (HET) is a novel approach presented by the authors [42] that evaluates the success of two-key and single-key encryption in securing data in sensor networks. The HET method guarantees data

security by maintaining security primitives, including authentication, secrecy, and integrity. There is little time spent decrypting and encrypting with this method, and no data on energy use was available. The authors suggested a new hybrid encoding approach [43] that combines asymmetric and symmetric algorithms to give high levels of security with low key management overhead. A lightweight hybrid cryptographic method (AES and Modified Playfair Cipher, or AMPC) was suggested for WSNs by Anwar and Maha [44]. The first method, Diffie-Hellman, protects the key exchange process. Two cryptographic algorithms modified Playfair and AES, are used to protect data in AMPC's suggested method of increasing WSN security. Even if it's safer now, the electricity usage is pretty considerable. LSA has a finite number of rounds, and each round has its own key to increase security. Therefore the suggested method may transmit data while consuming less power.

3. Materials and Methods

The criteria for sensor network security have been incorporated into the model. The overarching goal of the model is to provide trustworthy information for decision-making while also allowing for the safe identification of communication participants and data transmission. The model relies on the security provided by cryptography, digital envelopes, digital signatures, and public-key infrastructure (PKI) in the context of assaults on sensor networks. With the use of encryption, sensitive information may be changed so that only the intended recipient can decipher it. The concept employs symmetric cryptography for both secret key generation and message encryption. The key is protected via asymmetric encryption and digital certificates issued by a public key infrastructure.

The model employs digital envelope technology to encrypt messages and private keys. This ensures that the message's contents are only accessible to the intended recipient. A digital envelope is created by first encrypting the message's contents with a symmetric algorithm (such as DES, 3-DES, RC2, AES, or a custom algorithm). Once the recipient's public key has been extracted from their digital certificate, it is encrypted using an asymmetric cryptographic technique (such as the RSA (Rivest-Shamir-Adleman) algorithm) to create a secret key. The receiver's private key decrypts the secret key and then uses that key to decrypt the message.

Signing a message with a digital signature involves first reducing the message to a message digest and then encrypting the digest with the private key of the message signatory using an asymmetric cryptographic technique, such as the RSA algorithm. Its digital signature is now an integral element of communication. The recipient is responsible for completing the digital signature verification process. The certificate's function is to forge an association between the public and private keys of an identifiable (notified) entity. To do this, the Certification Authority uses its private key to sign the certificate, making it verifiable by anybody possessing the Certification Authority's public key.

3.1. Attacks in WSN

Attackers can disrupt WSNs in several ways, including introducing their own data bits into the network and re-relaying previously sent packets. An adversary may plant malicious nodes in the network that mimic the functionality of legitimate nodes, or they could intercept and wipe the memory of normally deployed nodes. An attacker's layer of choice determines the kind of network assault they may launch. As each network layer is responsible for a limited set of tasks, attacks are often directed against that layer specifically to prevent it from functioning or degrade its performance. In general, there are two kinds of assaults on WSN layers: those from within the network and those from beyond. Malware like worms and Trojan horse viruses, phishing, and other tactics are commonly used in external assaults to gain access to government and business websites, apps, and security systems in order to steal critical information. When disgruntled workers in a network have access to servers and sensitive information, they are more likely to steal intellectual property. When a current or former worker, advisor, or business associate of an organisation gains access to that company's network, software, or data and wilfully misuses them, or when such knowledge results in misuse, this is known as an internal threat.

3.2. Proposed Structure

The suggested framework is briefly summarised below, and its main components are described in the following sections. The proposed architecture consists of two primary parts: a secure data routing model and an initial network deployment that includes cluster management. In the first step, the basic routing architecture is set up so that each node may keep track of its neighbour in its own internal database. In this stage, we also hope to implement a mobile cluster head system that is both efficient and effective in terms of energy consumption. In addition, a paradigm has been introduced during this stage that keeps the nearly optimum data forwarding channels towards the current locations of mobile cluster heads. Phase 2 concludes by introducing a blockchain-based data security architecture to shield networks from infiltration threats and boost their dependability. Using blockchain technology, data is stored in blocks linked using cryptographic hashes. Each block includes a cryptographic hash of the preceding block, which is encrypted with the data for that block. This kind of technology is useful for keeping tabs on data packets and preserving the safety and integrity of networks. As a result, the suggested framework outperforms the network in various criteria.

3.3. Network Deployment

In its early days, BS could be located by sending out "beacon" signals into the network's background noise. The BS's immediate neighbour then uses this information to update their own routing tables. After that, the source nodes up the ante by sending out an even greater number of packets. Nevertheless, a node may receive the BS detection message from more than one neighbour; in this case, the routing path with the shortest hop count to the BS is

prioritised, and the resulting information is saved in the routing table. Every node creates its forwarding table based on the shortest path in this method. Only nodes with a hop count of 1 towards the BS, as determined by the finalised routing tables, will be able to engage in direct transmission. The voronoi architecture is then used to partition the network field into smaller "cells", and the suggested framework can function. The network field is divided into voronoi cells according to the distance of the sensor network to the calculated mean values. Each sensor node, thus, is associated with the cell whose mean value is closest to its own. With this new architecture, each voronoi cell is treated as a separate cluster. Moreover, a limit is established to determine the movable node, and it is gradually raised until any movable node is located within the perimeter of the voronoi cell. After locating a mobile node, it is promoted to the position of cluster leader. More than one moving node may be discovered inside the specified minimum distance. The proposed framework makes use of the variational principle to find the least-variable relative positions of mobile nodes, as shown in Equation 1.

$$\Delta a \, \Delta q \approx \frac{k}{2} \tag{1}$$

One Δa represents the node's current location, one Δq represents its momentum or speed per unit of time, and one $k$represents the Planck constant. Using the relative location provided by Equation.1, the proposed framework chooses the mobile node as the cluster leader. After mobile nodes are designated as cluster leaders, they will flood the network with data, while regular nodes will modify their routing tables to include the mobile node's unique identifier. The suggested system only updates the routing tables whenever a new mobile cluster head is chosen rather than doing so regularly. The motivation for the proposed platform's employment of base stations as cluster members is the need to speed up communication links and timely data delivery. A decrease in the ratio of power consumption across sensor nodes also improves network security. Algorithm 1 controls Voronoi cells and the identification of roving cluster heads.

The proposed framework uses blockchain technology to securely route data between sensor nodes, mobile cluster heads, and the base station, all while utilising a secure approach to ward off harmful attacks. The hash databases on the mobile cluster nodes may be accessed remotely. Every communication can be audited by utilising the hashes, and all of the hashes may be redirected. There is continuous two-way communication between the sensor nodes and the mobile cluster heads, which then connect to the base station (BS). Private keys are distributed to all the mobile cluster heads so that they may establish encrypted connections to the sensors and BS. Each message has its unique hash, computed similarly to any other function: it takes a value as input and returns another value using the formula in Equation 2.

$$h(z) = k \tag{2}$$

Algorithm 1 selection of moving cluster heads

1. Set of sensor nodes $N_i = \{S_1, S_2 \ldots\ldots\ldots S_n\}$, Cluster head C_h , distance d, threshold t, status
2. message M_i, voronoi cell V_i, routing table R_i
3. For each node n in N_i
4. do
5. if$C_h.d < t$then
6. calculate$\Delta a \, \Delta q \approx \frac{k}{2}$
7. end if
8. End for
9. setC_h
10. End for
11. for each $S_1 \in C$
12. updateM_i
13. For each $N_i \in V_i$
14. do
15. k.response
16. updateR_i
17. End for
18. End for
19. End for

The bitwise XOR operation is chosen as a hash function in the suggested architecture based on its minimal processing needs and computational efficiency. Another reason hash values are used in the proposed framework is because of their irreversible methodology. This method guarantees that identifying the output does not reveal the message's source.

The suggested architecture centres on the BS, whose primary duties are publishing payment systems, analysing sensor data, and issuing activities.

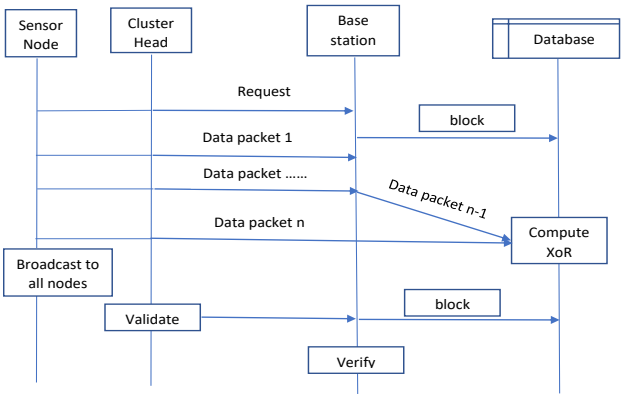

Fig. 2 Proposed data security

Table 1. Simulation setup

Parameter	value
Number of nodes	250
Simulation Area	300 m×300 m
MAC	802.11
Simulation duration	800s
Packet size	64bits
Payload	1024bytes
Deployment	Random

Each data packet's history, including sensor locations and mobile cluster head identifiers, is recorded in the Base Station's immutable databases. A limited number of approved sensor nodes and the BS are the only entities with access to the unchangeable database. On top of that, the mobile cluster heads use the private keys they've already acquired to ensure the integrity of the data packets they're sending out. In Fig. 2, we can see how the proposed security method uses blockchain technology to encrypt the routing data sent between wireless clusters and BS, rendering it traceable and irreversible for harmful threats. In addition, the BS acts as a supervisory body, keeping tabs on the operational state of mobile cluster heads and sensor nodes. As the BS is the ultimate authority in the proposed architecture and controls the routing for the whole network, it may kick any dead sensor node or questionable portable cluster head off the network.

4. Experimental Setup and Simulation Results

In this subsection, we show the mobile IoT-based WSN simulation scenario using the default settings listed in Table 1. As a means of gauging the effectiveness of the proposed framework, a range of experiments are carried out, with network node sizes and data transfer speeds manipulated. Sending speeds are also predetermined, ranging from 2 seconds to 4 seconds per node and 50 to 250 nodes in total.

Network Simulator 2 (NS2) simulations are used to validate the proposed method by comparing the simulated results to those obtained using the established method. The variables taken into account during the simulation are listed in Table 1.

The following criterion is applied to determine the efficacy of the suggested method. These include safety, key expansion time, energy use, and Packet Delivery Ratio (PDR). In this study, we present the mean of 10 simulation findings. The following factors are emphasised in the simulations' performance metrics: One of the most important aspects of protecting online conversations. As soon as security is compromised, the network as a whole is open to attack. Security is a fundamental concern for the many applications of WSNs in the Internet of Things. Network energy consumption refers to the total amount of power the network uses during data transmission, data processing, and reception between sensors and sink nodes. An efficient algorithm will have a low "key generation time," which is the amount of time needed to complete the key expansion procedure. The packet delivery ratio (PDR) is the ratio of transmissions at the sink node or default gateway to the entirety of the packets sent by all nodes. Data collisions, failed intermediary nodes, path-switching orders, heavy data traffic, and intrusion threats are all examples of PDR.

In Figure 3, we can see how the PDR changed during the course of the experiment. When compared to MECA's method (a somewhat recent research effort) and Tang's method (very recent research work), the proposed methodology proves superior. Initially, the provided method achieves a PDR that is comparable to Tang's method, but when the simulation duration is extended, the current method's PDR improves.

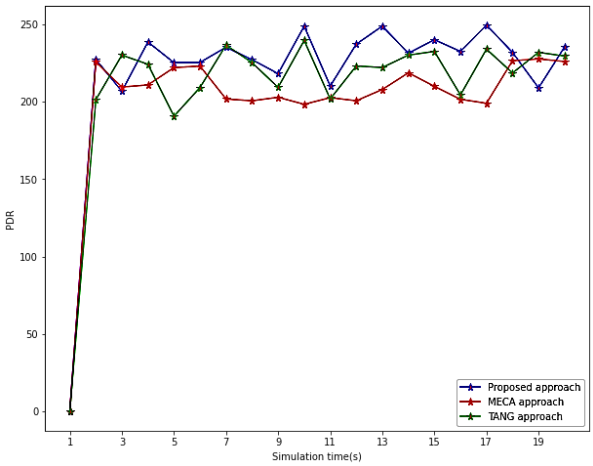

Fig. 3 PDR vs Simulation time

In this part, we compare the efficiency of the proposed framework to that of the existing solutions for various network nodes. Compared to existing methods, the proposed framework extends network lifespan by 25%, 28%, and 32%, as shown in Fig. 4.

In particular, present solutions' performance decreases the network's lifetime by building unstable network areas. As an added downside, the prior systems' routing choices are robust and suboptimal. As a result, the suggested architecture maintains relatively steady performance regarding network lifespan.

This is because we may create energy-efficient pieces using Voronoi cells dispersed throughout the structure. Also, building Voronoi cells may distribute the burden on the individual sensor nodes more evenly. Moreover, the suggested framework records the close relative position of movable cluster heads, which results in minimal communication overheads. The experimental findings show that the suggested framework outperforms competing alternatives in terms of extending the network's lifetime across a wide range of nodes.

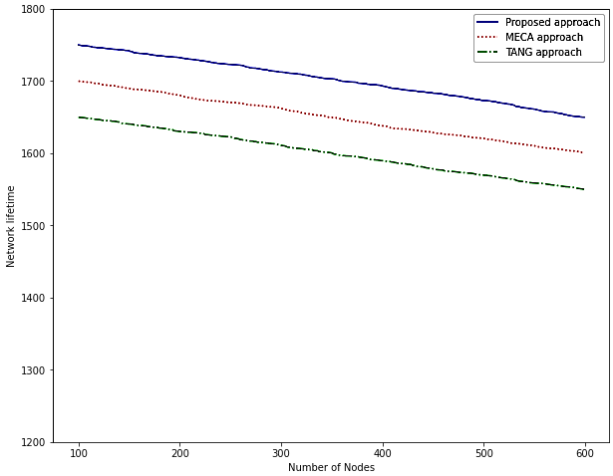

Fig. 4 Number of nodes vs Network lifetime

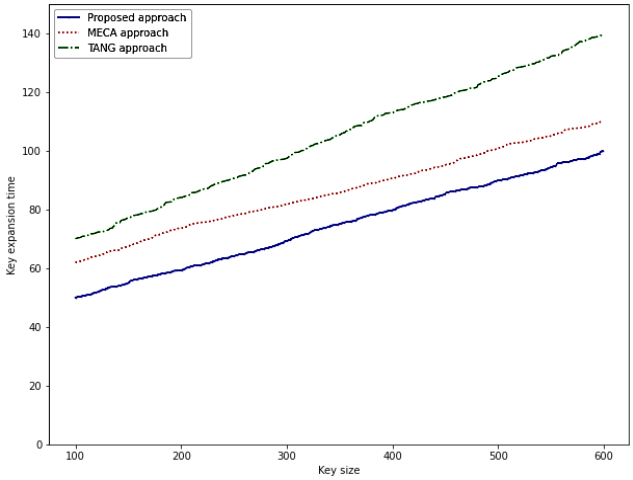

Fig. 5 Key size vs Key expansion time

As shown in Figure 5, the shortest amount of time required by TANG to produce a key is 80 milliseconds when the key length is 10 bits, while the most amount of time required is 150 milliseconds when the key length is 256 bits. Because TANG has a difficult and lengthier key expansion procedure that employs mathematical operations, the time it takes to execute is quite long. The security of the key is in danger if it is compromised in any way. If the execution time is prolonged, the adversary has more time and opportunity to manipulate or change the key and then resend it simply; as a result, the data's security will be compromised. The proposed solution outperforms both TANG and MECA while requiring less effort for essential connection since it was able to break their encryption.

The suggested framework for routing overheads is shown in Figure 6, which compares it to existing solutions under a range of different data transmission rates. According to the findings of the experiments, the newly suggested framework cuts routing overheads by 25%, 27%, and 30% compared to the solutions already in place. In contrast to other solutions, which suffer from high overheads when it comes to re-discovering routes more quickly in the presence of harmful actions, ours doesn't.

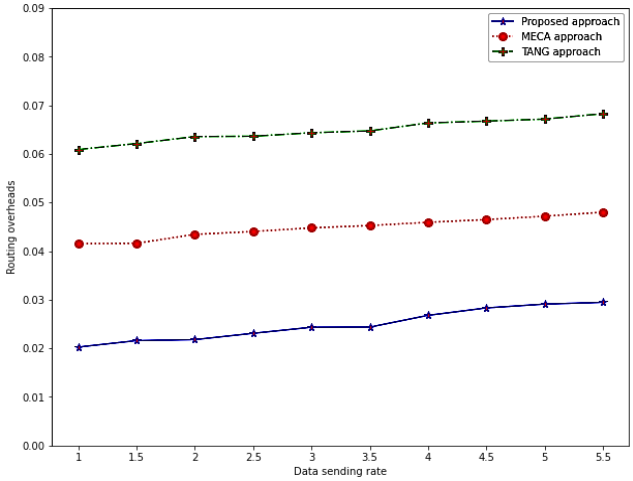

Fig. 6 Routing overheads vs Data sending rate

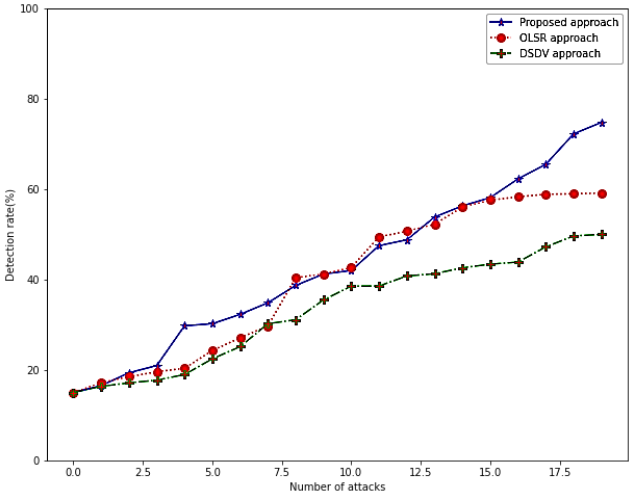

Fig. 7 Number of attacks vs Detection rate

A blockchain-based encryption system that is both lightweight and extremely safe is presented as part of the proposed architecture.

The proportion of wormhole and IP spoofing attacks that are detected is depicted in Fig.7. To listen in on MAC and routing layer data transfer, attackers attempt to breach channels or nodes. The story makes us feel safe in a world where attacks using mobile sensors are on the rise. The attack detection ratio across the sensor monitor nodes of choice is displayed, along with the results for various assaults on network lines and nodes. As an added bonus, it shows the outcomes of routing overhead in network route construction regarding mobility considerations. The suggested secure routing strategy was compared to the currently used protocols by comparing the outcomes of the tests. This shows that even when the network is busy, or nodes are moving randomly, the suggested method can discreetly handle the initial routing burden.

In addition, the currently available solutions have extra routing overheads, which increase when the number of mobile nodes is considerable. Current developments in cryptography and cybersecurity may be broken down into two distinct categories: symmetric and asymmetric. Because of their lesser complexity, symmetric cyphers have shorter key durations than asymmetric algorithms, making them less safe. On the other hand, unilateral cyphers require a higher level of complexity to protect the IoT communication network successfully. But, because of the longer key length, these cyphers are inefficient. After taking into account all of these significant aspects, it is necessary to devise an algorithm that would consume the smallest amount of power, call for the shortest amount of time, start providing the first and most basic level of security to low-end Internet of Things devices, and also reduce the amount of sophistication.

5. Conclusion

This research describes an intrusion prevention architecture based on wireless sensor networks. Its purpose is to ensure safe routing in mobile Internet of Things (IoT)

networks (WSN). The primary objective is to lengthen the network's lifetime while simultaneously increasing data dependability and network security against malicious attacks. The vast majority of energy-efficient systems centre their attention on stationary sensor nodes and utilise the greedy algorithm to route data. Consequently, it is impossible to implement solutions of this kind in dynamic settings. The structure that is being presented is made up of movable cluster heads as well as chunks of the network nodes located in various voronoi cells. In addition, the framework that has been developed places emphasis on the most optimal judgments together with the shortest and most energy-efficient routing chains. The uncertainty principle is used to choose mobile cluster heads that have the fewest fluctuations possible in the momentum they possess. This method reduces the costs of communicating and routing in big networks. In addition, using blockchain technology allows for implementing a lightweight XOR hash function, which enables safe and trustworthy data routing. In a further study, the performance of the suggested framework will be assessed in a hardware environment that is more representative of the actual world.

If a large number of competing nodes are located at various hops in the network, the strategy shown is straightforward and extremely successful. Because a new security codeword is created at each node, the suggested technique becomes more effective, the level of secrecy between the nodes is increased, and it is simpler to identify the competing node inside the network. In addition, the offered method simplifies the underlying mathematics, which, in turn, boosts the PDR by reducing the amount of time wasted waiting.

References

[1] Md. Mokammel Haque et al., "An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks," *KSII Transactions on Internet and Information Systems*, vol. 2, no. 5, pp. 265–279, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[2] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing For Mobile Wireless Ad Hoc Networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175–192, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[3] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Ariadne: A Secure on-Demand Routing Protocol for Ad Hoc Networks," *Wireless Networks*, vol. 11, no. 1– 2, pp. 21–38, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[4] Kun Zhang, Cong Wang, and Cuirong Wang, "A Secure Routing Protocol For Cluster-Based Wireless Sensor Networks Using Group Key Management," *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE*, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[5] Abedelaziz Mohaisen et al., "On the Insecurity of Asymmetric Key-Based Architecture in Wireless Sensor Networks," *KSII Transactions on Internet and Information Systems*, vol. 3, no. 4, pp. 376–384, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[6] Rafik Hamza et al., "A Privacy-Preserving Cryptosystem for IoT Ehealthcare," *Information Sciences*, vol. 527, pp. 493-510, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Jared Cordasco, and Susanne Wetzel, "Cryptographic Versus Trust-Based Methods for MANET Routing Security," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 131–140, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[8] Manik Lal Das, "Two-Factor User Authentication in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp.1086–1090, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Gavaskar, E. Ramaraj, and R. Surendiran, "A Compressed Anti IP Spoofing Mechanism Using Cryptography," *International Journal of Computer Science and Network Security*, vol. 12, no. 11, pp. 137-140, 2012. [Google Scholar] [Publisher Link]

[10] Alexander Becher, Zinaida Benenson, and Maximillian Dornseif, "Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks," *Technical Report*, Springer Berlin, Heidelberg, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[11] Juan Chen et al., "A Lossless Watermarking for 3D STL Model Based on Entity Rearrangement and Bit Mapping," *International Journal of Digital Crime and Forensics*, vol. 9, no. 2, pp. 25–37, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yao-Hsien Huang, and Yuan-Yu Tsai, "A Reversible Data Hiding Scheme for 3D Polygonal Models Based on Histogram Shifting with High Embedding Capacity," *3D Research*, vol. 6, no. 2, pp. 1–12, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[13] IIoan-Catalin Dragoi, and Dinu Coltuc, "Local-Prediction-Based Difference Expansion Reversible Watermarking," *IEEE Transaction on Image Processing*, vol. 23, no. 4, pp. 1779–1790, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[14] Xinpeng Zhang, and Shuozhong Wang, "Fragile Watermarking with Error-Free Restoration Capability," *IEEE Transaction on Multimedia*, vol. 10, no. 8, pp. 1490–1499, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[15] R. Surendiran, and K. Alagarsamy, "Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption," *International Journal of Engineering Trends and Technology*, vol. 4, no. 5, pp.2217-2224, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[16] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Circular Interpretation of Bijective Transformations in Lossless Watermarking for Media Asset Management," *IEEE Transactions on Multimedia*, vol. 5, no. 1, pp. 97–105, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jun Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Transaction on Circuits and Systems*, vol. 13, no. 8, pp. 890–896, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[18] Yongjian Hu et al., "Difference Expansion Based Reversible Data Hiding Using Two Embedding Directions," *IEEE Transaction on Multimedia*, vol. 10, no. 8, pp. 1500– 1512, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kumar Vasantha, and S V P K Satya Devu, "An Efficient and Reliable Data Transfer Protocol in Wireless Sensor Networks," *International Journal of P2P Network Trends and Technology*, vol. 9, no. 2, pp. 10-13, 2019. [Publisher Link]
[20] Ante Poljicak, Lidija Mandic, and Darko Agic, "Discrete Fourier Transform–Based Watermarking Method with an Optimal Implementation Radius," *Journal of Electronic Imaging*, vol. 20, no. 3, 2011. [CrossRef] [Google Scholar] [Publisher Link]
[21] Beijing Chen et al., "Full 4- D Quaternion Discrete Fourier Transform Based Watermarking for Color Images," *Digital Signal Processing*, vol. 28, pp. 106–119, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[22] Bo Ou et al., "Pairwise Prediction-Error Expansion for Efficient Reversible Data Hiding," *IEEE Transactions on Image Processing*, vol. 22, no. 12, pp. 5010–5021, 2013. [CrossRef] [Google Scholar] [Publisher Link]
[23] Xiao Wei Li, and Seok Tae Kim, "Optical 3D Watermark Based Digital Image Watermarking for Telemedicine," *Optics and Lasers in Engineering*, vol. 51, no. 12, pp. 1310–1320, 2013. [CrossRef] [Google Scholar] [Publisher Link]
[24] Blessey.P.M, R.Geetha "Fuzzy Logic Based Technique Using Trust Authentication for a Secure Data Exchange in Wireless Sensor Networks," *International Journal of P2P Network Trends and Technology*, vol. 5, no. 3, pp. 5-11, 2015. [CrossRef] [Publisher Link]
[25] Zhicheng Ni et al., "Reversible Data Hiding," *IEEE Transaction on Circuits Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006. [CrossRef] [Google Scholar] [Publisher Link]
[26] Piyu Tsai, Yu-Chen Hu, and Hsiu-Lien Yeh, "Reversible Image Hiding Scheme Using Predictive Coding And Histogram Shifting," *Signal Processing*, vol. 89, no. 6, pp. 1129–1143, 2009. [CrossRef] [Google Scholar] [Publisher Link]
[27] Ching-Yung Lin, and Shih-Fu Chang, "Semi-Fragile Watermarking for Authenticating JPEG Visual Content," *Proceeding of Electronic Imaging*, vol. 3971, pp. 140–151, 2000. [CrossRef] [Google Scholar] [Publisher Link]
[28] C. Karlof, and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003. [CrossRef] [Google Scholar] [Publisher Link]
[29] Roberto Di Pietro et al., "Data Security in Unattended Wireless Sensor Networks," *IEEE Transactions on Computers*, vol. 58, no. 11, pp. 1500– 1511, 2009. [CrossRef] [Google Scholar] [Publisher Link]
[30] Ch. Mounika, Ch. Suresh Babu, "A Novel Security Based Data Transmission Protocol for Cluster Based Wireless Sensor Networks," *International Journal of Computer & organization Trends*, vol. 6, no. 1, pp. 1-7, 2016. [CrossRef] [Publisher Link]
[31] Laurent Eschenauer, and Virgil D. Gligor, "A Key Management Scheme for Distributed Sensor Networks," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, 2002. [CrossRef] [Google Scholar] [Publisher Link]
[32] Hui Song, Sencun Zhu, and Guohong Cao, "Attack-Resilient Time Synchronization for Wireless Sensor Networks," *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 2005. [CrossRef] [Google Scholar] [Publisher Link]
[33] Tao Shu, Marwan Krunz, and Sisi Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," *IEEE Transactions on Mobile Computing*, Vol. 9, no. 7, pp. 941–954, 2010. [CrossRef] [Google Scholar] [Publisher Link]
[34] Xiaojiang Du et al., "Secure and Efficient Time Synchronization in Heterogeneous Sensor Networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2387–2394, 2008. [CrossRef] [Google Scholar] [Publisher Link]
[35] Wensheng Zhang, Sencun Zhu, and Guohong Cao, "Pre-Distribution and Local Collaboration-Based Group Rekeying for Wireless Sensor Networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1229–1242, 2009. [CrossRef] [Google Scholar] [Publisher Link]
[36] Nils Gura et al., "Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs," *2004 Workshop on Cryptographic Hardware and Embedded Systems*, 2004. [CrossRef] [Google Scholar] [Publisher Link]
[37] Ronald Watro et al., "Tinypk: Securing Sensor Networks with Public Key Technology," *Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN '04)*, ACM Press, pp. 59–64, 2004. [CrossRef] [Google Scholar] [Publisher Link]
[38] Mihaela Cardei, Yinying Yang, and Jie Wu, "Non-Uniform Sensor Deployment in Mobile Wireless Sensor Networks," *International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 1–8, 2008. [CrossRef] [Google Scholar] [Publisher Link]
[39] Yinying Yang, and Mihaela Cardei, "Movement-Assisted Sensor Redeployment Scheme for Network Lifetime Increase," *Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*, 2007. [CrossRef] [Google Scholar] [Publisher Link]
[40] M.Supriya, and Dr.T.Adilakshmi, "Secure Routing using ISMO for Wireless Sensor Networks," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 12, pp. 14-20, 2021. [CrossRef] [Publisher Link]
[41] Amit Dvir et al., "STWSN: A Novel Secure Distributed Transport Protocol for Wireless Sensor Networks," *International Journal of Communication System*, vol. 31, no. 18, p. e3827, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[42] Alakananda Tripathy et al., "Hybrid Cryptography for Data Security in Wireless Sensor Network," *Data Engineering and Intelligent Computing. Advances in Intelligent Systems and Computing*, V. Bhateja, S. C. Satapathy, C. M. TraviesoGonzález, V. N. M. Aradhya, Eds., Springer, Singapore, vol. 1407, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[43] L. Sachin, S. Bhushan, and Surender, "Hybrid Encryption Algorithm to Detect Clone Node Attack in Wireless Sensor Network," *Proceedings of the International Conference on Innovative Computing & Communications*, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[44] Md. Navid Bin Anwar, and Maherin Mizan Maha, "AMPC: A Lightweight Hybrid Cryptographic Algorithm for Wireless Sensor Networks," *International Journal of Innovative Science and Research Technology*, vol. 5, no. 6, pp. 1142-1146, 2020. [Google Scholar] [Publisher Link]
[45] Xiao Zhenghong, and Chen Zhigang, "A Secure Routing Protocol with Intrusion Detection for Clustering Wireless Sensor Networks," *International Forum on Information Technology and Applications*, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[46] Ali Modirkhazeni, NorafidaIthnin, and Othman Ibrahim, "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis," *Second International Conference on Network Applications, Protocols and Services*, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[47] Shanshan Chen, Geng Yang, and Shengshou Chen, "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks," *International Conference on Communications and Mobile Computing*, 2010. [CrossRef] [Google Scholar] [Publisher Link]