International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Encrypted Routing Using Trees and Energy Efficiency in WSN

Dr. Gowthami V [1], Dr. Praveen B M [2]
Post-Doctral Fellow, Institute of Computer Science and Information Science, Srinivas University [1]
Assistant Professor, School of Sciences and Computer Studies, CMR University[1]
Director, Srinivas University, Mukka, Mangaluru, Karnataka, India [2]
gowthamishalini@gmail.com

Abstract

Nowadays, the use of Wireless Sensor Networks is not constrained to research; it has been realistically implemented in numerous defence and general civilian applications. Although a great deal of research has been done on energy-efficient routing and message protocols, and progress has been made to a respectable level, widespread adoption of the technology is unlikely in the absence of secure messages. Owing to WSN's distinct features, safety plans designed for other wireless networks do not apply to WSN. This study presents a new tree-based method for hierarchical routing protocols called Encrypted Routing Using Trees and Energy Efficiency. It uses a lightweight key broadcasting mechanism in conjunction with the clustering approximation. The study's results were compared to the conventional SLEACH to determine that the recommended method would provide greater safety and energy efficiency.

Keywords: *SLEACH, RSA, TLS, WSN, ERTEE.*

Introduction

A wireless network is a kind of network that links different hardware, such as printers, and computing equipment, such as servers and clients. This is the most affordable substitute for a wired network, guaranteeing improved accessibility and significantly less maintenance concerns. Terrestrial microwave networks, WLAN (Wireless Local Area Networks), and cell phone networks are a few notable examples of wireless networks. Wireless networks can be broadly categorized as Cellular networks, Wireless Sensor Networks, MAN (Mobile Adhoc Networks), WPAN (Wireless Personal Area Networks), WLAN, WMN (Wireless Mesh Networks), WMAN (Wireless Metropolitan Area Networks), WWAN (Wireless Wide Area Networks), etc.

A wireless sensor network, or WSN, is made up of sensor nodes that are networked together to aggregate data. A sensor node is an apparatus that is proficient of detecting physical characteristics of its surroundings, such as temperature, pressure, wetness, motion, smoke, etc. The features of the node serve as the foundation for the numerous applications of WSN [1] [2]. Before wireless sensor networks were developed, safety was a crucial field of study. Even prior to the development of WSN, dependable safety protocols such as the Diffie-Hellman key exchange method [3], RSA [4], TLS [5], and Kerberos [6] were in place. Nevertheless, these methods did not view resource limitations as a significant concern. In all forms of WSN, confidentiality, integrity, availability, and authenticity should be upheld in addition to lowering resource consumption.

A network's availability, confidentiality, integrity, and authentication can all be compromised by an attacker using a variety of attack techniques. That being said, not every attack strategy works with every kind of wireless sensor network. For WSN safety, key management is the most crucial component. In addition to preserving secrecy, it supports authentication, privacy, and occasionally integrity in other modules. As a result, it's critical to have a key management strategy that both reduces burden on sensor nodes and offers safety in accordance with the needs of the target WSN application. In a wireless sensor network, a secure and energy-efficient message system typically consists of several clusters, each of which has a specific number of sensor nodes.

Group-based message systems rely entirely on effective key management or exchange systems to facilitate message, which in turn ensures safety during message between numerous clusters. Therefore, it is imperative to study the key-management tactics applied to cluster-based message systems that have been reported in diverse literatures. Ensuring

energy efficiency while maintaining safety is one of the difficult aspects of studying wireless sensor network applications, though. It is mostly necessary because wireless sensor networks can experience various threat situations or an attack that interferes with message. As a result, the recommended study presents a method that simultaneously suggests a mitigation strategy for safety and energy-related challenges.

The main focus of this work is to address the safety vulnerabilities that resulted from the Sybil assault. Section 2 talks about some of the most recent methods for incorporating safety and energy efficiency. The challenges that have been discovered for the proposed study are briefly discussed in Section 3, and the proposed model is then discussed in Section 4. While Section 6 talks about the study's benchmark results, Section 5 talks about the algorithm being employed for the recommended investigation. In Section 7, some final thoughts are expressed and the future course of the work is briefly hinted at.

Related Works

Numerous investigations have been conducted to guarantee maximum safety and energy efficiency in wireless sensor networks. A few noteworthy studies that were most recently identified are covered in this section. A routing protocol has been described by Chen et al. [7] to guarantee energy efficiency in wireless sensor networks. It was discovered that the result, which concentrated on asymmetric link formation, had a higher delivery rate. The effort does not, however, address safety. Takaishi et al.'s most recent study [8] is unusual in that it focuses on small-scale wireless sensor networks and uses the expectation-maximization technique to assure improved energy efficiency during the data aggregation process.

Rahman and Matin [9] conducted similar research in this area and describe a routing system that uses swarm intelligence to increase the network lifetime of wireless sensor networks. Nevertheless, the method can only improve 40% of energy without benchmarking. He et al.'s study [10] addressed energy concerns as well as lifespan reliability, and they provided a model that uses a greedy heuristic technique to determine the maximum coverage of a sensor network. It was discovered that the result had a far better degree of dependable network lifetime and a very low failure chance. It was not, however, contrasted with the conventional LEACH or any other routing algorithm variation that deals with energy-related concerns.

Li and Xiong [11] have put out a creative concept for combining Internet-of-Things with wireless sensor networks while guaranteeing messagesafety with identity-based cryptography. Nevertheless, the result is mainly talked about in terms of processing time; it doesn't really show how the method affects QoS metrics like energy or overall. Cho et al. [12] conducted a second investigation with a safety focus and provided trust-enhancing mitigating strategies. Energy efficiency and data redundancy still have to be traded off, though. To counteract phantom attacks, Long et al. [13] have recommended a method. The study's results were assessed using energy usage and safety factors.

Problem Statement

The following issues are being considered for the planned study:

- It is an extremely computationally demanding endeavor to jointly minimize safety and energy challenges.
- The majority of current research on attaining energy efficiency is largely influenced by LEACH. This leads to problems, such as: o
    - Such a technique doesn't handle safety.
    - These methods suffer from the same clustering issues as LEACH.
    - The focus of computational complexity is broader.

- Isn't scalable to wireless sensor networks on a big scale.

- Most of the current cryptographic protocols are either SHA1/SHA2 or MD4/MD5, and they are quite difficult to run on a node.

Proposed Methods

The main goal of the recommended system is to work together to solve the issue of a secure and energy-efficient data aggregation method. Using probability theory, the recommended approach is named ERTEE to guarantee exceptional energy efficiency and a reliable authentication method in wireless sensor networks.

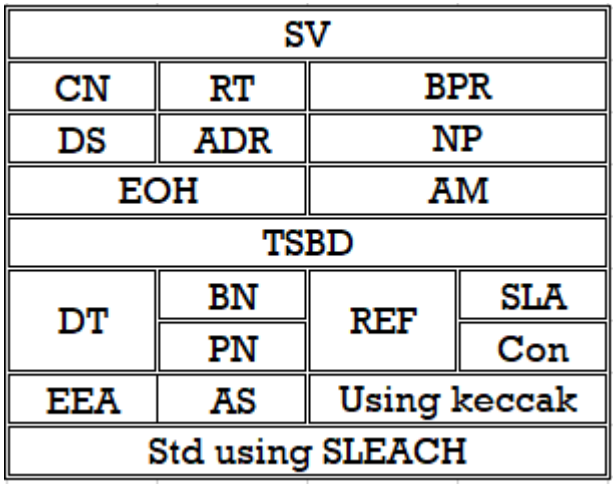

Fig 1: Architecture of ERTEE

The recommended system's main contributions are:

• Ensuring optimal energy saving through the use of a straightforward tree-based methodology.
• To guarantee an affordable safety protocol that uses Keccak to thwart Sybil attacks.
• To compare the ERTEE results with the SLEACH standard safety and energy efficient algorithm.

A tree-based method is taken into consideration in order to investigate the concerns of energy and safety management in wireless sensor networks. Two primary layers comprise the ERTEE architecture: the first layer pertains to the message model, while the second layer deals with the safety model. The study will employ a conventional radio-energy dissipation model since it is primarily motivated by standard hierarchical routing protocols. In this study, we make the assumption of a simple model in which energy is dissipated by the transmitter, power amplifier, and receiver in order to power the radio electronics. This phase's main goal is to create a system model for assessing the sample application's energy costs and safety effectiveness.

The recommended computational model can be built on top of the tree-based structure once it has been designed in order to run simulations and extract study results. The aggregator node selection process is intended for use in wireless sensor networks. Each node in the network is enabled to broadcast its unique information to the AN (Aggregator Node), from which the collected data is routed to the sink. This study phase's primary goal is to get as many aggregator nodes to actively engage in the process of choosing non-redundant data to be combined and sent via a novel tree-based routing protocol.

Solving the Energy Issue

In particular, ERTEE employs multi-valued logic to provide the best energy-efficient factors for hierarchical routing strategies in wireless sensor networks. In order to address energy efficiency, ERTEE performs the single-logic tree approximation and multi-logic tree approximation levels of clustering approximation. The following is how the tree approximation is discussed:

Estimation of a Single-logic Tree

Various energy-related variables are gathered in this phase using the standard radio-energy model [14] to ensure that the most efficient node of the tree is selected to carry out traffic flow based on the largest weight factor. This is a crucial stage in which the clustering approximation [15] is carried out from the root node to the candidate node while taking its spatial attributes and battery power factor into account. At this stage, clustering approximation is also carried out in order to extract the battery power factor, current coordinates of the nodes, updated information about the data being routed among the nodes, and their correlation factor with other groups.
There may be some network overhead because the root node will communicate on behalf of each candidate node in the single tree. In wireless sensor networks, overhead is typically caused by redundant data, which also wastes energy. Therefore, the root node will gather specific data from the candidate node, such as the battery power factor, current coordinates, adjacency matrix of other correlated nodes, and time-stamp in the data packet, in order to prevent data redundancy. Therefore, a significant amount of redundancies may be reduced in the single-logic tree approximation method itself, resulting in the single tree's energy being preserved.
As a result, the approximation factors employed in this stage will reduce network overhead and needless data loss while facilitating easy message between every candidate node and the root node in a single tree.

Estimation of Multi-logic Trees

This is the single-logic tree approximation's optimized operation, which further raises the tree's weight factor. Although the overhead problems are somewhat alleviated at the Single-Logic Tree Approximation stage, they do not apply to large-scale trees if the tree structure is dynamic in nature. We have opted to use this assumption, as is customary in wireless sensor networks, because base station mobility can occasionally decrease clustering performance [16] in terms of the energy needed for successful data delivery. This approximation stage makes the assumption that root nodes are sufficiently separated from one another.
It is conceivable for some nodes in a huge tree structure to behave selfishly and refuse to participate in the data forwarding process. We make this assumption for two reasons, for example: (i) a compromised node will never help transfer data; instead, it will be more likely to drop the packet; and (ii) nodes with lower battery power factor may decide to save energy by refusing to help forward data packets. These problems typically affect the intermediate node that helps with data delivery rather than the candidate or root nodes. Therefore, estimations of the node-density factor, battery power factor, zonal pivotal component, and contiguity factor are taken into account in this step along with different tree structures.
By calculating the spatial correlation between each root node and each candidate node, the ZPF (zonal pivotal factor) is calculated. The only tree structure utilized in data message's spatiotemporal factor is used to calculate the CF (contiguity factor). ERTEE places a strong emphasis on achieving lower ZPF values to guarantee that the least amount of energy is lost during message.

Solving the Safety Issue

ERTEE is centred on utilizing a very low-tech cryptographic method to guarantee a safe data aggregation procedure. The set of random indexers that represents the nodes is given to all candidate and root nodes at this point. We regard the

adversarial model as a Sybil assault capable of stealing and faking the sensor nodes' identities. Consequently, the main goal is to carry out authentication between the nodes themselves, allowing access to resources or the ability to execute specific operations such as forwarding packets to be prohibited in the event that a hacked node is discovered. These indexers are therefore designed for these purposes.
Incorporating symmetric keys between the nodes that will be utilized for inter-node message is another function of ERTEE. To analyze several likely vulnerable circumstances, we consider the adversary module in the proposed ERTEE model to be both mobile and static. Because of the system's design, the key can be randomly generated even though previous studies typically take a specified key size into account. This is done in order to prevent adversaries from ever estimating the size of the key prior to cryptanalysis. In the safety algorithm, we have included one more intriguing example, though. It is observed that the primary goal of any Sybil attack aimed at breaching the sensor node is typically the derivation of the shared key. As a result, we make use of this knowledge and further encrypt the key to make it useless to the attacker. Thus, in this sense, it both lessens the internal attack and the external onslaught.

Application Of Algorithm

ERTEE is implemented using Matlab as the design platform on a standard Windows OS 32-bit computer. The ERTEE algorithm design is divided into two sections: an energy-related algorithm and a safety-related algorithm.

The Energy Efficiency Algorithm
Enter: Tx: Transmission range

BF: Battery power factor

N: Number of Nodes A: Simulated Area

i: Incoming Data Size

α: the amount of energy needed for one bit of data to be processed by hardware

Node Position (Lx, y)

adjacency matrix (Amat) Tstamp: The packet's time stamp Root node (Rnode)

candidate node (Cnode)

Number of nodes with enough battery life as an output

Start

1.Set up N, Tx, BF, and deploy at random in A.
2.Use the graph G=(V, E), where V stands for nodes and E for routes.
// Apply an approximation using single-value logic
3. Determine the Tree Eex's Weight = ɥ.
4. Based on ArgMax (Eex), choose the root.
5. Build the GIJ IJ-threshold tree.
6. Perform the following for j=1 to k:
7. Choose the node nj in GU with the highest degree.
8. Take nj and its adjacency matrix out of G, isolate it, and map it to cluster C(nj).
9. Create the k cluster by formulating C(n1),... C(nk-1)
10. Construct a matrix to hold particular data for a single tree. Munit_hop= Exclusive ({\)| {\ ={BF, Lx,y, Amat,

Tstamp}
11. Update Munit_hop and carry out data message from the root to every node.
12. If the data that is received matches Munit_hop.
13. Toss updating Munit_hop; this removes redundant info.
// Apply an approximation using multi-value logic.
14. Recalculate the node density.
15. Calculate ZPF using Corspat (Rnode, µCnode).
16. Determine the overhead by evaluating CF={Corspat(œCnode), \Tstamp}
17. If BF<0, 18. Signal node failure
19. Else
20. Calculate the total node-to-node death of the remaining nodes.
End

In a wireless sensor network, Algorithm 1 addresses the mitigation strategy for energy dissipation among the sensor nodes. In order to simulate a real-time scenario, the algorithm first determines the number of nodes, transmission range, and battery power factor. The nodes are then deployed randomly. The approach maps with the nodes and routes in a wireless sensor network using the graph technique for tree structure construction. Single-valued logic and multi-valued logic approximation are then applied. Next, the algorithm calculates the least energy required to process a single bit of data, with the goal function being its minimization.After applying the clustering approximation technique, which evaluates candidate nodes based on maximum node degree, the criterion specified in step 4 selects the root node. At last, the neighborhood nodes are assessed based on the graph threshold factor Ġ, which subsequently forms the clusters. A specific matrix called Munit_hop contains all of the transactional routing data in addition to data on channel capacity, node positions, adjacency matrices for neighboring nodes, and time stamp factors. Every cycle of the data distribution process, the uniqueness of the data is verified by contrasting the incoming data with Munit_hop. If it is discovered to be the same, we refer to it as data-redundancy. As a result, redundant data packets are ignored, optimizing memory. In order to further optimize energy efficiency, multi-valued logic is used in the following step, where steps 15 and 16 are used to compute the ZPF and CF (contiguity factor). BPR (Battery power Ratio is evaluated at each step to determine the total number of active nodes involved in the message process. Thus, Algorithm-1's energy consumption is much reduced while its space and temporal complexity are extremely low.

Sybil attack mitigation algorithm
{: indexers, ş1: BF, ş2: Node ID, and ş3: Public Key are input.
Final Product: Secured Standard Key Beginning:
1. Use random indexers ({\) to initialize the nodes. {\n=rand(ş1, ş2, ş3)
2. Determine the key's size at random and carry out authentication
3. Should nodex(ş3) == nodey(ş3)
4. Don't generate a key and break off the contact
5. Another
6. Produce the secret key using the formula Key1= | nodex(ş1)- nodey(ş1) |2+4.Nodey(ş2) - nodex(ş2)
7. In the event that (K (K nodes −2 nodes
8. Max(2||key-chain(Knodes)) = Key2
9. Create a Common Key by using Scom_key=[Skey2|| }
10. Encrypt data using key S = h(S)//keccak enc_key.

End

Algorithm 2 talks about how to protect ERTEE from a Sybil attack. The nodes in this approach are defined using random indexers {\1, {\2,... {}n etc. I ş1 as battery power factor, ii ş2 as Node ID, and iii ş3 as Public Key are the three

main characteristics of indexers. The intriguing aspect of indexers' assumptions is that every data message cycle causes all three attributes (ş1, ş2, and ş3) to change in value. As a result, even in the unlikely event that one or more of the attributes are compromised by internal or external attackers, they will be unable to use them to compromise, steal, or falsify the identities of any sensor nodes that are present in the simulation environment.
It is assumed that each sensor node has been equipped with specific public keys to enable group message. When a node broadcasts a RR (Requesting Route), the nodes authenticate with one another. In that scenario, we merely take the public keys into account to deduce the authentication procedure. The attacker in a Sybil attack will often try to obtain this public key. However, even in the event that the key is obtained, the step 3 condition guarantees that the key won't be generated, preventing the connection (RACK) from being accepted. But, it can also occur with a regular node; in such instance, additional parameters like ş1 and ş2 are also examined, and their values will never coincide with those of the adversary module. Step 6 mentions using the quadratic root strategy to generate the secret key for authentication. Once each node's key has been evaluated using this method, it is compared to key chains that already exist to create a common key. The common key is then further encrypted using the sophisticated hash function known as keccak.

Result Discussion

It is imperative that ERTEE be compared with a few previous, highly standard techniques that address safety incorporation and energy efficiency in a similar manner in order to conduct a comparative analysis. As a result, we decide to take into account Oliveira et al.'s groundbreaking SLEACH [17]. When the algorithm SLEACH was first presented in 2006, more than 118 researchers had already used it for benchmarking. Fig. 2 demonstrates that, in contrast to SLEACH, which only achieves 14% energy saving during 700 simulation rounds, ERTEE can guarantee the retention of the maximum number of sensor nodes up to 90%. The main cause of this is that SLEACH implements a sophisticated key distribution method without giving any thought to key size. Additionally, key pre-distribution, shared-key discovery, and path-key setup carry out the key generation procedure. Nevertheless, ERTEE generates, recognizes, and encrypts the key using a straightforward one-step process; the sizes of the keys are scalable based on the network vulnerabilities found outside of the Sybil assault.

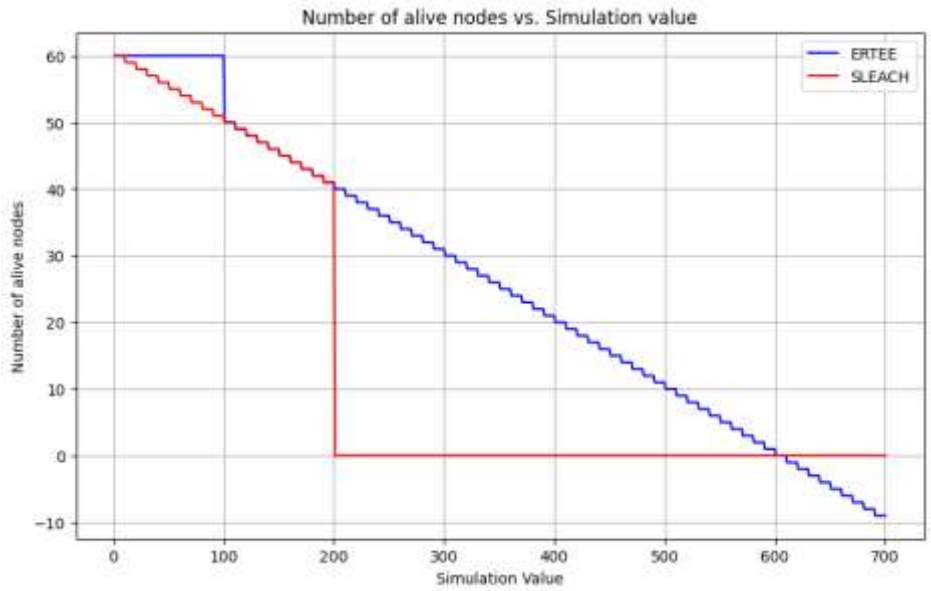

Fig 2:Assessment of Functional Nodes

To comprehend the extent of energy drainage rate, Fig. 3 presents the evaluation of the battery power factor. The result demonstrates that SLEACH is discovered with an impending slow decline in the energy curve. Approximately 200 steps later, the entire network eventually crashes with robust safety. This fact's main cause is that SLEACH increases system

overhead, which guarantees robust safety but not energy efficiency. Conversely, ERTEE offers greater energy stability in the network and is less vulnerable to Sybil attacks.

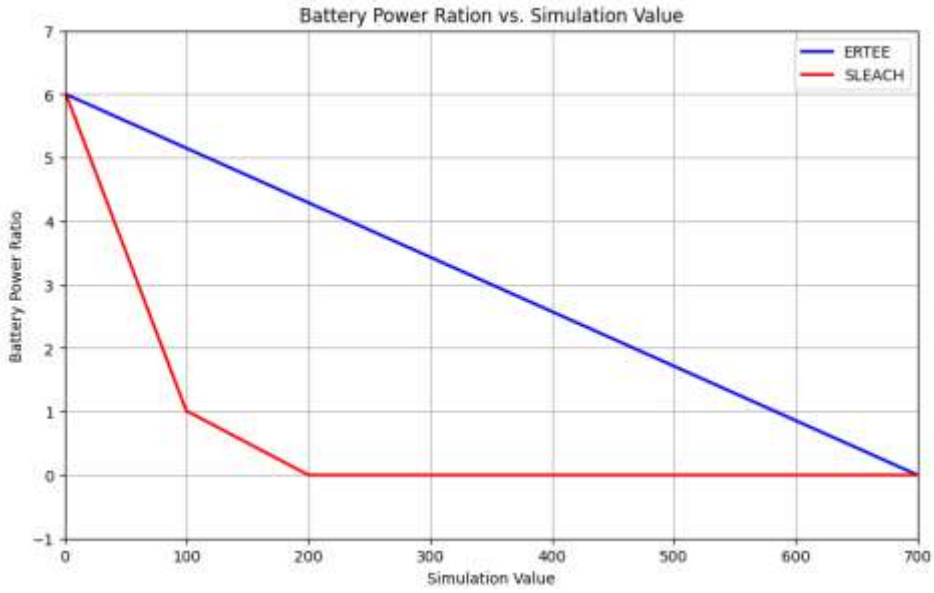

Fig 3: Assessment of battery power factor

The examination of the battery power factor deviation for both SLEACH and ERTEE is displayed in Fig. 4. It was discovered that there is a quick fluctuation in energy during operation that results in a larger energy dissipation while employing SLEACH. The main reason for this is that SLEACH takes into account sizable pools of keys with predetermined IDs. But while node IDs just identify the sensor node, none of them change. In contrast, ERTEE takes into account an indexer, which changes with each message cycle while requiring very little overhead and offering a higher level of safety. While ERTEE's BPR fluctuates, it is still rather stable when compared to traditional SLEACH.

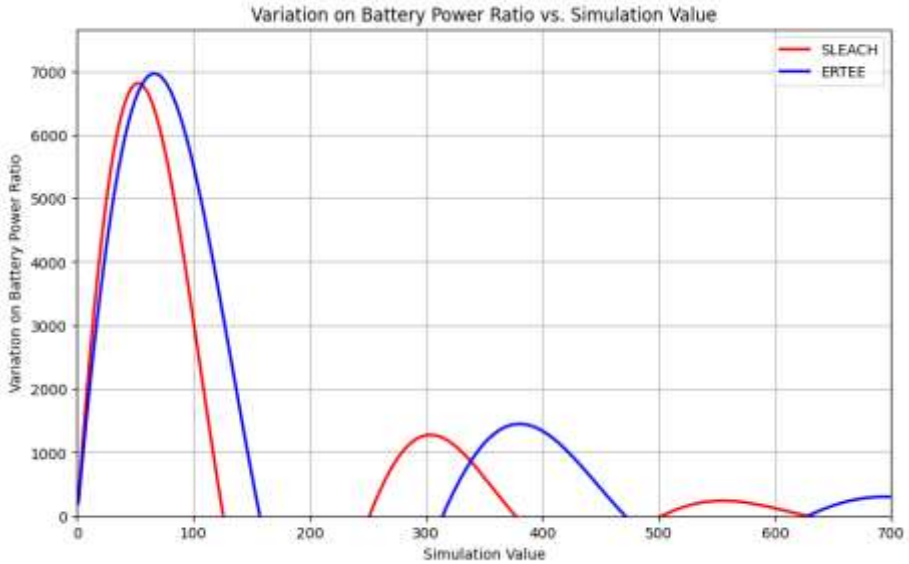

Fig 4:Variation in the battery power factor

The processing time analysis for both the recommended ERTEE and the traditional SLEACH is displayed in Fig. 5. The standard clustering approach is the foundation of SLEACH, and cluster heads are chosen at random. Furthermore, even if we presume that the nonce used in SLEACH cannot be compromised, the encryption techniques entailed a higher number of repeated processes with the danger of generating stale routing information, as the node's id can be readily taken by a Sybil attack. As a result, processing these processes requires more computation time.

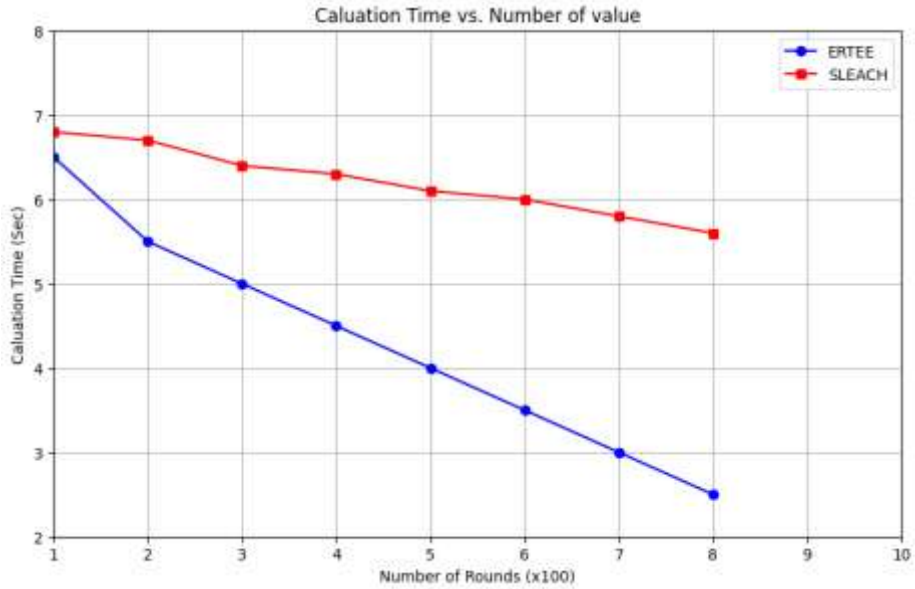

Fig 5:Analysis of the Processing Time

The processing time of the recommended ERTEE does not significantly improve until 200 out of 1000 simulation cycles because the first stages of processing involved computing single-valued logic approximation. Nevertheless, the system picks up speed once the multi-value logic approximation is completed because it only needs to update the adjacency matrix to reduce the redundancy of both data. As a result, ERTEE has greater flexibility to address safety and energy-related concerns.

Conclusion

Ensuring energy efficiency and safety is a difficult challenge that is not often picked for WSN research. We have exposed that in WSN, the emphasis is either entirely on safety or on energy efficiency. As a result, the ERTEE system that is being recommended provides a hierarchical routing protocol that can simultaneously address safety and energy concerns for large-scale wireless sensor networks. Thanks to the consumption of a multi-valued logic approximation system and a straightforward cryptographic technique, the recommended system can guarantee both secure data aggregation and excellent node sustenance. As a result, ERTEE can meet the safety requirements to lessen a variety of deadly attacks on WSN, with a special emphasis on the Sybil attack.

The adoption of the least complex cryptography design, which guarantees potential resilience against safety attacks, is what makes the recommended system novel. It tackles routing, energy, and safety challenges together, which is not found in previous studies. When the study's results were compared to the conventional SLEACH procedure, it was discovered that ERTEE performed better than SLEACH in terms of energy preservation, least energy deviation, and processing speed. Future research may examine delay-based routing strategies to lessen wormhole assaults in WSN.

Reference

[1] I.M.M.ElEmary,S.Ramakrishnan,'WirelessSensorNetworks:FromTheorytoapplications',CRCPress,Computers,799pages,2013

[2] V. C. Gungor, G.P. Hancke, "Industrial Wireless Sensor Networks:Applications, Protocols, and Standards", *CRC Press*, Computers, 406pages,2013

[3] I.Dubrawsky,"HowtoCheatatSecuringYourNetwork",Syngress,Computers,432pages,2011

[4] Rivest,RonaldL.,AdiShamir,andLenAdleman."Amethodforobtainingdigitalsignatures and public-key cryptosystems."CommunicationsoftheACM,no.2pp.120-126,1978

[5] Allen,Christopher,andTimDierks."TheTLSprotocolversion1.0."TheInternetSociety,RFC2246,1999

[6] Kohl,JohnT.,B.CliffordNeuman,andY.Theodore."TheevolutionoftheKerberosauthenticationservice."*IEEEComputerSociety*,1994

[7] X. Chen, Z. Dai, W. Li, and H. Shi, "Performance Guaranteed RoutingProtocols for Asymmetric Sensor Networks", *IEEE Transactions OnEmergingTopicsInComputing*,Vol.1,No.1,June2013

[8] D.Takaishi,H.Nishiyama,N.Kato,R.Miura,"TowardEnergyEfficientBigDataGatheringinDenselyDistributedSensorNetworks",*IEEETransactionsonEmergingTopicsInComputing*,Vol.2,No.3,September2014

[9] Md.N.Rahman,MAMatin,"EfficientAlgorithmforProlongingNetworkLifetimeofWirelessSensorNetworks",*IEEE-TsinghuaScienceAndTechnology*,Vol.16,No.6,December2011

[10] J.He,S.Ji,Y.Pan,Y.Li,"ReliableandEnergyEfficientTargetCoverageforWirelessSensorNetworks",*IEEE-TsinghuaScienceAndTechnology*,Vol.16,No.5,October2011

[11] F. Li and P. Xiong, "Practical Secure Communication for IntegratingWireless Sensor Networks Into the Internet of Things", *IEEE SensorsJournal*,Vol.13,No.10,October2013

[12] Y. Cho and G. Qu, Y. Wu, "Insider Threats against Trust MechanismwithWatchdogandDefendingApproachesinWirelessSensorNetworks",*IEEESymposiumonSecurityandPrivacyWorkshops*,DOI10.1109/SPW.2012.32134,2014

[13] J.N Long, M. Dong, K. Ota, and A. Liu, "Achieving Source LocationPrivacyandNetworkLifetimeMaximizationThroughTree-BasedDiversionaryRoutinginWireless SensorNetworks",*IEEE-Access*,
Vol.2,2014

[14] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-EfficientCommunicationProtocolsforWirelessMicrosensorNetworks",Proceedingsofthe33rdHawaaianInternationalConferenceonSystemsScience(HICSS),January2000.

[15] M.F.Balcan_A.Blum,A.Gupta,"ApproximateClusteringwithouttheApproximation",*Proceedingsofthetwentiethannualacm-siamsymposiumondiscretealgorithms*,pp.1068-1077,2009

[16] M. Lehsaini, H. Guyennet, and M. Feham, "CES: Cluster-based Energy-efficientSchemeforMobileWirelessSensorNetworks",*Springer-IFIPInternational Federation for Information Processing*, Vol.264; pp. 13–24,2008

[17] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, A. A. F. Loureiro,"SecLEACH–ARandomKeyDistributionSolutionforSecuringClusteredSensorNetworks",*ProceedingsoftheFifthIEEEInternationalSymposiumonNetworkComputingandApplications*,pp.145-154,2006