IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The SEAST : Scheme for Efficient Health Monitoring in Wireless Sensor Networks

R. Sivaranjani
Assistant Professor,
Department of Informtion Technology,
PSGR Krishnammal College for Women, Coimbatore, India

Abstract

Data sharing about health must now be done safely. Effective remote patient observation is essential because the majority of the population has chronic conditions including diabetes, high blood pressure, and heart problems. This enables surgeons to spot health issues as soon as feasible. This is likely due to the use of inexpensive, low-energy, calculational, and memory-intensive sensors. Transmission of health data must be energy efficient, secure, and safeguarded, which is a difficult issue. As part of the general systems incorporating WSN that should assure privacy and dependability, attention should be paid to the disruption and manipulation of healthcare data. Healthcare professionals should have access to the data so they can treat patients appropriately and suitably. The information becomes life-threatening if it is impacted. Furthermore, data should only be accessible to legitimate users. Data from sensor nodes is transferred to the Base Station for analysis in isolated environments, focusing on the end-user's access to data. There are issues to be addressed in this work to be guaranteed that the Base Station receives the accurate result

Keywords : Wireless Sensor Network, SEAST, Base Station, Cluster Head.

1. Introduction

1.1 Wireless Sensor Networks

A Wireless Sensor Network (WSN) consists of thousands of small sensors that are capable of sensing, processing signals and communicating with other sensors. The WSNs are universally used in everyday life of human beings due to their appropriateness and applicability in varied situations that include military operation, weather predicting, health observing, investigation etc., WSNs can be deployed and applied in fields wherein the human risk is high. It is also proficient in data acquisition from varied environments that involve indispensable actions to prevent the likelihood of tragedies.In data communication networks, the sensor nodes in WSN are capable of self-organizing themselves in an ad hoc manner[1]. Each sensor node includes a sensor unit, transceiver, memory, power supply and a processing unit. The sensor nodes are capable of sensing temperature, pressure and sound. The processing unit processes the incoming signal and facilitates essential actions that support forwarding of radio signals. The transceiver plays a dominant role in communicating the radio signals from the sensors that share a shared range of communication. The sensors have restrictions in terms of the range of transmission and data rate as sensors cannot communicate with other sensor nodes located afar off [2]. The communication between nodes at longer distances is made possible by multi-hop communication which conserves power. Distant environments are to be observed and the data gathered from sensors are sent to the BS thus permitting the user to gain access to the data[3].

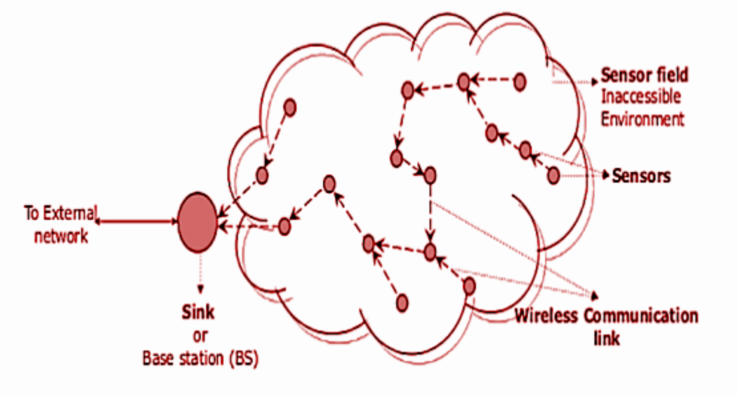


Figure-1 Model of WSN

1.2 Purpose of the work

WSNs keep the problems with energy consumption in order to extend network lifespan and make it suitable for network-based applications. To detect and collect data from the area where it is placed, the sensor nodes of WSNs incorporate smaller-sized batteries. However, it is not possible to change or renew the energy source used by sensor nodes. The sensing nodes are responsible for collecting and transferring data from the networks to the BS so that choices can be made in the future. The primary focus for determining optimal performance is thought to be energy usage. Operating and extending the life of the network. Since fluctuating energy consumption causes network segregation that eventually causes the network to become unresponsive, energy conservation and optimized use of residual energy are considered to be essential for supporting the network lifetime.

Clustering is seen as a crucial approach to energy conservation. However, CH(Cluster Head) election, which supports balancing energy with enhanced network lifetime, is the only factor that can truly determine how effective clustering algorithms are. The majority of CH election schemes are illogical and probabilistic in character. Given that they are weak in selection, the arbitrary CH election systems are proven to be suitable for dynamic networks.

Additionally, the probabilistic clustering methods enable CH selection based on the prior behavior of the sensor nodes, which may not always be accurate. Therefore, clustering strategies that choose a sizable number of cluster heads based on anticipating the current behavior of sensor nodes are essential.

1. Review of the Literature

It is difficult to reduce energy dissipation and increase the lifespan of the WSNs because the sensors are energy-dependent. Clustering has been proven to be energy-efficient because CHs handle routing and relaying. Additionally, the CHs gather the sensor data in a cluster, reducing network stress and bandwidth. There are clustering and routing methods that use less energy while extending network lifetime that may be found in the literature.

Distributed Energy-Balanced uneven Clustering (DEBUC) protocol, created by Jiang et al. (2010), combines multi-hop routing across clusters with an uneven clustering technique. The sensors are divided into uneven clusters based on the time-based competitive clustering scheme, and the CHs manage the "hot-spots" problem to save energy. It uses energy-based multi-hop routing to handle traffic between clusters, balancing the energy overhead[4].

Chamam & Pierre (2010) proposed a distributed clustering technique for CH election in which a three-way handshake is started between the sensors and their neighbours. The RE and degree of the nodes are taken into account in the proposed Energy-Efficient Cluster Formation protocol (EECF) before a node is chosen as the CH[5].

Bagci & Yazici (2010) have taken into consideration fuzzy descriptor based on the separation between sensors and BS in addition to RE. As the size of the clusters close to the BS exhibit an indeterminate decrease, this may result in uneven clustering[6].

Min et al. (2010) provide an analytical clustering model that takes the 1-hop distance and clustering angle into account. The optimal 1-hop distance and clustering angle are discovered by minimising the inter- and intra-cluster energy consumption, and from these values, the optimal incessant working hours of each CH are determined. The CHs referred to as local centres are not replaced until their constant working hours reach the ideal values, preventing the CH from being updated frequently. The connectivity is preserved and less energy is used for cluster communication as the nodes are separated into static clusters of different sizes[7].

For dynamic networks, Mitton et al. (2011) developed a stable clustering approach based on Directed Acyclic Graphs (DAG) to shorten stabilisation times and improve stability[8].

The routing algorithms can benefit from a number of biological system traits, including autonomy, self-organization, adaptivity, robustness, and scalability. A distributed clustering technique based on social colonies was put forth by Cheng et al. (2011), and it was assessed in light of a first-order radio model[9].

In order to arrange the optimal number of sinks and achieve load balancing in each sink, Xu and Liang (2011) proposed an energy-efficient routing strategy[10].

Improvements to the LEACH protocol include Hierarchical Multi-path Routing-LEACH (HMR-LEACH) (Liu & Wei 2011) and Low Energy Adaptive Clustering Hierarchy-Trust Minimum (LEACH-TM) (Wang et al 2009). They deal with inter-cluster multipath discovery and CH selection. While LEACH-TM provides several inter-cluster pathways, HMR-LEACH does not deal with multipath forwarding to send data packets to the BS[11].

The Efficient Cluster Head Selection Scheme for Data Aggregation (ECHSSDA) protocol was developed by Maraiya et al. (2011). After each round is complete, the BS determines the mean energy of the normal sensors and the RE of the current CHs in each cluster.The BS chooses the relevant CH from the regular sensors based on the energy level for the upcoming round if the CH's RE is lower than the average energy of the normal sensors.
New clusters are created after the associate CHs are chosen[12].

While sensors further away communicate to the sink via their neighbours, those closer to the sink send the available data directly. The sensors next to the washbasin undergo numerous transmissions, which puts them at risk for battery depletion. This is referred to as a hot-spot issue. Sharma and Monga (2013) suggested a method for applying ACO to optimise the location of the washbasin[13].

Ang et al. (2016) offer a study that uses insect-based groups for routing in WSNs. Ants and termites are the two sorts of insects that are considered. Simple, independent, and compliant organisms that depend on one another for survival make up insect communities. To accomplish shared objectives, they cooperate with one another. For straightforward routing scenarios, the effectiveness of the insect-based strategies is demonstrated[14].

A strategy to choose a Super-CH (SCH) from CHs based on fuzzy descriptors like RE, motion of BS, and cluster importance has been put forth by Nayak & Devulapalli (2016). The CHs are selected as the super-CHs based on the fuzzy inference engine[15].

In a multi-hop transmission proposed by Balaji et al. (2019), fuzzy logic type 1 is combined with the trust factor and distance. The nodes close to the BS and with a high trust factor are chosen to serve as the CH. By decreasing network overhead, this lengthens the life of the network[16].

Priyadarshi et al. (2018) addressed the issue of random CH selection leading to uneven power utilisation and coverage in cluster-based communication. The algorithm in the suggested method selects the CH in two stages. The CH is chosen in the first phase according to the indicated probability, and in the second phase according to the estimated durability time.The scheme provides longer network lifetime than the LEACH protocol and longer endurance time than the EBDC and AEOC algorithms, which improve network energy efficiency[17].

For efficient CH selection, Ren & Yao (2020) have taken into account the unequal energy harvesting of nodes known as Energy-Harvesting Wireless Sensor Networks (EH-WSNs).Scheduling, member, and CH nodes make up the nodes. The scheduling nodes monitor and record information on the nodes' RE, CH, and member in real time. The scheduling node selects a member as the new CH during the CH election phase based on the observed outcomes, which reduces energy use. The CHs may move to SNs, and they could save energy for data advancement. The transmission radius of nodes is also used to prevent the nodes from wasting the energy captured once the batteries are fully charged[18].

The nodes that are closest to the sink serve as interfaces to forward data to the sink in the case of a WSN with a fixed sink, using less energy in the process. The Denial-of-Sleep Attack (DoSA), in which the nodes are prevented from going to sleep, has been addressed by Fotohi & Bari (2020). A mobile sink, Firefly Algorithm (FFA) with leach, and Hopfield Neural Network (WSN-FAHN) are used to form a hybrid approach. Both the network lifespan and energy consumption are increased by doing this. To get around DoSA, FFA is utilised in clustering and two-level authentication. HNN detects the movement of the washbasin when the CH transmits data[19].

Research on energy conservation through effective routing, clustering, choosing the right Cluster Head (CH), and maintaining security in WSNs were discussed.

2. Proposed Work

The volume of medical data is rapidly growing. The issue of gathering and protecting data obtained through a WSN is still up for debate. The security and privacy of the health information must be ensured; failure to do so will have grave consequences. Additionally, energy conservation is a problem with WSN. A Secured Energy Aware (SEA) mechanism is proposed in this chapter. Only legitimate nodes establish connections to the Cluster Heads (CHs), which collect data and deliver it to the Sink or other CHs to avoid duplication. In terms of Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), Residual Energy (RE), Throughput, and Routing Overhead, the suggested method outperforms the current systems.

3.1 Methodology

The integrity of the combined and aggregated data must be guaranteed. It also emphasises ensuring credibility with the least amount of power. With the proposed Secure Energy Aware Scheme to Ensure Trust (SEAST), transmission overhead is reduced by merely sending the aggregate of the data rather than the entire amount. Each of the Base Station and CHs has a unique private key and public key. The CHs used to transmit the aggregate data to the BS, which decrypts the value acquired using the conforming key, are chosen at random.The sender's private key and the recipient's public key are used in the encryptions and decryptions. The aggregate is encoded by the BS before being sent to the CHs.The Base Station watches for disapproving votes from CHs who disagree with the fusion's outcome. The CHs that reject the total generate encoded negative votes and send them to the Base Station. The Base Station data is not recognised due to a rise in negative votes.

An energy-efficient data assurance strategy using a negative voting system is suggested in this chapter. The energy required for transmission will increase if many copies of the data are sent to the BS. Instead of sending the full collection of data gathered from the sensor nodes to the BS, the suggested technique merely sends the aggregate. Public Key (PK) cryptography is used in the suggested approach. It requires the keys listed below. As with the current methods, the CHs are picked at random to forward the accumulated data. The CH, however, sends the aggregate to the BS by encrypting it with the key "K1," which is different from the existing systems.

$$K_1 = PRI_{CH} + PUB_{BS} \qquad (3.1)$$

PRI_{CH} - Private Key of the Cluster Head

PUB_{BS} - Public Key of the Base Station

$$ENC(Text) = Text\hat{}K_1 \qquad (3.2)$$

The Base Station on receiving the encrypted text, decrypts it using the key ‘K2’, where

$$K_2 = PRI_{BS} + PUB_{CH} \qquad (3.3)$$

PRI_{BS} - Private Key of the Base Station

PUB_{CH} - Public Key of the Cluster Head

$$DEC(Text) = Text\hat{}K_2 \qquad (3.4)$$

The Base Station transmits the aggregate after encrypting it using the key ‘K2’ The Base Station waits for negative votes from the CHS that discard the aggregated data The CHs obtain the encrypted aggregate forwarded by the Base Station . They compute additional aggregate utilizing the closely accessible data and associate it with the decrypted replica of the expected aggregate. Decryption is done using the key ‘K1’ If the aggregate varies, then the CHs produce negative votes, encrypt them using ‘K1’ and pole the same to the Base Station . If the negative votes from the CHs are not sufficient, then the Base Station demands the chosen CH for the original data and receives it.

In this scheme, effectively there is no demand for resending of the entire set of accumulated data, until the arbitrarily chosen CH is malevolent. As the CH is arbitrarily chosen for data transmission, the invader will not be capable of finding the CH that is selected at a particular point of time. This reduces the susceptibility of attacks. If a malevolent CH produces negative votes to nullify the data received from CHs selected to forward the data, it will be discarded at the Base Station, as the number of negative votes from candid nodes will not be adequate to support this node (Figure 2). As a PK system is utilized, a malevolent CH cannot pole for proxy negative votes The chief merit of the proposed scheme is that there is no transmission of private keys and hence they are exposed to any node.

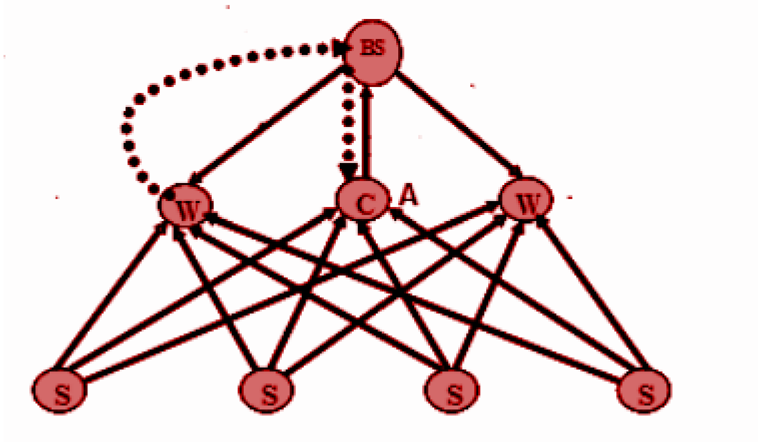


Figure-2 : Indirect Anti-Voting

A malicious node that tries to convey an illegal aggregate to the Base Station is rejected by the Base Station after receiving a number of negative votes from additional honest CHs.

Algorithm: Proposed Secure Energy Aware Scheme to ensure Trust (SEAST) Scheme (SEAST)

```
Step 1: Form a collection of nodes that act as witnesses. Let the number of
witness nodes be 'm-1'
Step 2: The BS arbitrarily selects a CH for forwarding the data.
Step 3: The BS requests for the aggregate and the chosen node transmits the
aggregate to the BS by encrypting it using the key 'K1', where K1 = PRICH +
PUBBS
Step 4: The BS on receiving the encrypted text, decrypts it using the key
'K2', where K2 = PRIBS + PUBCH
Step 5: The BS transmits the aggregate after encrypting it using the key
'K2' to the witnesses
Step 6: The CHs obtain the encrypted aggregate forwarded by the BS.
Step 7: The BS waits for negative votes from the CHS that discard the
aggregated data
Step 8: They compute additional aggregate utilizing the closely accessible
data and associate it with the decrypted replica of the expected aggregate.
Decryption is done using the key 'K1
Step 9: If the aggregate varies, then the CHs produce negative votes,
encrypt them using 'K1' and pole the same to the BS.
Step 10: If the negative votes from the CHs are not sufficient, then the BS
demands the chosen CH for the original data and receives it.
```

3.2 Results and Discussion

The NS2 is used to implement the suggested system. At a Base Station, the sensor nodes are arranged like a deep-rooted tree. The CHs acquired information from sensor nodes. In Figure 3 and 4, the communication overhead is drastically decreased.

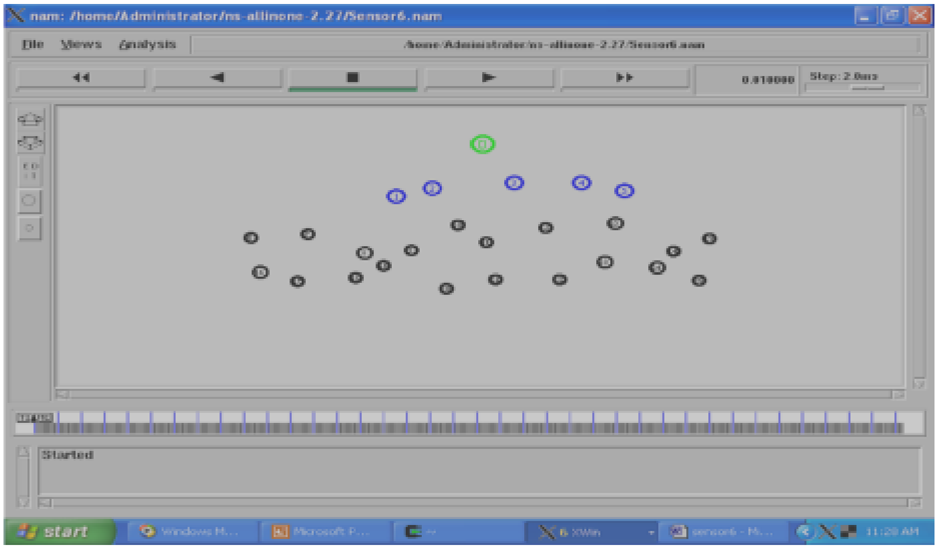
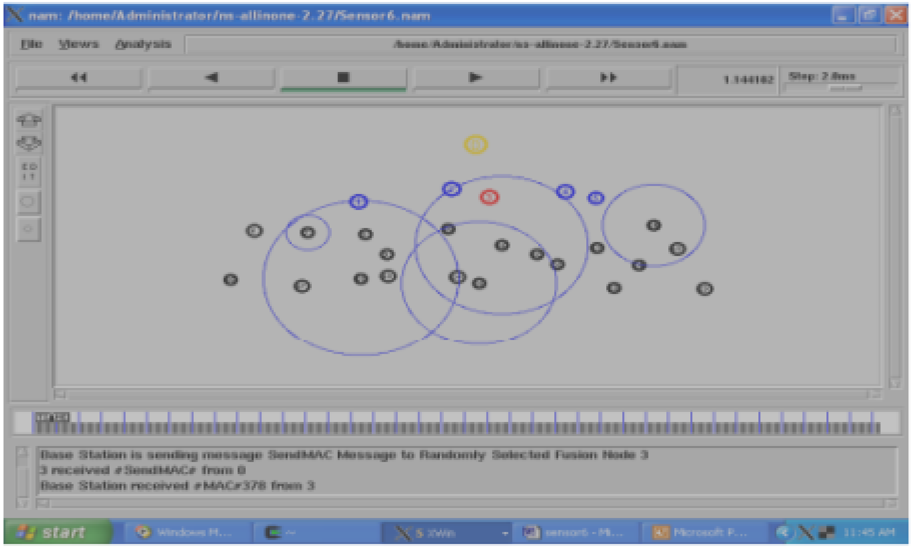

nam: /home/Administrator/ns-allinone-2.27/Sensor6.nam
File
Views
Analysis
/home/Administrator/ns-allinone-2.27/Sensor6.nam
0.010000
Step: 2.0ms
Started
start

Figure-3: Node Deployment


nam: /home/Administrator/ns-allinone-2.27/Sensor6.nam
File
Views
Analysis
/home/Administrator/ns-allinone-2.27/Sensor6.nam
1.144182
Step: 2.0ms
start
Windows M...
5 Xwin
sensor6 - Mi...
Microsoft P...
11:45 AM

```
Base Station is sending message SendMAC Message to Randomly Selected Fusion Node 3
3 received #SendMAC# from 0
Base Station received #MAC#378 from 3
```

Figure-4: Communication between the BS and the randomly selected CH

Figure 5 compares the Packet Delivery Ratio (PDR) of the proposed Secure Energy Aware Scheme to Ensure Trust (SEAST) Scheme with that of the Witness based Scheme (WS), Voting based Scheme (VS), and other existing schemes. In comparison to the current WS and VS, it can be noted that the suggested scheme gives 29% and 15.8% increased PDR.

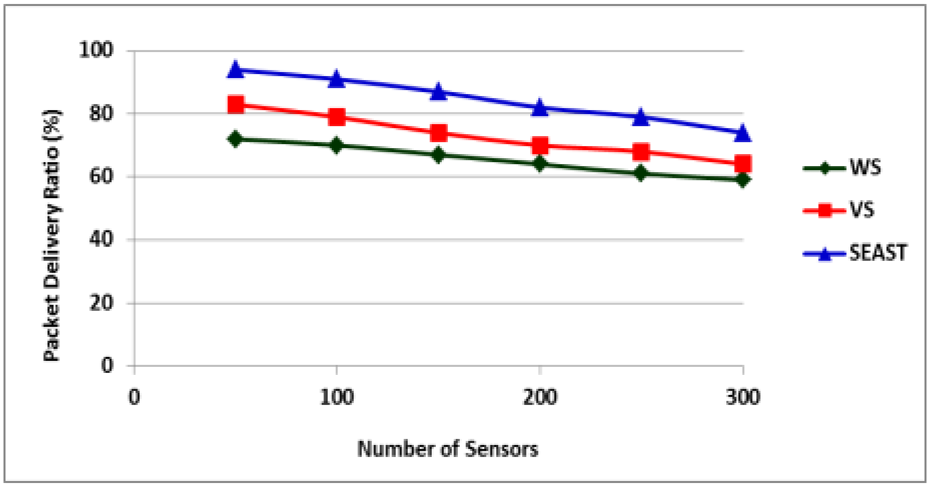


Figure-5: Packet Delivery Ratio of the Proposed SEAST Scheme

Figure 3.6 compares the proposed SEAST scheme's throughput to that of the current witness(WS) and voting(VS) schemes. In comparison to the current method by comparing existing witness and voting schemes, it can be noted that the suggested system delivers improvements in Throughput of 47.7% and 18%.

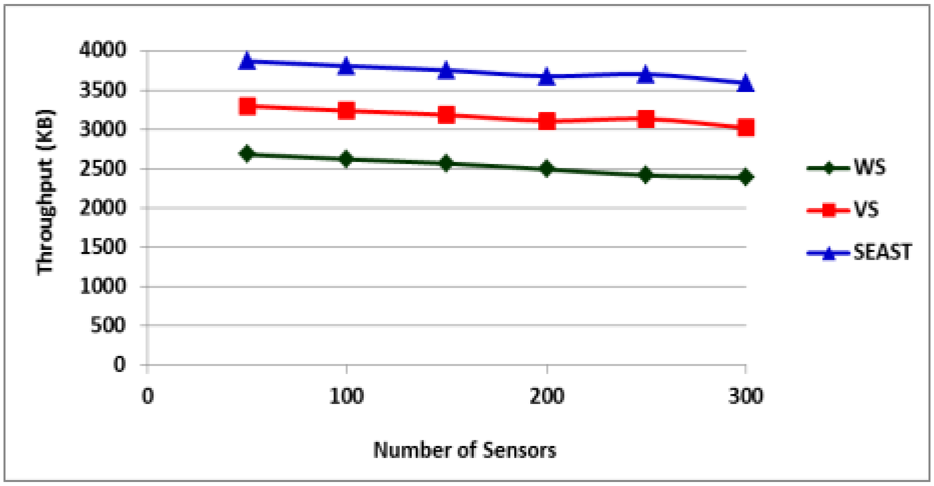


Figure-6: Throughput of the Proposed SEAST Scheme

Figure 3.7 compares the Routing Overhead of the proposed SEAST scheme with that of the current WS and VS. When compared to the current WS and VS, it can be noted that the suggested method requires 46.8% and 23.7% reduced routing overhead.

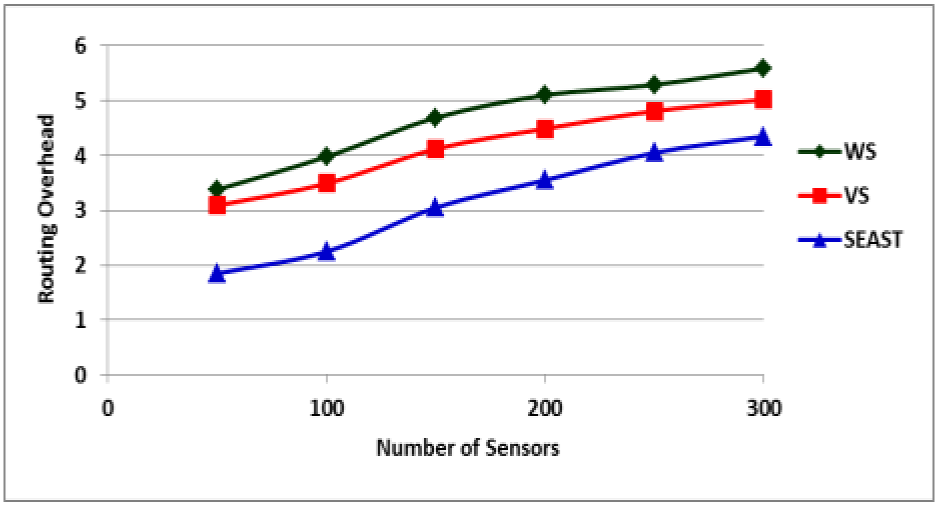


Figure-7: Routing Overhead of the Proposed SEAST Scheme

Figure-8, the Packet Loss Ratio (PLR) of the existing WS and VS and the proposed SEAST scheme are seen. It is seen that the proposed scheme involves 25.8% and 12.1% improved PLR when compared to the existing WS and VS.

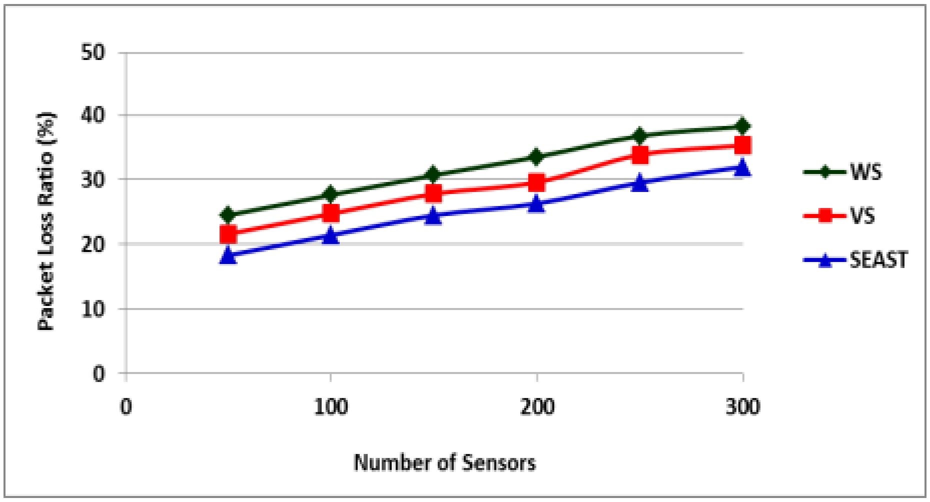


Figure -8: Packet Loss Ratio of the Proposed SEAST Scheme

It is found that the propounded SEAST scheme involves reduced Routing overhead and Packet Loss Ratio (PLR) with better Packet Delivery Ratio (PDR), Residual Energy and Throughput.

3. Conclusion

In the proposed Secure Energy Aware Scheme to assure Trust (SEAST) mechanism, the BS only collects the fusion data from the randomly selected CH and the negative votes from the witness nodes when there are insufficient negative votes available. Comparing the proposed technique to the current witness and voting-based schemes, it is clear that it has less overhead. As the data is sent as a hash value for approval by the BS and agreement by the witnesses, the power required for the scheme is decreased. Data is only transmitted when the BS requests it. Furthermore, only negative votes are sent along. Each node is given a set of keys—a private key and a public key—to fend off attacks. In the network, the keys are not forwarded. Key attacks and key exploitation are avoided. The suggested method prevents re-transmission and allows safe data passing.

References

1. Li, XJ, & Chong, PHJ 2010, ‘Performance analysis of multihop cellular network with fixed channel assignment’, Journal of Wireless Networks, vol. 16, no. 2, pp. 511-526.
2. Sohraby, K, Minoli, D, & Znati, T 2007, ‘Wireless sensor networks: technology, protocols, and applications’, John Wiley & Sons, pp. 1-307.
3. Raghunathan, V, Kansal, A, Hsu, J, Friedman, J, & Srivastava, M 2005, ‘Design considerations for solar energy harvesting wireless embedded systems’, Proceedings of the fourth IEEE International symposium on Information processing in sensor networks, pp. 64.
4. Jiang, CJ, Shi, WR, & TANG, XL 2010, ‘Energy-balanced unequal clustering protocol for wireless sensor networks’, Journal of China Universities of Posts and Telecommunications, vol. 17, no. 4, pp. 94-99.
5. . Chamam, A, & Pierre, S 2010, ‘A distributed energy-efficient clustering protocol for wireless sensor networks’, Journal of Computers & Electrical Engineering, vol. 36, no. 2, pp. 303-312
6. Bagci, H, & Yazici, A 2010, ‘An energy aware fuzzy unequal clustering algorithm for wireless sensor networks’, Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ), pp. 1-8.
7. Min, X, Wei-Ren, S, Chang-Jiang, J, & Ying, Z 2010, ‘Energy efficient clustering algorithm for maximizing lifetime of wireless sensor networks’, AEU-International Journal of Electronics and Communications, vol. 64, no. 4, pp. 289-298.
8. Mitton, N, Sericola, B, Tixeuil, S, Fleury, E, & Lassous, IG 2011, ‘Self-stabilization in Self-organized Wireless Multihop Networks?’, Ad Hoc & Sensor Wireless Networks, vol. 11, no. 1-2, pp. 1-34

9. Cheng, CT, Chi, KT, & Lau, FC 2011, ‘A clustering algorithm for wireless sensor networks based on social insect colonies’, Journal of IEEE sensors, vol. 11, no. 3, pp.711-721.
10. Xu, X, & Liang, W 2011, ‘Placing optimal number of sinks in sensor networks for network lifetime maximization’, Proceedings of the IEEE International Conference on Communications (ICC), pp. 1-6.
11. Wang, W, Du, F, & Xu, Q 2009, ‘An improvement of LEACH routing protocol based on trust for wireless sensor networks’, Proceedings of the fifth International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4
12. Liu, G, & Wei, C 2011, ‘A new multi-path routing protocol based on cluster for underwater acoustic sensor networks’, Proceedings of the IEEE International Conference on Multimedia Technology (ICMT), pp. 91-94.
13. Sharma, K, & Monga, H 2013, ‘Improved termite hill routing protocol using ACO WSN’, Proceedings of the International Conference on Computer Science and Engineering (ICSEC), pp. 365-370
14. Ang, LM, Seng, KP, & Zungeru, AM 2016, ‘Utilizing Social Insect-Based Communities for Routing in Network-based Sensor Systems’, Journal of Swarm Intelligence Research, vol.7, no. 4, pp. 52-70.
15. Nayak, P, & Devulapalli, A 2016, ‘A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime’, IEEE Journal on Sensors, vol. 16, no. 1, pp. 137-144.
16. Balaji, S., Julie, E. G., & Robinson, Y. H. (2019). Development of fuzzy based energy efficient cluster routing protocol to increase the lifetime of wireless sensor networks. Mobile Networks and Applications, 24(2), 394-406.
17. Priyadarshi, R., Soni, S. K., & Nath, V. (2018). Energy efficient cluster head formation in wireless sensor network. Microsystem Technologies, 24(12), 4775-4784.
18. Ren, Q., & Yao, G. (2020). An energy-efficient cluster head selection scheme for energy-harvesting wireless sensor networks. Sensors, 20(1), 187.
19. Fotohi, R., & Bari, S. F. (2020). A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. The Journal of Supercomputing, 1-2