Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NODE AUDITOR BASED TRUSTED ROUTE SELECTION WITH NODE AUTHENTICATION USING MULTI KEY DISTRIBUTION MODEL FOR SECURE DATA TRANSMISSION

ORCHU ARUNA[1], MIDHUNCHAKKARAVARTHY[2]

[1]PDF Scholar, Computer Science and Engineering, Lincoln University College Main Campus, Wisma Lincoln, 12-18, Jalan SS 6/12, 47301 Petaling Jaya, Selangor, Malaysia.

[2]Faculty of Computer Science and Multimedia, Lincoln University College Main Campus, Wisma Lincoln, 12-18, Jalan SS 6/12, 47301 Petaling Jaya, Selangor, Malaysia.

E-mail: [1]oaruna.pdf@lincoln.edu.my [2] midhun@lincoln.edu.my

ABSTRACT

Wireless Sensor Network (WSN) is an advanced and difficult-to-implement system that makes minimal use of computer resources. Security is a major concern in the WSN. It is susceptible to attacks and data packet loss because to its wireless nature. Avoiding such issues necessitates the use of secure routing. Routing is a crucial WSN technique for ensuring the safety of the network by distributing data to other nodes. The predicted trust value is used by the routing process's trust algorithm to either exclude or include nodes. Multiple secure communication protocols have been developed and deployed in WSNs to guarantee the confidentiality, integrity, and availability of the data and nodes involved. The importance of trusted communication in WSNs applications is growing in order to ensure their widespread adoption. A WSN platform needs a TMS in order to set up a trustworthy connection. This study suggests a different way to do secure sensor communication, building on ideas put forward by the secure Computing Group. This model suggests a secure routing protocol that takes trust into account in order to safeguard wireless sensor networks from different types of threats. Using a cryptographic architecture for node authentication, this study chooses an Auditor node to carry out route selection in the WSN. To prevent attacks such as black holes, selective forwarding, wormholes, hello floods, and sinkholes, nodes must first calculate the overall trust values of their neighbors by combining the direct and indirect trust values, as well as the volatilizing factor and residual energy. Sending a routing request message to neighbors in multi-path mode is the initial step for a source node to transfer data to a sink node. The batteries used to power WSN nodes have a very short lifespan of only a few days. As a rule, sensor nodes are deployed in convoluted places, making it difficult to access them for battery maintenance or recharging. As a result, employing the elaborate procedure for securing data is not recommended. In this research, Node Auditor based Trusted Route Selection with Node Authentication using Multi Key Distribution (NAbTRS-NA-MKD) Model is proposed for secure data transmission in WSN. The proposed model when compared with the traditional methods exhibits 98.8% accuracy in trust factor calculation and trusted route selection.

Keywords: *Wireless Sensor Networks, Routing, Auditor Node, Trusted Node, Node Authentication, Multikey Distribution, Secure Data Transmission.*

1. INTRODUCTION

One type of network that allows for wireless communication between sensor nodes is known as a WSN [1]. The enormous wide spread use of WSNs applications in modern living is significantly due to the advancements in sensor, low power processor, and wireless communication technologies. Several pervasive convergence applications and services, such as environmental monitoring, disaster handling, and traffic control, are examples of such applications [2]. Future WSN applications are driven by a desire for low-cost solutions that do not require wires [3]. The security of these applications must be carefully considered, particularly with relation to authentication of nodes, data integrity, and confidentiality. Unattended sensor nodes are a

common entry point for hackers [4]. When sensor nodes include cryptographic materials like keys and other crucial data, the situation becomes critical [5]. Further rendering the sensor nodes untrustworthy, attackers can insert dummy nodes that mimic the existing network nodes.

Extensive research on two approaches to ensure the validity of network nodes provides more proof of the need of trustworthy communication between nodes in the network. Nodes in WSNs often use trust management as a strategy to cope with the unpredictability of participant actions in the future [6]. By analyzing the actions of the nodes in the network over a given time frame, it finds the trust value. When enough time has elapsed, however, trust management will be able to identify counterfeit nodes. Thus, it is possible that harmful nodes were already present in the network and were causing disruptions prior to the identification of trustworthy nodes. In addition, sensor nodes incur indirect costs, such as increased processing power, memory requirements, and network connectivity, due to the mathematical basis of the trust node detection paradigm [7].

1.1 Trust Management

In order to guarantee that a node is trustworthy, it is essential to establish trust amongst them. Users can't trust a node until it can detect its surroundings and send data to its destination without compromising the security or privacy of that data. The network's performance can be negatively impacted by the limitations imposed by the various approaches used to find the trust node and identify malicious nodes. A node's credibility and actions dictate its trustworthiness in a trust-based system [8]. The system classifies nodes as benign if their values are greater than a particular threshold and as malicious if their values are lower than that threshold [9]. In order to identify malevolent nodes in WSN, a cryptographic method is employed, which provides a solid framework for node analysis. Common security measures used to ward off malicious nodes' routing assaults include authentication and encryption. The converse is true for internal routing attacks; an attacker already has all the credentials they need to succeed [10]. On top of that, these gadgets require complex computations, which use more power. Security solutions based on trust-awareness have so been proposed as a solution to the problems with encryption and authentication-based methodologies.

When it comes to protecting WSNs from attacks that aim at specific nodes, trust-based approaches clearly shine [11]. One new way to secure WSN routing is via a trust-based strategy, which uses observed node behavior to forecast what the nodes will do next and then figures out what to do effectively when a node acts suspiciously. Nevertheless, traditional trust-aware routing protocols do have several drawbacks, such as a high energy consumption and a lack of attack types that can be protected against [12]. Data forwarding might not work well for paths where the value is determined by the number of hops, even though more hops mean a higher comprehensive trust value. The perpetrator may meddle with machinery or spy on conversations. Additionally, attackers can alter transmitted data or link them to the network if illicit devices are placed in the physical surroundings [14]. For security considerations, it is important that messages sent and received by nodes in a WSN be encrypted. The network must also retain a key that may be used for decryption. Therefore, key management is crucial for WSN security. For safe and effective data transfer in WSN, particularly in resource-constrained settings, obtaining such a key arrangement is essential [15]. Problems with computational complexity, plaintext assaults, brute force attacks, and side-channel attacks are only a few of the security vulnerabilities plaguing current algorithms [16]. Improved safe and energy-efficient data transmission in WSNs can be achieved using the practical and efficient technology of clustering in conjunction with cryptography.

Some of the qualities that make WSNs susceptible to several kinds of attacks include open media, numerous important applications, and open and hostile surroundings. Traditional security measures, such as authentication and encryption, are inadequate against composed node assaults due to their complexity. The entire WSN may be disabled or taken over if one infiltrating node responded to orders from outside sources by launching assaults. Malicious nodes can influence the efficiency of the routing protocol in a number of ways. One is by tricking other nodes into sending data to them; after they have received some data, they can either delete it all or pick at random. The most effective strategy for dealing with these nodes is to be vigilant and detect them. Due to the lack of a centralized authority, nodes in WSNs should spread monitoring and threat detection. One of the new aspects of secure WSNs is routing. Because it is responsible for transmitting data to the base station, the routing

Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protocol is a crucial component of WSNs. This highlights the importance of secure routing, which can resist deliberate packet drops, modifications, and interruptions to routing processes. Many solutions have been proposed for the problem of routing security, especially when dealing with compromised nodes. One of these solutions is trust establishment, which is used in many different areas of study. Establishing trust allows one to distinguish between trustworthy and untrustworthy nodes by looking at their previous actions and outcomes. During routing operations, it stays away from unreliable nodes and chooses only reliable ones. Research into ways to strengthen network security and cooperation has been extensive due to the trust mechanism's simplicity and efficiency in detecting compromised nodes.Figure 1 displays the model of the WSN network.

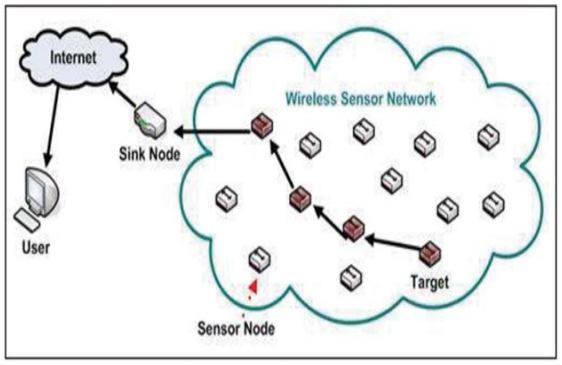

Fig 1: Wsn Network Model

While many different approaches have been considered by computer professionals to ensure the safety of data transport, data encryption has proven to be the most popular and effective solution. Encryption works by encoding the data in a way that only the intended recipients can decipher. Encrypting data means changing it into a format that can only be viewed by authorized individuals who have the decryption key. The term cipher text describes the transformed form of data from plaintext before encryption [17]. The objective of data encryption is to secure sensitive information during storage or transmission between systems. An important part of keeping data and data centers safe is the use of advanced encryption algorithms, which have begun to replace or modify conventional encryption standards [18].

1.2 Security using Cryptography

Advanced encryption algorithms ensure confidentiality by transmitting data correctly, verifying its authenticity, and maintaining its integrity [19]. Data providers can be easily identified and verified through authentication; data accuracy can be guaranteed through integrity; and data transmission cannot be interrupted by the sender thanks to non-cancellation. An early method of data encryption involved changing specific letters inside a sentence. The entire sentence became unintelligible as the meaning of the deformed characters required some time to decipher. The decryption key, which allows the receiver to view communications, is only accessible to that party [21]. As deciphering codes became easier, more complex encryption methods were required to keep messages secret. In Figure 2, the WSN model routing was executed.

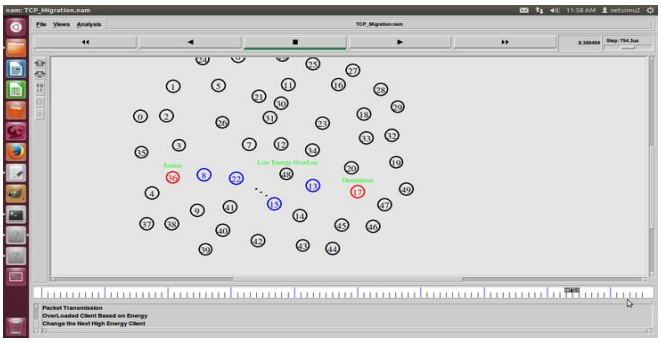

Fig 2: Wsn Routing

Cryptography algorithms can be broadly classified into two categories: symmetric and asymmetric. Both encrypt data, but one employs asymmetric keys and the other an asymmetric one. In symmetric-key cryptography [22], one key is utilized for both encoding and decoding, while in asymmetric-key cryptography [22], two keys are utilized for each operation. Advantages and disadvantages are specific to each approach. The symmetric key approach has several advantages and is quick to deploy. While symmetric encryption is efficient and inexpensive, it is less secure than alternative techniques due to its reliance on a single safe key [23]. However, the increased security provided by asymmetric algorithms comes at the cost of increased complexity and latency [24]. As an alternative to traditional symmetric key encryption, asymmetric key cryptography (also known as public-key cryptography) employs separate keys for encrypting and decrypting data. In Figure 3, asymmetric cryptography model is depicted.

The process of encrypting and decrypting data using a pair of keys is called asymmetric encryption or public-key cryptography. A public key is one half of a key pair; the other half is private and should be kept hidden. Anyone can use the public key. To encrypt data via asymmetric encryption, the sender utilizes the public key of the recipient. After that, the receiver can decode the data using their private key. Two parties can communicate securely using this method even if they don't have the same secret key. In comparison to symmetric encryption, which reuses the key for decryption and encryption, asymmetric encryption offers a number of benefits. Removing the need to exchange secret keys is a major perk, especially when dealing with numerous parties at once; doing so may be a real pain. Digital signatures, which can be generated via asymmetric encryption, can also be utilized to confirm the legitimacy of material. Many applications rely on asymmetric encryption, such as digital signatures, safe data transfer, and online communication.

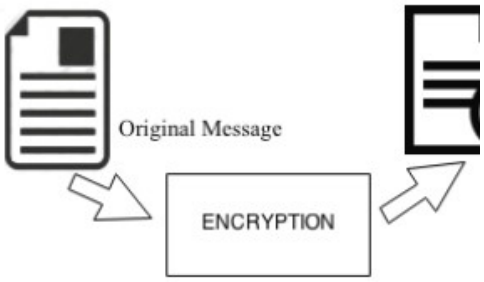

Fig 3: Asymmetric Model

Finding an appropriate cryptographic mechanism in WSN is challenging because of the low processing power, energy, and storage resources of the sensor nodes [25]. Cryptography is the practice of encoding and decrypting data in a way that not even a highly trained criminal can decipher it, protecting sensitive information from prying eyes. Taking into account only trusted nodes in the network, this research aims to develop an efficient algorithm for Secure Data Communication in WSNs [26]. This method needs to be able to make the most of the limited resources of the sensor nodes while yet ensuring the privacy and integrity of the data collected [27]. An integral aspect of WSN security architecture is the use of cryptographic algorithms, which help to prevent the threats mentioned above and ensure the security of data in WSNs [28]. In order to prevent unauthorized parties from reading the plaintext data packets as they travel over the network, cryptography techniques encrypt them into more secure packets of coded words. Encrypted data, when transmitted over a network that uses a layered model, consists of a series of additional bits added to the data bits with the purpose of protecting the original data from attackers. This ensures that the data remains secure and is compatible with existing protocols. When it comes to network security, the most fundamental needs are secrecy and integrity, which are addressed by cryptography systems.

To prevent security risks including eavesdropping, message replay, and message fabrication, several safety procedures have been suggested, including authentication, secrecy, and message integrity. Although these methods perform well against external attacks, they are not strong enough to protect networks against insider threats. This is due to the fact that malicious sensor nodes can impersonate genuine nodes in the network by acquiring all the necessary cryptographic keys. Thus, these cryptographic safety methods necessitate a strong and protected key exchange system. Any following safeguards will be useless if a compromised node or nodes are able to communicate with each other before a successful key exchange. Verifying the trustworthiness of all interacting nodes is essential for establishing safe communications and ensuring secure key exchange. This demonstrates how important it is for two communicating nodes to build confidence with one another. This study proposes a model for secure data transmission in WSN that uses Node Auditor based Trusted Route Selection with Node Authentication utilizing Multi Key Distribution (NAbTRS-NA-MKD). The applications of WSN is shown in Figure 4.

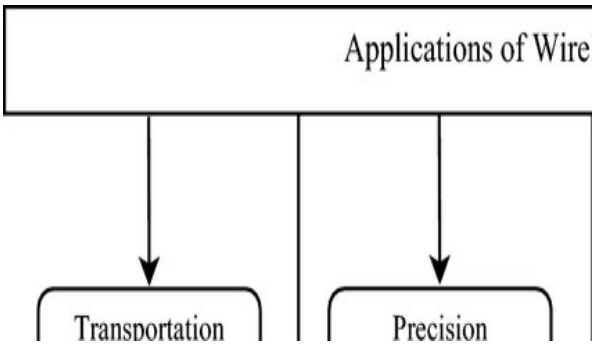

Fig 4: Applications of WSN

This research article discusses about the trust management in the networks for detection of secured and trusted route. The use of cryptography in networks is also discussed in the introduction section 1. The section 2 discuss about the literature

survey. The traidtional models are clearly discussed in this section. The section 3 discuss about the proposed model. The trust factor calculation, key generation and distribution and authentication is briefly explained. The section 4 provides the results. The comparison graphs of the proposed model with the traditional models are included in revised paper. The section 5 concludes the reseach article.

2. LITERATURE SURVEY

Due to its resemblance to conventional computer networks, WSNs need special attention when planning their infrastructure in terms of security features such as privacy, authenticity, and resilience. While many security protocols have been refined for use in wired networks, not all of them are directly applicable to WSNs. Research on curve-based encryption algorithms has disproved the long-held belief that public-key cryptography requires too many resources for WSNs, demonstrating the technique's practicality in this setting. Among the current security protection solutions for WMSN, cryptography is an effective technology that could provide authenticity, confidentiality, and integrity to sensed data and sensor nodes. The field of cryptography encompasses a wide range of techniques for encoding sensitive data such that it can only be read by the intended receiver. Cryptography often employs security keys for data encryption; this provides some leeway in the encryption and decryption process but introduces additional challenges with administration. Choosing the best algorithm is a crucial design decision that can impact the algorithm's performance in terms of memory and processing costs as well as resistance to attacks. This is because cryptography makes use of a broad array of mathematical algorithms and approaches.

The integrity and availability of the network could be jeopardized in the event of a data breach. Key management, authentication, and trust management in WSNs are some of the current research hotspots. It is challenging to choose the most appropriate key management or trust management scheme for a given WSN application due to the abundance of protection systems offered by researchers. In our research, we thoroughly examined the ways in which different trust management, authentication, and key management techniques might be applied for certain purposes.

Wireless sensor networks are susceptible to a variety of security threats due to their restricted resources and poor processing power. Due to their resource-constrained nature, conventional security techniques need an excessive amount of resources, which prevents WSNs from reliably operating. Furthermore, WSNs necessitate guaranteed Quality of Service (QoS) due to multihop communication. Hence, it is crucial to design WSNs with security in mind while simultaneously preserving QoS and energy economy. Improving WSN performance requires fixing the energy-hole issue that causes them to cover too small of an area. Inadequate deployment tactics lead to the creation of an energy-hole problem. A novel technique called lightweight secure routing (LSR) was introduced to manage WSNs in this study by Pathak et al. [1]. The algorithm directly tackles the multi objective WSN optimization problem. In order to solve the multi-objective WSN optimization problem, the LSR algorithm employs Ant Colony Optimization (ACO), an adaptive security model that relies on direct and indirect trust calculations, an adaptive quality-of-service model, a hybrid deployment model that combines 2-D Gaussian and uniform distributions, and an adaptive connectivity model that measures the communicational radius to guarantee high connectivity between sensor nodes.

In software-defined wireless sensor networks, malicious sensor nodes can cause problems by randomly doing things like flooding or deleting messages. Negligible network availability can be caused by malicious nodes due to in-band communications and the absence of secure channels in software defined WSNs. In order to detect internal threats and promote node collaboration and decision-making during forwarding, Bin-Yahya et al. [2] developed a hierarchical trust management technique for SDWSNs. This model can identify potentially harmful activity and assess the reliability of the nodes involved at multiple stages of the SDWSN design. The author developed computational models that are sensitive to trust in order to detect multiple malicious attacks. In order to enhance detection performance when attacks target the key traffic on the control plane, the author also proposed separate trust ratings and characteristics for control and data traffic. The author also constructed an acknowledgment-based trust recording approach using some built-in SDN control messages. To guarantee trustworthy and long-lasting trust scores, the author established a reliability trust metric and employed a weighted averaging method.

At the moment, energy efficiency, quality of service, or security are the three main goals of most WSN routing systems. Still, a broader view of WSNs is required since many uses call for guarantees of security and quality of service in addition to the need to prolong the network's lifetime. Because of their limited power capacity, sensor nodes have to choose between maximizing network lifetime, service quality, or security. To overcome these challenges, Rathee et al. [3] introduced an ant colony optimization-based QEBSR algorithm for WSNs. New and improved techniques for calculating the end-to-end transmission delay and the trust factor of routing path nodes are presented. Energy efficient routing with node compromised resistance and distributed energy balanced routing are two previously published methods that are compared to the proposed one.

Because of their layout's openness, WSNs are susceptible to attacks. The wormhole assault is among the most dangerous types of attacks. Because it breaks WSNs during data transfer and generates erroneous routing by private tunnels, the wormhole attack is difficult to detect. So, Teng et al. [4] suggested a detection technique that incorporates the node trust optimization model (NTOM-DA) to counteract wormholes in WSNs, making networks more resilient to attacks and enhancing overall performance. To begin, every node with a neighbor count higher than the threshold is flagged as suspicious; subsequently, the exclusive neighbors of these nodes engage in communication with one another. Choose to test the path whose hops are greater than the wormhole threshold. To determine the trustworthiness of nodes and paths, it is necessary to set up a trust model.

The Internet of Things makes it possible for a wide variety of physical items to establish connections to the web. By facilitating data exchange via a number of new technologies, this connectedness is important in making intelligent identification a reality. With their central role in the Internet of Things (IoT), WSNs have found applications in many domains, including smart transportation and smart healthcare, as examined by Saleem et al. [5]. Researchers have taken data security concerns, such as the potential disclosure of sensitive information, very seriously in light of the fast expansion of WSNs and WMSNs, among others. Many of the authentication mechanisms for WMSNs that have been developed recently by researchers suffer from significant security vulnerabilities. According to their research, their suggested protocol may protect sensor nodes against impersonation attacks and also provides users with anonymity.

As a hot topic in the IoT, WSN data transfer is currently everywhere. A number of multifactor authentication solutions have been proposed as a means to reduce the security vulnerabilities associated with wireless channels, which are well acknowledged. Wu et al. [6] suggested a novel three-factor authentication technique to meet these challenges; it provides session keys for WSNs. The formal verification by Proverif indicates that the security aspects of the new system are intact. Based on the informal analysis, the proposed strategy is both feasible and fulfills general demands. Countering different types of attacks and offering security features are among these needs. The proposed method surpasses previous comparable ideas put up recently in terms of both security and practicality.

As 5G approaches commercialization, it is being considered as a possible communication network for the IoT, with the substantial role that WSNs have played in the IoT. While 5G and WSNs together can increase the IoT reach and the variety of services it can provide, they also introduce new security concerns. User authentication and key agreement are essential for end-to-end communication security from this perspective. With the proliferation of Internet of Things (IoT) devices, such as sensors, comes the need for anonymous authentication and authorization in order to protect users' privacy and stop unauthorized parties from accessing their sensitive data. The study by Oladipupo et al. [7] offered a system design that considered the integration of WSNs and 5G for the Internet of Things. The author suggests a method for 5G-integrated IoT WSNs to use ECC for authentication, authorization, and key agreement; this method is based on cryptanalysis of existing schemes and standards.

For distributed nodes that function in a distributed manner and make professional use of the transmission lines, Awan et al. [11] develop a routing approach that combines IoT with Blockchain (BC). The offered protocol uses smart contracts in diverse IoT settings to locate BS. Assuring routes from IoT nodes to sink and BS might be done by every node, enabling IoT devices to work together during transmission. Reducing

energy consumption and improving network life, the offered routing protocol gets rid of redundant data and attacks on IoT networks. The independence and safety of an IoT network can be guaranteed by a decentralized technique that is introduced by Sanchez et al. [12]. The proposed method aids in safeguarding the accessibility and authenticity of data pertaining to the security advantages of BC and the application of cryptographic instruments. An IoT-related WSN that senses temperature and humidity has been used to assess the accuracy of the provided technique. The results show that the concept meets the main requirements of an IoT network. It can function independently, transmit data securely between users and devices, protect user privacy, reliably store data, and make data accessible in the infrastructure.

According to [13], a novel approach to trust-aware localized routing and class-related dynamic encryption was proposed. The method first determines the path to the destination and transmits the data packets along that path. It is possible to quantify the worth of trustworthy data forwarding support (TDFS) by determining the values of these variables. Protocols for low-energy adaptive clustering hierarchy (DDR-LEACH) based on distance, degrees, and residual energy were modeled by Amjad et al. [14]. Using DDR-LEACH, the ordinary node can take the place of CHs in relation to the maximum RE, degree, and minimum distance from BS. Not to mention how costly it may be to store a large volume of data in BC. To address this issue, one can utilize an interplanetary file system (IPFS), an external data storage system. Additionally, AES 128-bit was used to secure IPFS data, which is better than the current techniques of encryption.

Referenced in [15] is an approach that is effective for real-time service-centric feature-sensitivity-analysis (RSFSA). Different features accessible through any service are subject to multi-level sensitivity analysis by the RSFSA algorithm. At each step, the method checks whether the feature set has been accessed and how many features the user has allowed access to in order to calculate the FLAG value for the user based on the provided profile. Users' access to the service is granted or prohibited based on the value of FLAG. The solution alternately handles multiple encryption algorithms and keys for each feature level. With the help of artificial intelligence, Elhoseny et al. [16] want to create an IoT solution that uses BC to transfer massive data while preserving user privacy. The first step of the given approach is to use graph-modeling to develop a trustworthy and extensible data collection and transmission system. After that, BC-based communication sources could benefit from authentic and private exchanges thanks to symmetric-related digital certificates.

3. PROPOSED MODEL

It is possible to classify WSN security techniques into three interconnected stages. To ensure the sensor node's integrity and the network's original creator can guarantee it, the first step is to secure the platform or node itself. The next major step is to secure the wireless medium or the network infrastructure so that trustworthy, dependable, and secure communication can take place [29]. Given that anyone can intercept data sent via wireless communication, the last step is to ensure that the data remains private and uncompromised. Security in wireless sensor networks is therefore paramount for the sensor node, the network infrastructure, and the data. For a reliable wireless sensor architecture to be built, this was an essential prerequisite. Secure routing collaboration is based on nodes' trust values; so, a node with a higher value is more likely to be chosen as the routing path's relay node. The comprehensive trust value is determined by adding a node's direct and indirect trust values as well as its residual energy and volatility factors. If the result falls below a certain level, the node is deemed untrustworthy.

Numerous wireless sensor network applications are vulnerable to the loss of important, private, and sensitive data due to inadequate security mechanisms. An information security breach could lead to irretrievable data loss in the worst-case situation. Additionally, unreliable security measures can lead to costly recovery costs, user distrust, and even dangerous network and server congestion. The development of a secure solution presents WSN with a number of challenges. The fundamentals of security standards, hazards, energy efficiency, and cryptographic and clustering-based security solutions are analyzed for sensor networks. In actual implementation scenarios, node failures can also occur at random. Conventional safety methods in WSNs are not practical because of the limited resources in the sensor nodes. These techniques have considerable computing and communication overhead. This makes the development and deployment of WSNs that are both secure and efficient with energy a particularly daunting undertaking. Using the idea of hybrid

cryptography and clustering based routing, a methodology is created to improve energy economy and data security in WSNs [30].

Cryptography is one of the several WSN security mechanisms that has the potential to ensure the confidentiality, authenticity, and integrity of the data detected and the sensor nodes themselves. Simply said, cryptography is the practice of encoding data in a way that only the intended receiver can decode, therefore preventing unauthorized parties from gaining access to the data. There are new issues with key management brought up by security keys, even though they make cryptography more versatile in its encryption and decoding procedures. Algorithm performance in terms of memory costs, processing power, and attack resistance can vary greatly depending on the mathematical formula and approach used to generate the algorithm. Accordingly, selecting the most appropriate algorithms is a crucial design decision in cryptography.

In WSN, sensor nodes often encounter constraints in resources such as processor speed, memory, sensing capabilities, and energy supply. Although more robust sensor nodes have joined the IoT with novel, low-cost technology, numerous contemporary wireless multimedia sensor networks are likely to encounter constraints that limit the application of cryptographic methods. Research in this area has mostly concentrated on different conceptual levels of ideal cryptographic algorithms for multimodal sensing up to now. There is a wealth of literature detailing the specific requirements for media coding methods in terms of compression and encryption, and many publications have proposed solutions that do just that. There are a number of proposed ways for encrypting multimedia data, with efficiency being a primary consideration for wireless multimedia sensor networks employing cryptography. Fixing WSNs primarily involves addressing their coverage and deployment, scalability, quality-of-service, size, computational power, energy efficiency, and security. Security is one of the major challenges faced by wireless sensor networks.

Wireless networks are often more vulnerable to a range of security threats due to the fact that unguided transmission media is more susceptible to security attacks compared to guided transmission medium. More and more, data must be securely transmitted via an unstable medium. Secure routing, privacy protection, energy efficiency, resistance to node capture, and robustness against communication denial of service attacks are some of the several components that make up WSN security. Key management also assists with secrecy and authentication. This challenge calls for an improvement in the efficiency of existing cryptographic algorithms. Since cryptographic algorithms are fundamental to the security architecture of WSNs, it is highly recommended to use the most efficient and appropriately safe algorithm in order to save resources. In order to optimize execution time, data storage, and energy usage, a cryptographic approach is employed.

Many academics have developed different WSN models in an effort to protect the communication of WSNs and guarantee their durability. One of the best ways to make WSNs last longer is to group similar wireless sensors together; this lessens the strain on individual nodes and, in turn, their power consumption. It has not been thoroughly investigated, however, if multicore sensors combined with sensor clustering significantly reduce the sensors' power consumption. It was shown that the model had been security-analyzed and that it had been performance-compared to other models. The proposed model is secure and able to withstand several types of attacks, according to the results of the security analysis. Figure 5 displays the proposed model framework.

Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

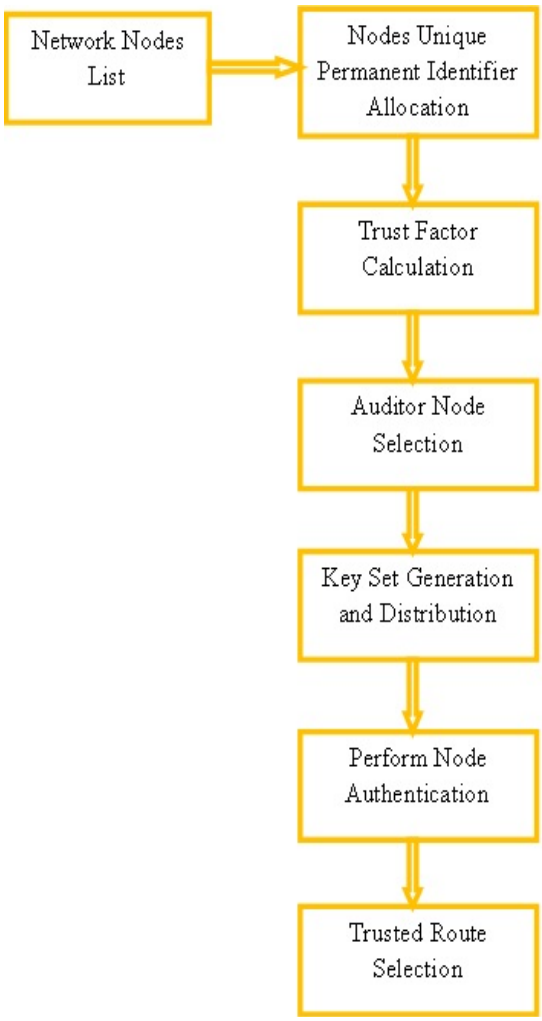

Fig 5: Proposed Model Framework

In addition to being able to handle data that is both recent and scalable, the model that is being projected is also energy efficient. This study suggests a method for secure data transmission in WSNs called Node Auditor based Trusted Route Selection with Node Authentication utilizing Multi Key Distribution Model.

Pseudo Code: NAbTRS-NA-MKD

For each node n in NNlist
addr←getnodeaddr(n)+range(n)
ID←addr(n)+PDR(n)+max(range(n)
ener←allocener(n)-remainingener(n)
end For
For each node n in Nnlist
If (max(ener(n)))
If(max(PDR(n)))
Trustfacor←setVal(n)

$$Rval \leftarrow getVal(n)$$
$$Mval \leftarrow geteven(n)$$
$$Lval \leftarrow getPrime(n)$$
$$KeyU = Rval \;\&\&\; Mval \oplus Lval$$
$$KeyR = KeyU \oplus Mval$$
$$KeyU = Rval \;\&\&\; Mval \oplus Lval$$
$$KeyR = KeyU \oplus Mval$$
$$KeyS = \sum_{n=1}^{M} KeyR(n) \oplus \frac{\text{KeyU}}{\text{Rval}}$$
$$KeyD = \sum_{n=1}^{M} KeyS(n) \oplus \text{Lval(n)} \&\& Rval(\text{n}) \ll 2$$
$$KeySet[M] = \sum_{n=1}^{M} \{KeyS(n) : KeyD(n)$$

For each node n in Nnlist
Troute←getstatus(KeySet(n))+max(PDR(n))+UPI(n)

Algorithm NAbTRS-NA-MKD
{
Input: Network Nodes List{NN_{List}}
Output: Trusted Nodes List in Route {TN_{List}}
Step-1: The nodes that enters into the network or nodes forming the network will be registered with the network and each node will be allocated with a unique permanent identifier that is used for node identification. The node registration and the unique permanent identifier allocation is performed as

$$NReg[M] = \sum_{n=1}^{M} getnodeattr(n) + nodephyaddr(n) + \mu(n)$$
$$UPI[M] = \sum_{n=1}^{M} \frac{get\ NReg(n) + \max(\mu(n, n+1)) + \max\ (PDR(n))}{M} + Th$$

Here μ is used to consider the node communication range. PDR is the packet delivery rate of node n and Th is the threshold value.
Step-2: The proposed model that is allocated with a unique permanent identifier undergo trust calculation. The node transmission rate, energy consumption, delay levels and computational capabilities are considered in trust factor calculation. The trust factor calculation is performed as

$$PDR[M] = \sum_{n=1}^{M} \frac{\delta(n) - \lambda(n)}{T}$$

$$Ener[M] = \sum_{n=1}^{M} \tau(n) - \beta(n)$$

$$Tfactor[M] = \sum_{n=1}^{M} \frac{\text{getUPI(n)} + \max\ (PDR(}{T}$$

$$+ \min\ (Ener(n,n+1)) \begin{cases} Tfa \\ Tfa \end{cases}$$

Here δ is the model that considers the packets sent, λ is the packets received and T is the total packets generated. τ is the allocated energy to a node and β is the consumed energy. eTh is the energy threshold value.

Step-3: The trusted nodes only will be involved in the routing process and only these nodes can transmit the data in the network. The node that is having maximum computational capabilities, less energy consumption and high data transmission rate with less delay is considered as auditor node that is used to monitor the entire network. The auditor node selection process is performed as

$$AuditorNode[M] = \sum_{n=1}^{M} getUPI(n) + getaddr($$

$$+ \max\ (Tfactor(n,n+1)) \begin{cases} \leftarrow \\ continue \end{cases}$$

Here TTh is the trusted threshold value. A node having maximum capabilities will be considered as auditor node.

Step-4: The proposed model generates the keys set for node authentication and also for involving in data transmission process. The key set contains a pair of keys where one key is used for authentication and another key is used to get access for data transmission. The key set generation and distribution to the trusted nodes is performed as

$$Rval \leftarrow getVal(n)$$
$$Mval \leftarrow geteven(n)$$
$$Lval \leftarrow getPrime(n)$$
$$KeyU = Rval \ \&\& \ Mval \oplus Lval$$
$$KeyR = KeyU \oplus Mval$$
$$KeyS = \sum_{n=1}^{M} KeyR(n) \oplus \frac{\text{KeyU}}{\text{Rval}}$$
$$KeyD = \sum_{n=1}^{M} KeyS(n) \oplus \text{Lval(n)} \&\& Rval(n) \ll 2$$

$$KeySet[M] = \sum_{n=1}^{M} \{KeyS(n) : KeyD(n)$$

Step-5: Each node in the network will be authenticated to maintain trust in the network. The nodes that are trusted only will be allowed for transmission process. The node authentication helps to identify malicious nodes in the network. The node authentication is performed as

$$(n) < eTh$$
$$Otherwise$$

$$NAuth[M] = \prod_{n=1}^{M} getUPI(n) + getTfactor(n) + \gamma(AuditorNode(n))$$

$$+ getKeyS(n) \begin{cases} \leftarrow 1 \ \ if\ KeyS(n) == KeySet(KeyS) \\ \leftarrow 0 \qquad\qquad Otherwise \end{cases}$$

Here γ is the model for considering the Auditor Node feedback that is used to select only trusted nodes.

Step-6: Packet loss rate, data packets, and control packets are the typical parameters used to model trust. Upon request, the auditor node is the sole one to whom each node reports the values stored in its trust table, which includes all nodes in the immediate vicinity. One way to determine route trust is by looking at the total number of packets that the node in question has received and $\tau, n+1))$ forwarded. The trusted route selection process is performed as $if(Tfactor > TTh$

$$Otherwise$$

$$Troute[M] = \sum_{n=1}^{M} \frac{getaddr(NAuth(n))}{M} + getUPI(\max(Tfactor(n,n+1)))$$
$$+ \gamma(AuditorNode(n,n+1)) + getStatus(NAuth(n))$$

}

4. RESULTS

The big nodes that make up a wireless sensor network are set up on the fly. There is the ability for sensing and calculating data to be communicated by each sensor node. The sensor nodes use wireless transfer mechanisms to send data to the base station. However, a sensor network system cannot function without a lifetime routing design. Traditional routing methods fall flat when applied to these types of networks due to limitations such as power consumption and the requirement for vast capabilities. Nodes in WSNs depend significantly on routing. The routing protocol, also known as a routing policy, allocates control data to determine the optimal paths between any two nodes, given a large number of alternative routes. It goes on to detail the interplay between the various network routing mechanisms. The routing protocol enables data to be transmitted from one

node to another by means of neighboring nodes until it reaches its ultimate destination. During routing, it uses algorithms to find the optimal path from the source node to the destination node.

Transportation, industrial control, military reconnaissance, drone monitoring, industrial control, and countless more sectors make heavy use of WSNs to collect a wide range of physical or environmental data. In some cases, WSN are deployed in areas that are dangerous or otherwise difficult to reach. Dispersed detection, the decentralized assessment of a target's physical state by means of several sensors placed in the target area, is a common decision-making approach in WSN. Every sensor collects data, analyses it, and then relays its results to a command center over a wireless channel. All of the data collected by the sensors is analyzed by the centralized authority before a final decision is made on the target. Because sensor data transfers are broadcast, an attacker on the network might easily intercept them, posing a serious threat to the privacy of data transmissions in WSNs. A strict node authentication mechanism is employed by the proposed model to guarantee that every node is either trustworthy or malicious. In order to verify the identity of nodes, a cryptographic model is used to create and assign keys. In this research, Node Auditor based Trusted Route Selection with Node Authentication using Multi Key Distribution (NAbTRS-NA-MKD) Model is proposed for secure data transmission in WSN. The proposed model is compared with the traditional Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm (AQoS-TbLSRA) for WSNs, A Lightweight Authentication Framework for Fault-Tolerant Distributed WSN (LAF-FT-DWSN) and a Secure Three-Factor User Authentication Protocol with Forward Secrecy (STFUAP-FS) for Wireless Medical Sensor Network Systems. The proposed model when compared with the traditional methods performs better in trust calculation, node authentication and secured route selection.

After the data has been processed, every node in the network will have been registered. Each node is identified and their properties are analyzed using the information provided by the nodes. After each node's registration is processed, a Unique Permanent Identifier (UPI) is assigned to it. Additional communication and analysis are conducted using this UPI. The Node Registration Time Levels of the existing and proposed models are depicted in Table 1 and Figure 6.

Table 1: Node Registration Time Levels

Nodes in the Network	Models Considered			
	NAbTRS-NA-MKD Model	AQoS-TbLSRA Model	LAF-FT-DWSN Model	STFUAP-FS Model
50	11	17	15.2	19.4
100	11.2	17.2	15.4	19.5
150	11.3	17.5	15.7	19.7
200	11.5	17.7	15.9	20
250	11.8	17.8	16.1	20.2
300	12	18	16.3	20.4

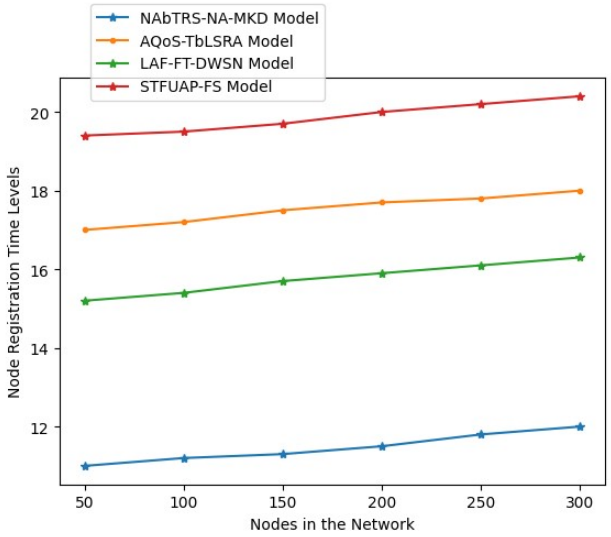

Fig 6: Node Registration Time Levels

The trust factor of each node is calculated and this trust factor represents the node properties. The node parameters are considered for calculation of node trust factor. The Trust Factor Calculation Accuracy Levels of the proposed and existing models are shown in Table 2 and Figure 7.

Table 2: Trust Factor Calculation Accuracy Levels

Nodes in the Network	Models Considered			
	NAbTRS-NA-MKD Model	AQoS-TbLSRA Model	LAF-FT-DWSN Model	STFUAP-FS Model
50	97.7	94.2	95.4	92.3
100	97.9	94.5	95.6	92.5
150	98.1	94.6	95.8	92.8
200	98.4	94.8	96.1	93
250	98.6	95	96.3	93.2
300	98.8	95.2	96.5	93.4

Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

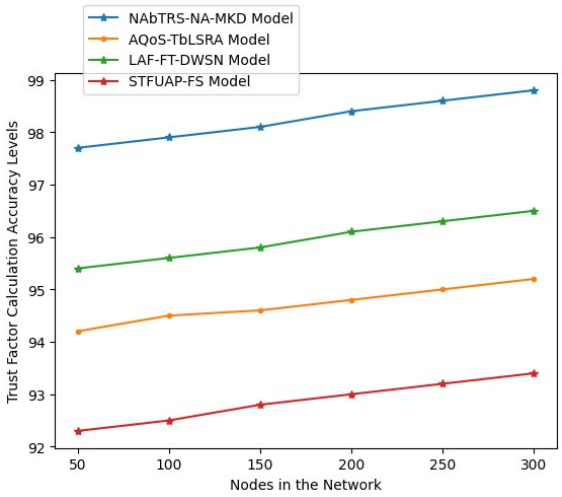

Fig 7: Trust Factor Calculation Accuracy Levels

The proposed model considers auditor node from the available trusted nodes. The trusted node having high capability is considered as a auditor node. The auditor node is used to monitor the entire network. The Network Node Auditor Selection Accuracy Levels of the existing and proposed models are indicated in Table 3 and Figure 8.

Table 3: Network Node Auditor Selection Accuracy Levels

Nodes in the Network	Models Considered			
	NAbTRS-NA-MKD Model	AQoS-TbLSRA Model	LAF-FT-DWSN Model	STFUAP-FS Model
50	97.5	91	92.8	91.8
100	97.7	91.2	93	92.1
150	97.9	91.4	93.2	92.3
200	98.1	91.5	93.5	92.5
250	98.4	91.8	93.7	92.8
300	98.6	92	94	93

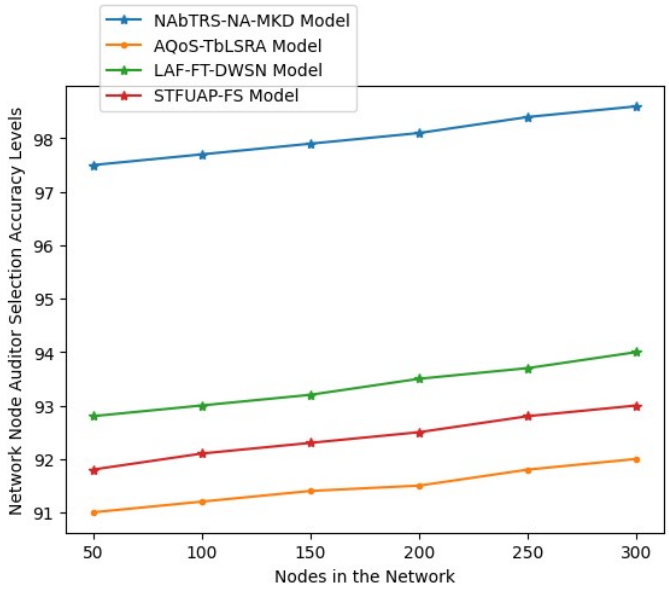

Fig 8: Network Node Auditor Selection Accuracy Levels

In key generation, auditor node generates a set of cryptographic keys, including both public and private ones. Distributed key generation is distinct from other public key encryption techniques in that it does not depend on TTPs. Key management is the process of overseeing a cryptosystem's cryptographic keys. All aspects of keys, from creation to storage, usage, crypto-shredding, and replacement, fall under this category. Included in this category are protocols for cryptography, key servers, user procedures, and any others that may be pertinent. The Key Set Generation and Distribution Time Levels of the existing and proposed models are indicated in Table 4 and Figure 9.

Table 4: Key Set Generation And Distribution Time Levels

Nodes in the Network	Models Considered			
	NAbTRS-NA-MKD Model	AQoS-TbLSRA Model	LAF-FT-DWSN Model	STFUAP-FS Model
50	7.0	15.2	11	17
100	7.2	15.4	11.2	17.2
150	7.4	15.7	11.3	17.5
200	7.6	15.9	11.5	17.7
250	7.8	16.1	11.8	17.8
300	8	16.3	12	18

Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

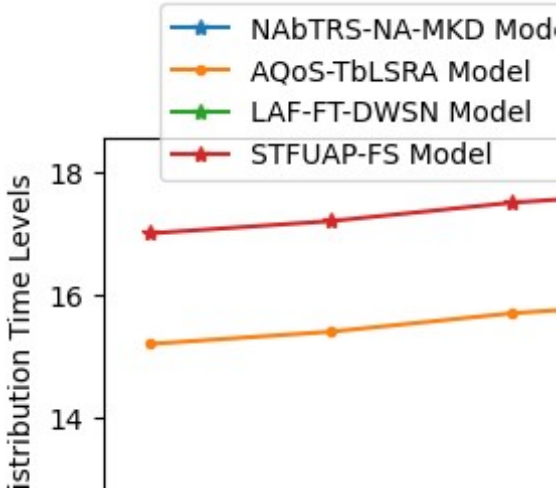

Fig 9: Key Set Generation And Distribution Time Levels

To guarantee safe communication between the management server and data collectors, Node Authentication is employed. The purpose of network authentication is to confirm the user's identity before granting access to a network service. The Node Authentication Accuracy Levels of the proposed and existing models are represented in Table 5 and Figure 10.

Table 5: Node Authentication Accuracy Levels

Nodes in the Network	Models Considered			
	NAbTRS-NA-MKD Model	AQoS-TbLSRA Model	LAF-FT-DWSN Model	STFUAP-FS Model
50	97.5	92.9	94	92.6
100	97.7	93.1	94.2	92.9
150	97.9	93.3	94.6	93.1
200	98.1	93.6	94.9	93.3
250	98.4	93.8	95.1	93.5
300	98.7	94	95.3	93.7

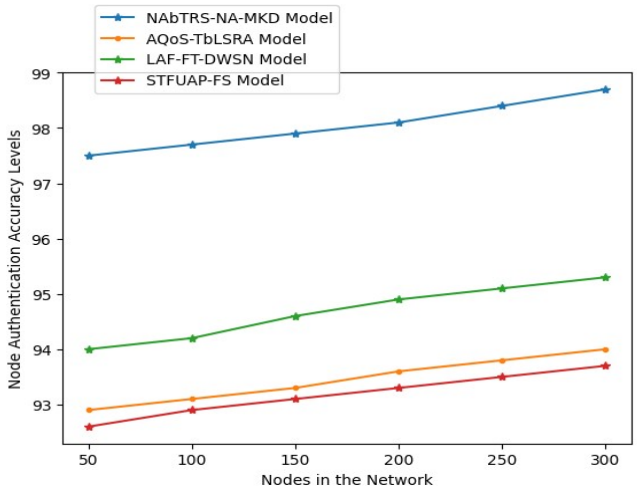

Fig 10: Node Authentication Accuracy Levels

The auditor node in the proposed model will monitor each node performance levels, performs node authentication to make the network route secured. The nodes which are successfully authenticated and trusted nodes are involved in updating the routing table. The Trusted Route Selection Accuracy Levels of the existing and proposed models are represented in Table 6 and Figure 11.

Table 6: Trusted Route Selection Accuracy Levels

Nodes in the Network	Models Considered			
	NAbTRS-NA-MKD Model	AQoS-TbLSRA Model	LAF-FT-DWSN Model	STFUAP-FS Model
50	97.5	92.9	93.5	91.2
100	97.8	93.1	93.7	91.7
150	98.1	93.4	93.9	91.9
200	98.3	93.6	94.2	92.3
250	98.6	93.9	94.6	92.5
300	98.8	94	94.8	92.7

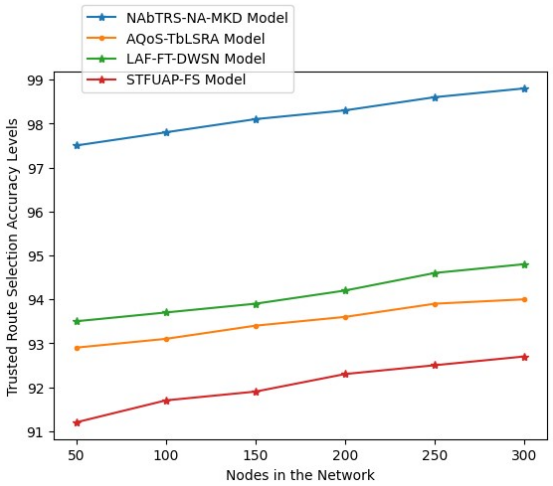

Fig 11: Trusted Route Selection Accuracy Levels

The quantitative metrics are shown in the table 7. The results reresent that the proposed model exhibits better performance.

Table 7: Quantitative Metrics

Models Considered	**Quantitative Metrics**			
	Throughput	Latency	Packet Delivery Rate	Loss Rate
NAbTRS-NA-MKD Model	98.9	2.3	99.6	0.4
AQoS-TbLSRA Model	94.5	4.5	95.6	1.3
LAF-FT-DWSN Model	95.2	6.8	94.6	5.4
STFUAP-FS Model	96.6	7.4	93.8	6.2

5. CONCLUSION

Despite the fact that existing routing protocols are not safe, secure routing is essential for the acceptance and implementation of sensor networks in numerous applications. The research of routing in sensor networks is still in its infancy, but what little there is expanding at a rapid pace. Data security during transmission between intra-network nodes is achieved by processing and measurement in a wireless sensor network. By analyzing changes in node behavior, it hopes to address the issue of typical nodes being isolated in practical communication. An auditor node that studies the actions of nodes and finds a trust factor is part of the suggested model. The node's activity is evaluated and labeled as malicious or normal based on the trust factor. The suggested approach improves performance by increasing the packet delivery rate by making it easier to detect rogue nodes. Improvisation is feasible, which aids in keeping the network alive for longer and increases performance, because harmful qualities are detected based on their behavior and previous performance, instead of demanding all the nodes in a route, as is done in traditional techniques. A new line of inquiry into trustworthy sensor node platforms has been launched by the proposed work. Only nodes that have been verified as trustworthy are included in the proposed model's communication process. In order for each node to participate in updating the routing table and selecting routes, authentication is required. Among the many potential uses for WSNs, public-key cryptography stands out as an effective and trustworthy method for key management and security. When compared to symmetrical methods that provide positive energy profits through random drops, public key cryptography offers more benefits because to its lower key size, low CPU consumption, and low memory utilization. You don't have to reveal the size of the key to every node in a network to use asymmetrical algorithms; instead, you can use variable key management generation techniques to achieve efficient security goals. This is because the private key isn't calculated using the public key of the network, which is a security feature of asymmetrical cryptosystems. In this research, Node Auditor based Trusted Route Selection with Node Authentication using Multi Key Distribution Model is proposed for secure data transmission in WSN. The proposed model achieved 98.7% accuracy in node authentication and 98.8% accuracy in trusted route selection. In future, the cryptography models complexity levels can be reduced to enhance the performance levels. The trust factor calculation can be extended by considering more number of nodes factors including internal and externals factors to improve the quality of service levels.

REFERENCES

[1] Pathak, I. Al-Anbagi and H. J. Hamilton, "An Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23826-23840, 1 Dec.1, 2022, doi: 10.1109/JIOT.2022.3189832.

[2] M. Bin-Yahya, O. Alhussein and X. Shen, "Securing Software-Defined WSNs Communication via Trust Management," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22230-22245, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3102578.

[3] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy and R. Patan, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks," in IEEE Transactions on Engineering Management, vol. 68, no. 1, pp. 170-182, Feb. 2021, doi: 10.1109/TEM.2019.2953889.

[4] Z. Teng, C. Du, M. Li, H. Zhang and W. Zhu, "A Wormhole Attack Detection Algorithm Integrated With the Node Trust Optimization Model in WSNs," in IEEE Sensors Journal, vol. 22, no. 7, pp. 7361-7370, 1 April1, 2022, doi: 10.1109/JSEN.2022.3152841.

[5] M. A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar and K. Mahmood, "Security Analysis on "A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems"," in IEEE Systems Journal, vol. 15, no. 4, pp. 5557-5559, Dec. 2021, doi: 10.1109/JSYST.2021.3073537.

[6] F. Wu, X. Li, L. Xu, P. Vijayakumar and N. Kumar, "A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks With IoT Notion," in IEEE Systems Journal, vol. 15, no. 1, pp. 1120-1129, March 2021, doi: 10.1109/JSYST.2020.2981049.

[7] E. T. Oladipupo et al., "An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks," in IEEE Access, vol. 11, pp. 1306-1323, 2023, doi: 10.1109/ACCESS.2022.3233632.

[8] K. S. Sai, R. Bhat, M. Hegde and J. Andrew, "A Lightweight Authentication Framework for Fault-Tolerant Distributed WSN," in IEEE Access, vol. 11, pp. 83364-83376, 2023, doi: 10.1109/ACCESS.2023.3302251.

[9] S. Itoo, A. A. Khan, M. Ahmad and M. J. Idrisi, "A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System," in IEEE Access, vol. 11, pp. 56875-56890, 2023, doi: 10.1109/ACCESS.2023.3280542.

[10] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities attacks and countermeasures", *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616-644, 1st Quart. 2020.

[11] S. H. Awan, S. Ahmed, A. Nawaz, S. Sulaiman, K. Zaman et al., "BlockChain with IoT, an emergent routing scheme for smart agriculture," International Journal of Advanced Computer Science and Applications, vol. 11, no. 4, pp. 420–429, 2020.

[12] .A. E. G. Sanchez, E. A. R. Araiza, J. L. G. Cordoba, M. T. Ayala and A. Takacs, "Blockchain mechanism and symmetric encryption in a wireless sensor network," Sensors, vol. 20, no. 10, pp. 2798, 2020.

[13] 13.M. H. Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar and G. Nagalalli, "Trust aware localized routing and class-based dynamic blockchain encryption scheme for improved security in WSN," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 5, pp. 5287–5295, 2021.

[14] 14.S. Amjad, S. Abbas, Z. Abubaker, M. Alsharif, A. Jahid et al., "Blockchain-based authentication and cluster head selection using ddr-leach in internet of sensor things," Sensors, vol. 22, no. 5, pp. 1972, 2022.

[15] 15.A. S. Kumar, S. G. Winster and R. Ramesh, "Efficient sensitivity orient blockchain encryption for improved data security in cloud," Concurrent Engineering, vol. 29, no. 3, pp. 249–257, 2021.

[16] 16.M. Elhoseny, K. Haseeb, A. A. Shah, I. Ahmad, Z. Jan et al., "IoT solution for ai-enabled privacy-preserving with big data transferring: An application for healthcare using blockchain," Energies, vol. 14, no. 17, pp. 5364, 2021.

[17] L. Yang, Z. Yu, M. A. El-Meligy, A. M. El-Sherbeeny and N. Wu, "On multiplexity-aware influence spread in social networks", IEEE Access, vol. 8, pp. 106705-106713, 2020.

[18] L.Narayana,V., Lakshmi Patibandla, R.S.M., Pavani, V., Radhika, P. (2023). Optimized Nature-Inspired Computing Algorithms for Lung Disorder Detection. In: Raza, K. (eds) Nature-Inspired Intelligent Computing Techniques in Bioinformatics. Studies in Computational Intelligence, vol 1066. Springer, Singapore. https://doi.org/10.1007/978-981-19-6379-7_6.

[19] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for

prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437

[20] Q. Luo and J. Wang, "FRUDP: A reliable data transport protocol for aeronautical ad hoc networks", IEEE J. Sel. Areas Commun., vol. 36, no. 2, pp. 257-267, Feb. 2018.

[21] J. Wang, Y. Liu, S. Niu and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking", Comput. Commun., vol. 165, pp. 131-140, Jan. 2021.

[22] Y. Liu et al., "Zero-bias deep learning for accurate identification of Internet-of-Things (IoT) devices", IEEE Internet Things J., vol. 8, no. 4, pp. 2627-2634, Feb. 2021.

[23] V. L. Narayana, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394.

[24] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437

[25] L.Narayana, V., C.R. Bharathi. (2023). Efficient route discovery method in MANETs and packet loss reduction mechanisms. International Journal of Advanced Intelligence Paradigms, 2023 Vol.25 No.1/2. 10.1504/IJAIP.2023.130818.

[26] A. Adavoudi-Jolfaei, M. Ashouri-Talouki and S. F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks", Peer-Peer Netw. Appl., vol. 12, no. 1, pp. 43-59, Jan. 2019.

[27] S. Shin and T. Kwon, "A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes", Sensors, vol. 19, no. 9, pp. 2012, 2019.

[28] N. A. Khan and A. Awang, "Elliptic curve cryptography for the security of insecure Internet of Things", Proc. Int. Conf. Future Trends Smart Communities (ICFTSC), pp. 59-64, Dec. 2022.

[29] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks", J. Ambient Intell. Humanized Comput., vol. 12, no. 1, pp. 547-566, Jan. 2021.

[30] S. Bonomi, A. Del Pozzo, M. Potop-Butucaru and S. Tixeuil, "Approximate agreement under mobile Byzantine faults", Theor. Comput. Sci., vol. 758, pp. 17-29, Feb. 2019.