International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7628
***Article Received:** 02 June 2023 **Revised:** 30 July 2023 **Accepted:** 12 August 2023*

SRP-HEE: A Modified Stateless Routing Protocol based on Homomorphic Energy based Encryption for Wireless Sensor Network

Vemula Kesava Kumar[1], Prof P Suresh Varma[2]
[1]Depertment of Computer Science and Engineering
Aya Adikavi Nannaya Uniersity
Rajamahendravaram,India
vemulakesav58@gmail.com
[2]Depertment of Computer Science and Engineering
Aya Adikavi Nannaya Uniersity
Rajamahendravaram,India
sureshvarmap@gmail.com

Abstract— Due to the wireless nature, the sensors node data are prone to location privacy of source and classification of the packet by unauthorized parties. Data encryption is one of the most effective ways to thwart unauthorized access to the data and trace information. Traditional wireless network security solutions are not viable for WSNs In this paper, a novel distributed forward aware factor based heuristics towards generating greedy routing using stateless routing is SRP-HEE for wireless sensor network. The model employs the homomorphic Energy based encryption technique. Energy based Encryption model is devoted as homomorphic mechanism due to their less computational complexity. Additionally, privacy constraint becoming a critical issue in the wireless sensor networks (WSNs) because sensor nodes are generally prone to attacks which deplete energy quickly as it is exposed to mobile sink frequently for data transmission. Through inclusion of the Forward aware factor on the Greedy routing strategies, it is possible to eliminate the attacking node which is depleting the energy of the source node. Heuristic conditions are used for optimizing the sampling rate and battery level for tackling the battery capacity constraints of the wireless sensor nodes. The Node characteristics of the propagating node have been analysed utilizing kalman filter and linear regression. The cooperative caching of the network information will enable to handle the fault condition by changing the privacy level of the network. The Simulation results demonstrate that SRP-HEE model outperforms existing technique on basis of Latency, Packet Delivery Ratio, Network Overhead, and Energy Utilization of nodes.

Keywords- Wireless Sensor Network, Location Privacy Preserving, Forward Aware Factor Fault Tolerance, Energy Based Homomorphism Encryption, Packet Classification Attack.

I. INTRODUCTION

Wireless sensor networks face difficult challenges include node replication, node failure, packet loss, and packet alteration by an attacker. In order to increase the data transfer rate in a wireless sensor network and therefore reach a high throughput level, several strategies have been developed to prevent or accept such assaults, but very few of them can accurately and efficiently determine the network's severity [1]. Moreover, data categorization attacks may easily compromise Wireless Sensor Networks. For WSNs to be widely used, especially for mission-critical jobs, robust protective measures against such attacks must be developed [2]. Since the sender and the receiver of a message have to share a secret key, symmetric-key based approaches have the disadvantages of requiring complicated key management, being unable to scale, and being vulnerable to attacks involving a large number of compromised nodes. As part of this work, we built energy-based homomorphism encryption and distributed forward-aware factor-based greedy routing. SRP-HEE measures to protect against Sybil attack, distributed denial of service assault, and data categorization attack [3]. The Stateless protocol enables concurrent data collection from several mobile devices. When a node's energy supply runs out, the quality of its sensors and the network as a whole suffer. Keys for energy-based homomorphism encryption are generated, encrypted, and decrypted according to the energy state of the data being protected. Recent work on massive sensor networks has shown some very promising findings. These interconnected systems may serve as the backbone of many different kinds of intelligent settings, including hospitals, battlefields, earthquake response systems, and classrooms. However, despite the wide variety of possible uses, they all share the need of a reliable and effective routing protocol. The primary purpose of sensor networks is to transmit data. We identify three distinct communication patterns that contribute to data delivery in these networks. First, it often occurs that a node in a network spots suspicious behaviour that must be sent to the network's central hub. Unicast describes this method of transmission. In another option, a base station may send a command or query to a specific region inside the sensor networks. It might, for instance, order all lights in a certain area to come on, or it could ask all sensors near a damaged nuclear facility to transmit radiation levels. An alternative routing service is motivated by this kind of communication since a route's final destination may not be a node but rather a region. This method is referred to as area-multicast. As a final point, given that sensors often detect highly redundant information, it may sometimes be enough to have any node in a region react. An area-anycast routing service is one that has this capacity built in.

As you can see, SRP-HEE offers all three forms of communication. Since sensor networks interact with the actual environment, real-time communication requirements are typically essential. For example, in surveillance systems, tracking quality is negatively impacted by communication lags between the sensing and acting loops. Results for sensor networks that meet real-time needs are few at present. In this research, we present SRP-HEE, a protocol for large-scale sensor networks that enables soft real-time communication through feedback control and stateless algorithms. Five different ad hoc routing protocols, including DSR [5], AODV [10], GF [13], and two scaled-down variants of SRP-HEE, are compared to SRP-HEE in our simulation using GloMoSim [15]. The findings reveal that SRP-HEE 1) decreases the amount of time that packets spend waiting between hops, 2) responds to temporary congestion in the most reliable way, and 3) manages voids [6] effectively with little control overhead. Moreover, we deploy SRP-HEE on the Berkeley swarm of micro beacons [4]. The findings demonstrate that SRP-HEE aids in balancing the traffic load to lengthen the lifespan of the system.

The remainder of this paper is organized as follows: In Section 2, the literature review on mobile sink scheduling framework towards energy harvesting and throughput maximization is provided. Details of SRP-HEE framework are given in Section 3. The simulation results and performance evaluation of SRP-HEE framework are presented in Section 4. The paper is concluded in Section 5 with final remarks and future research directions.

II. STATE OF THE ART

Numerous routing protocols are available for use in wireless ad hoc networks. A subset of these types of networks, sensor networks have their own unique set of parameters. There is greater emphasis on physical location than on node IDs in sensor networks. A tracking app, for instance, is only concerned with the target's location and not the node ID that is reporting it. This kind of location awareness is crucial in sensor networks because it gives the collected data context. Thus, location-aware routing should be used as a matter of course. It has been suggested that we use a collection of location-based routing algorithms. To get around these gaps, Finn [2] developed a greedy geographical forwarding mechanism with restricted flooding. Karp and Kung's GPSR [6] makes advantage of perimeter forwarding to bypass gaps in coverage. GEDIR [13] ensures distribution without any possible loops by using a geographically dispersed network. By limiting routing packet flooding in a certain "request zone," LAR [7] by Young-Bae Ko improves the efficiency of on-demand routing algorithms.

For more precise routing choices, SPEED additionally takes into account the user's current location. The primary focus of earlier location-based routing protocols was not on handling congestion or providing a soft real-time communication service; these are two of SPEED's primary objectives. As an added bonus, SPEED offers a means to deal with gaps apart from methods based on planar graph traversal [6] and restricted floods [16]. There have been many proposals for real-time protocols in sensor networks. To ensure that real-time UDP data may continue to flow, SWAN [1] employs MAC layer feedback information to control the transmission rate of background TCP traffic. Prioritizing real-time traffic using velocity monotonic scheduling and enforcing it via a distinct MAC Layer is the focus of RAP [9]. To ensure that nodes of varying distances from the base station are treated equally, Woo and Culler [14] devised an adaptive MAC layer rate control. These algorithms are effective because they each degrade traffic in a certain area. However, long-term congestion requires aid with routing to shift traffic away from any hotspot, and this kind of local MAC layer adaption cannot do that. For such problems, SPEED offers an adaption strategy that combines the MAC and network layers. As far as we're aware, there isn't a routing method that targets sensor networks that is designed to give soft real-time assurances. AODV [10] and DSR [5] are examples of reactive routing algorithms that only keep routing information for the presently visited destinations. A route discovery procedure is initiated if an existing path cannot be used to reach a new destination. Delays caused by route finding broadcasts may add up quickly in a sensor network with a wide area of coverage. Because of this drawback, on-demand algorithms are not optimal for use in time-sensitive contexts[17,18].

***Article Received:** 02 June 2023 **Revised:** 30 July 2023 **Accepted:** 12 August 2023*

III. STATELESS ROUTING PROTOCOL BASED ON HOMOMORPHIC ENERGY BASED ENCRYPTION- (SRP-HEE)

The architecture and framework of the system are explained, which consists of mobile sinks and some stationary sensor nodes to set up greedy routing for energy conscious factor towards data forwarding. Sensing data, including location and time stamps, may be gathered with the use of a mobile sink.

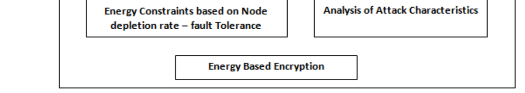
3.1. Wireless Sensor Network Model

Nodes in a Wireless Sensor Network are scattered over the network at random. When first set up, nodes often have enhanced sensing capabilities and processing power. Power for the sensor node comes from rechargeable batteries. High data traffic and interference in the network cause each node to gradually run out of energy after deployment [20]. We model an N-node, battery-operated sensing system, and deploy it throughout a 2-dimensional sensing region. It's used to keep an eye on that specific setting [19]. Having a model that works in both directions is essential for manipulating a sensor.

3.1.1 Localization of Mobile Sink

Along the route determined by the demand constraint, a mobile sink is modelled with a large data buffer, which it uses to gather data from the nodes within a single-hop or multiple-hop transmission range. The time it takes a sink to make a complete circuit of its designated course is broken up into discrete intervals [10]. The sink may move along the route at a constant speed vm or alter its velocity at predetermined intervals along the trajectory, depending on the circumstance.

The node's location inside the sensing area, as recorded in the routing table, is determined using a localization algorithm. To alleviate stress on the network and power shortages, each Node has the option to charge its own battery. The energy for sensor nodes is replenished at their base station through wireless charging technology.



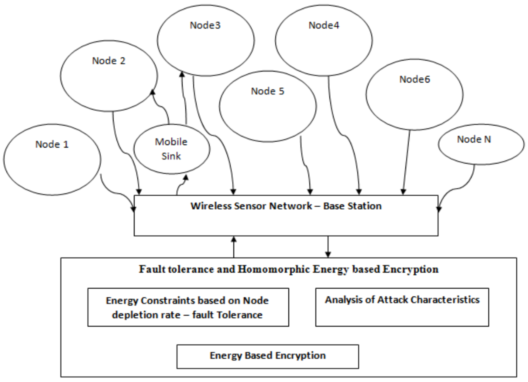

Node 1
Node 2
Node3
Node4
Node 5
Node6
Node N
Mobile Sink
Wireless Sensor Network – Base Station
Fault tolerance and Homomorphic Energy based Encryption
Energy Constraints based on Node depletion rate – fault Tolerance
Analysis of Attack Characteristics
Energy Based Encryption

Figure 1: Architecture of the SRP-HEE model

The mobile charger is both economical and adaptable to changes in the network's structure. When the charger is in a mobile configuration, it is attached to a moving vehicle or robot, whose speed might vary. And when used in tandem with a mobile base station, the mobile charger may assist reduce data collecting delays and energy spikes caused by heavy network use. Mobility of the charger is often restricted in terms of both time and location while charging a mobile device. It's been modelled to follow the routes we've set out for it [21]. Figure 1 depicts the overall design. The charge's patrolling cycle is a unit of measurement for its travel time. It is also responsible for calculating the speeds and accelerations of the sensors.

3.2. Forward Aware Factor Constraints

In this Module, we build a model using information about energy consumption and data or load usage at the forwarding node. Message transmission from the source node transmits data to the cluster head, which then forwards it to the destination node (Sink). Here are some explanations and definitions:

- All sensor nodes are identical and have little processing, transmission, and storage potential. Sensor nodes have finite amounts of energy, and after they've used it all up, they're dead. There is, however, the option to include the sink node's energy. After being set, the locations of the nodes and sink remain static, and a node cannot determine its precise location using just its internal sensors[22].

It's possible for nodes to adjust the amount of power being sent to the receiver according on how far away they are. A message from the sink node may be sent out to all of the sensors in the area. The intensity of the received signal may be used to estimate how far away the signal's origin is. Central nodes within regions are not predetermined, but rather emerge as the network structure develops. When compared to their adjacent nodes, the number and strength of connections at pivotal nodes is much greater. Information volume grows exponentially as the number of nodes increases.

According to this SRP-HEE layout, the connectivity is reflected in the edge weight. Most network data communication prioritizes a local connection. Data transmission similarly prioritizes low-load links when the size of the data being sent makes the communication channel busy. When the residual energy of and is high enough and powerful enough for data transmission, edge weight is heavily influenced by energy. In order to gather static data and identify events, R-FAF is implemented in the wide-area WSN. The first method considers the forwarding efficiency distribution (FED) of all potential next-hop nodes, or their capacity to transfer data [23]. The second method takes into account the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7628
***Article Received:** 02 June 2023 **Revised:** 30 July 2023 **Accepted:** 12 August 2023*

transmit link's weight, which may then be utilized to choose the next-hop node. The routing algorithm based on FAF is able to take into account a wide range of elements and provide a more energy-balanced solution since the definition of the weight of edge takes into account things like the energy, length, and load of individual nodes [24].

Algorithm 1: The routing algorithm of Forward aware factor for data Communication

- Identify the node and all of its potential successors. It is necessary to first ascertain the set of all the nodes that have edges, which signifies connection quality, and use this value as the communication radius.
- Determine the set of all potential next-hop nodes and the furthest node, and then choose the ones that are closer to Sink than they are to themselves.
- To do this, you need to find out the end of every node that may be the next hop. Input the maximum distance between the FTA and Sink nodes.
- Determine the relative importance of each potential next-hop node by calculating their respective strengths. Data transmission nodes that use a lot of power should be disconnected.
- For each node, determine its edge weight by multiplying its weight by (18).
- Determine the Forward Accuracy Factor (FAF) for each conceivable transmit connection. Select the next hop node based on its proximity and other spatial considerations.

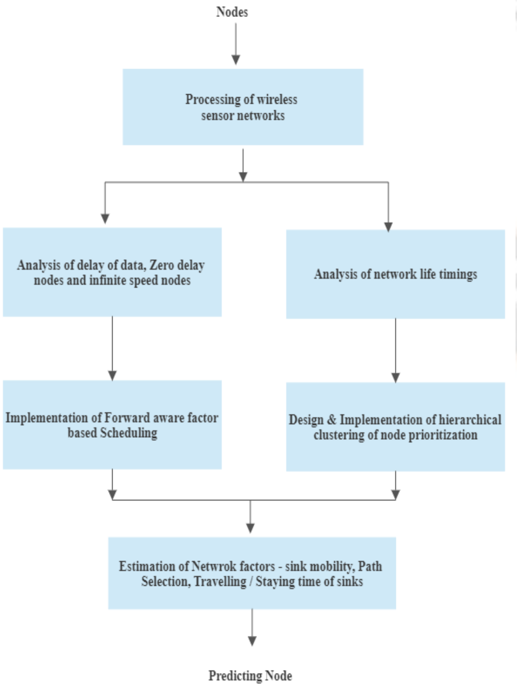

Nodes
Processing of wireless sensor networks
Analysis of delay of data, Zero delay nodes and infinite speed nodes
Analysis of network life timings
Implementation of Forward aware factor based Scheduling
Design & Implementation of hierarchical clustering of node prioritization
Estimation of Netwrok factors - sink mobility, Path Selection, Travelling / Staying time of sinks
Predicting Node

Figure 2: Flowchart of Forward Aware Factor Constraint towards Location Security

Algorithm 2: Energy Aware Factor based Location Security

Input: Sensed Multimedia Data from self & neighbour nodes

Output: Reliable Energy efficient Route selections

Variables: Link delivery ratios estimates, packets residual energy, thresholds, received signal strengths

```
Let $REL_{diffth}$be Predicted Reliability Difference Threshold
Let $E_{diffth}$ be Energy Difference Threshold
Let $R_a$ be best ReliableTXRoute()
Let $R_b$be best EnergyRoute()
$REL_{diff}$ be $R_b$. REL – $R_a$.REL
$E_{diff}$ be $R_b$.Energy – $R_a$.Energy
start
when $R_a$=$R_b$ then
    selected Route will be $R_a$
    end here
else continue
when $REL_{diff} \geq REL_{diffth}$ then
    selected Route will be $R_b$
    end here
else continue
    when$E_{diff} < E_{diffth}$then
        Set$R_b$as invalid path and remove from list
        Repeat above steps with next reliable route
    endhere
endhere
```

Reliable TX Route Estimation:

For each route R_{score} is calculated at time T_i as

$$R_{score_{Ti}} = \sum_{i=0}^{N\_hops} Reliable_{TXi} * RSSI_{norm}$$

where,

$Reliable_{TXi}$is Link Reliability for each link, calculated as

$$Reliable_{TXi} = \frac{1}{(d_f * d_r)}$$

$d_f$is links' forwardpacket delivery ratio

$d_r$islinks' reverse packet delivery ratio

N_hops is the number of hops in that path

DOI: https://doi.org/10.17762/ijritcc.v11i10s.7628
***Article Received:** 02 June 2023 **Revised:** 30 July 2023 **Accepted:** 12 August 2023*

$RSSI_{norm}$ is normalized RSSI, calculated as

$RSSI_{norm}=\frac{\mathrm{RSSI_{mean}}}{\mathrm{RSSI_{max}}}$

$RSSI_{mean}$is mean RSSI of all packets on that path

$RSSI_{max}$is max RSSI of all packets on that path

Predicted Reliability is calculated using drift method as

$$\mathrm{R}_{\mathrm{score}_{Ti+h}} = \mathrm{R}_{\mathrm{score}_{Ti}} + \left(h * \frac{\mathrm{R}_{\mathrm{score}_{Ti}} - \mathrm{R}_{\mathrm{score}_1}}{T_i - 1}\right)$$

where,

$\mathrm{R}_{\mathrm{score}_{Ti+h}}$ispredicted reliability score (at time T_{i+h})

$\mathrm{R}_{\mathrm{score}_{Ti}}$is last known reliability score (at time T_i)

$\mathrm{R}_{\mathrm{score}_1}$is initial reliability score(at time, T=1)

h is the prediction duration and T_i is current time

3.3. Data Classification attack model

A data classification attack is a sort of sensor information retrieval assault that is undertaken by an adversary without authorization. In order to collect data, malicious nodes set up attacks on multiple gateways via a series of intermediate nodes. In addition, it prevents the mobile sink from receiving a charge. Features are retrieved from attributes of nodes using Kalman Filter and Regression Linear

Node information with five features through the help of mobile agent in each sample such as, y1, y2, y3, y4 and y5, are extracted by the equation as follows:

$$y_k = \frac{c^k}{\max\limits_{i=1}^{5}\left(c^i\right)}$$

where k=1, 2,. . ., 5,

c^k – Absolute sample of the replica nodes.

(1) The absolute information is calculated for different samples given by,

$$Y_6=\log_{10}\left(\max_{m=1}^{5} c^m\right)$$

Thus, attack features are extracted, gives a feature vector

$Y = [y1\ y2\ y3\ y4\ y5\ y6]^T$ for attack diagnosis by hierarchical clustering logic and gives the complete description about the classified attack types of wireless sensor Network.

A soft-margin of attack features is determined and trained by solving a quadratic programming problem,

x is the node features

Minimize (with respect to **x**)

Quadratic function related to node replication features

$F(x) = x_{tQ}x+ c_{tX}$

Ct is the cluster attack weight

${}_{Q}x$ = level of fails

Algorithm 3: Classification of the Nodes using Constraints and Characteristics

Input: $\alpha = \{T=\sum t_k\}$

Output: $\alpha^{|} = \{T^{|}\}$

- Create two distinct types of nodes, attack nodes and regular nodes, and link them via a network.
  - Use an energy-balancing strategy on every regular node to determine the best way to the sink and any alternative paths.
  - Disable the attack node for a timed duration, or remove it altogether; alternatively, employ it for experimental purposes.
  - Determine the total amount of time spent in each node, beginning with the source node, and ending with the final node.

- If you want your data to go where it has to go as quickly as possible, you should use the route with the longest possible network lifespan.
- Ascertain the Best Destinations for Data Transfer by Computing Linear Trajectories, Boundary Trajectories, and Arbitrary Trajectories.

Begin

For k=1: k<m: k++ do

Where k = network life time

M is the mobility of the mobile Sink

d. Energy based Homomorphism Encryption

In this part, we use the node's energy computation throughout the cipher text generation cycle to identify the energy based homomorphic encryption model. The encrypted text is generated according to the number of nodes and their energy constraints. Among the steps involved in homomorphic encryption are the ones below.

- Key generation
  Key is considered is odd number p ξ $[2^{n-1}, 2^n]$

- Encryption
  Encrypt (p,m)
  M ξ [0, 1]
  M is the data
  Cipher text = C
  C= pq+2r+m
  Q and r is energy values of the intermediate node n2, n3.
  $C_w \geq C_{max}$, $C_w = C_w + 1$
  Where C_w is cipher text generated file on node n
- Decryption
  Decrypt (p,c)
  M=(C mod p)mod2

IV. RESULTS AND DISCUSSION

Currently, we are evaluating SRP-performance HEE's in the directing test. Two methods, including SRP-HEE, are compared and contrasted. Subterranean insect settlement calculations are a mix of fanciful logic and one of nature's own. The suggested technique combines both hard scientific calculations and more ethereal justifications. The cuckoo search computation, insect settlement, and the papers mentioned here are all used in conjunction with other forms of directional research. An essay that used a scientific calculation based on the behaviour of insects to compare the efficiency and feasibility of the underground bug state computation with the cuckoo's calculation. Results are evaluated based on how well AESP-VANET is designed and implemented. Multiple widely used protocols, including Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Control Routing (DSR), Dynamic Manet on Demand (DYMO) protocol, An Enhanced Hybrid Routing Protocol in Vehicular Ad-hoc Networks (TIHOO), and Temporally ordered routing algorithm, are simulated and compared to one another (TORA). Throughput, direction overhead, bundle conveyance percentage, package misplacement percentage, and total time required to complete a shipment are all evaluated.

The packet delivery rate (PDR) is defined as the ratio of the number of packets successfully delivered to the destination hubs to the total number of packets sent from the source hub. This is shown graphically in Figure 3 for Packet Delivery Ratio.

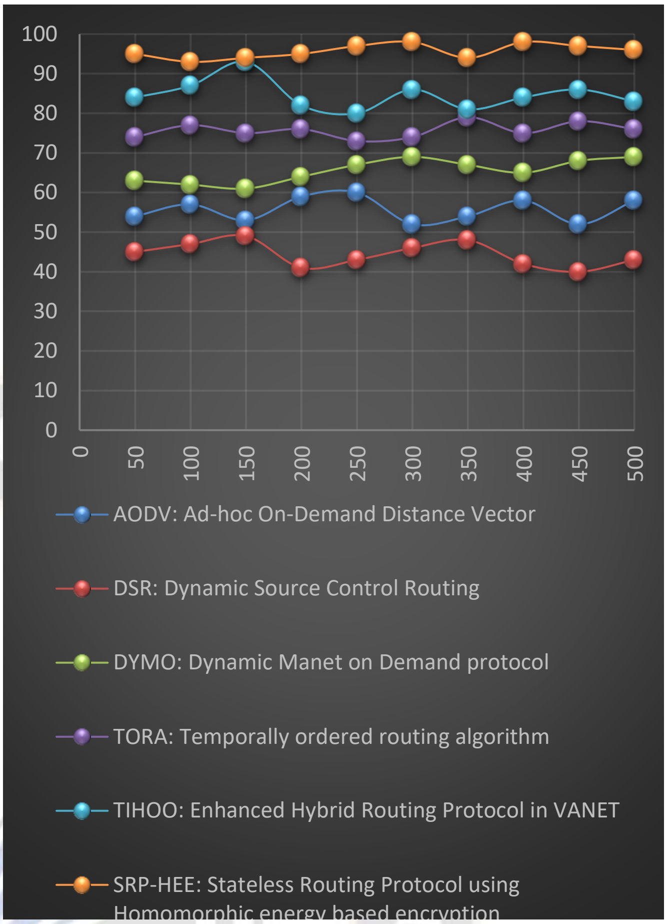


Figure 3. Graphical representation of Packet Delivery Ratio

End-to-end latency is another important metric for a network (EED). The source sends packets to the destination with a typical delay in between each one. This is known as the end-to-end delay or just the delay. End-to-end delay is measured in milliseconds and accounts for every conceivable delay that might occur during transit. This includes route reveal, information acquisition, and lining delays, as well as delays caused by handling at intermediate hubs. The End-to-end latency for AODV, DSR, DYMO, TORA, TIHO, and AESP-VANET is graphically shown in Figure 4. Cuckoo metaheuristic computation used to SRP-HEE facilitated the selection of the optimal path in less time than the other two methods. Unlike AODV, whose deadline has been significantly pushed back due to ACO. The AESP has a high rate of mixing and can identify the best path quickly.

DOI: https://doi.org/10.17762/ijritcc.v11i10s.7628
Article Received: *02 June 2023* ***Revised:*** *30 July 2023* ***Accepted:*** *12 August 2023*

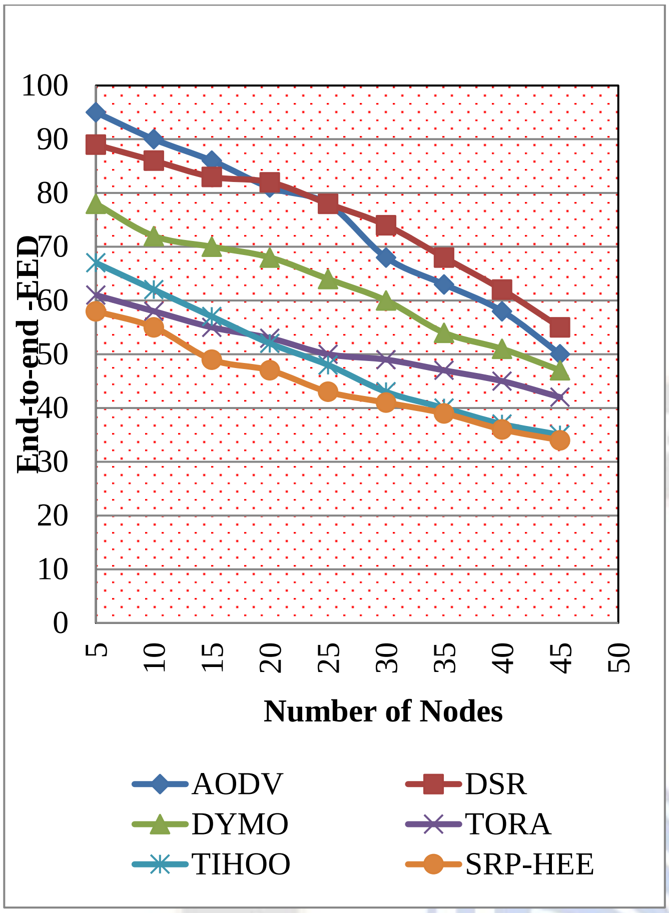


Figure 4. Graphical representation of End-to-end delay

Throughput is graphically shown in Figure 5. Check out our detailed throughput comparison of the widely-used routing protocols AODV, DSR, DYMO, TORA, TIHOO, and SRP-HEE. Out all the protocols studied, SRP-HEE was shown to be the most effective. Computer science techniques used to SRP-HEE have sped up convergence, however the process of selecting the optimum route still takes time and makes use of inefficient methods like Ant colony optimization. In addition to speeding up the selection of the ideal route and increasing the proposed protocol's throughput, this metaheuristic method also requires less parametric setting during the implementation phase. The AESP has been shown to be superior than other conferences, according to recreation-based research. When compared to other metaheuristic calculations, SRP-CS HEE's calculation allows for a faster combination and fewer parametric design requests during the use stage, since it uses a heuristic based on ant colony optimization to determine the optimal path.

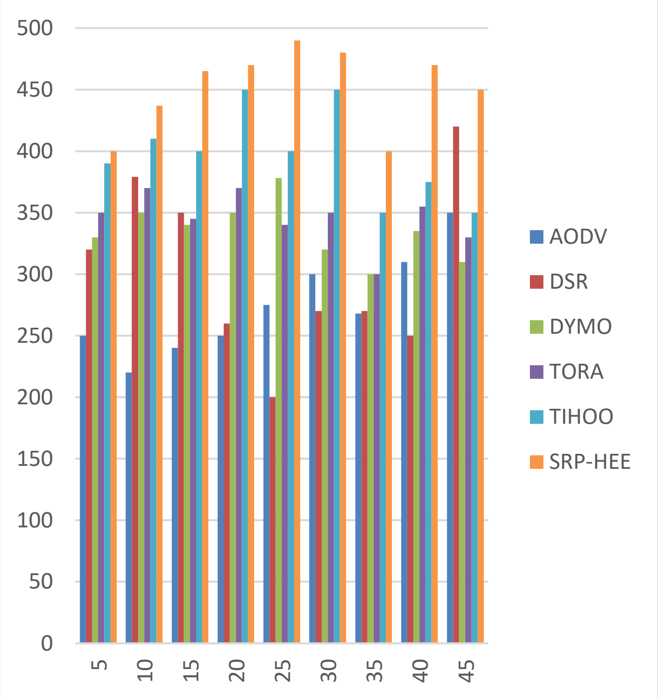


Figure 5. Graphical representation of Throughput

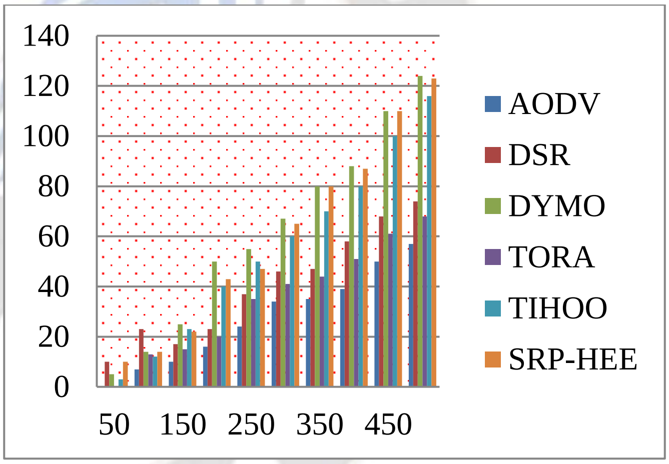


Figure 6. Graphical representation of Routing overhead

The routing overhead is graphically shown in Figure 6. The routing overhead of many different algorithms, including AODV, DSR, DYMO, TORA, TIHOO, and SRP-HEE, are compared and contrasted. In the AESP-VANET, packets for regulating the course load are broadcast. In other computations algorithms, executing this step generates growth of framework overhead, but disclosure leads to a regulated approach. Costs associated with the system's growth are incurred as a result of the suggested technique. As a result of storing all of the data from the whole province and then using a metaheuristic computation inspired by ant colonies, we have achieved this result

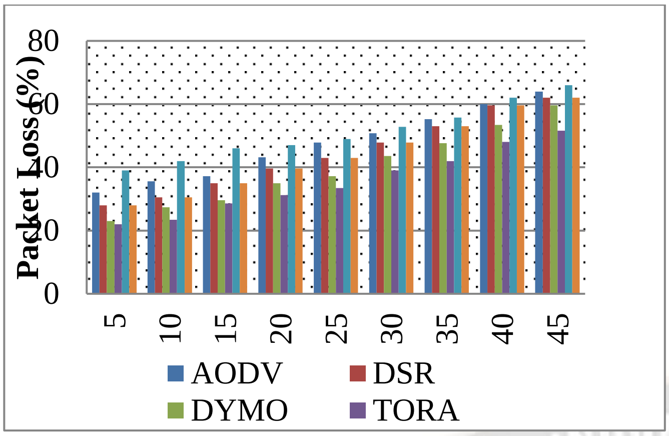


Figure 7. Graphical representation of Packet Loss

The visual depiction of packet loss is shown in Figure 10. Methods are compared to one another. Interface dissatisfaction, bundle crashes, inadequate data transfer, and excessive support overhead all contribute to packet data loss. According to characteristics such as course longevity and its unchanging quality, the SRP-wellness HEE's capacity is organized by general computation. Applying these factors helps pinpoint the progressive steady with fewer connection disappointments, which affects packet misfortunes. A less obstructed path with extraordinarily high viability is established as the basis for the easily available support representation.

V. CONCLUSION

We designed and simulated the Distributed Energy Aware Factor based greedy routing through stateless routing protocol in the Wireless Sensor Networks. It is proven to be a better network infrastructure by providing the location privacy and energy security on the node for fault free data transmission. The protocol reduces the packet loss with reference routing table based on malicious characteristics and benign characteristics using linear regression based classification model. The Node density and node ranking calculation has enabled to handle the attack with help of energy aware constraints. Data securing mechanism can further increase the packet delivery ratio and throughput of the network on greedy routing strategies

References

[1] C. Ma et al., "Coverage overlapping problems in applications of IEEE 802.15.4 wireless sensor networks" in Proc. IEEE Wireless Communications and Networking Conference (WCNC): Services Applications, vol. 4369, 2013, pp. 4364-4369 [doi:10.1109/WCNC.2013.6555280].

[2] Liang Cheng Shiu, Chao Yang Lee, and Chu Sing Yang, "The divide-and-conquer deployment algorithm based on triangles for wireless sensor networks," IEEE Sensors J., vol. 11, no. 3, pp. 781-790, Mar. 2011 [doi:10.1109/JSEN.2010.2059006].

[3] Ting-Yu Lin, Member, IEEE , Hendro Agus Santoso, and Kun-Ru Wu, " Global Sensor Deployment and Local Coverage-Aware Recovery Schemes for Smart Environments in IEEE, Transactions on Mobile Computing, vol. 14, no. 7, Jul., 2015,pp-1382-1396. [doi:10.1109/TMC.2014.2353613].

[4] Seapahn Megerian, Farinaz Koushanfar, Miodrag Potkonjak, and Mani B. Srivastava, Senior Member, IEEE, "Worst and best-case coverage in sensor networks," IIEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 4, no. 1, pp. 84-92, Jan./Feb. 2005 [doi:10.1109/TMC.2005.15].

[5] Amin Vahdat and David Becker, Epidemic Routing for Partially Connected Ad Hoc Networks Technical Report CS-200006. Duke Univ., 2000.

[6] D. Tian and N. D. Georganas, "A Coverage-preserving node scheduling scheme for large wireless sensor networks" in Proceedings of the1st ACM international workshop on Wireless sensor networks and applications., Sept. 2002, pp. 32-41 [doi:10.1145/570738.570744].

[7] Ze Li, Haiying Shen, "A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless Networks" in IEEE TRANSACTIONS ON MOBILE COMPUTING~~,~~IEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 13, pp. 693-708, Mar. 2014 [doi:10.1109/TMC.2012.258].

[8] Mahesh Vaidya; Ekjot Singh Walia; Aditya Gupta, "' IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014) [doi: 10.1109/ICAETR.2014.7012798]

[9] Alejandro Proan˜o and Loukas Lazos, " Packet-Hiding Methods for Preventing Selective Jamming Attacks",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, pp.101-114, JANUARY/FEBRUARY 2012, [doi:10.1109/TDSC.2011.41].

[10] R.L. Rivest, A.Shamir and D.A.Wagner, 'Time-Lock Puzzles and Timed-Release Crypto,' Technical Report. Massachusetts Inst. of Technology, 1996.

[11] DOUGLAS S. J. DE COUTO, DANIEL AGUAYO, JOHN BICKET and ROBERT MORRIS, "A High-Throughput Path Metric for Multi-Hop Wireless Routing" in Wireless Networks Springer Science + Business Media, Inc. Manufactured in The Netherlands., vol 11, no. 4, Jul. 2005, pp. 419-434, [doi:10.1007/s11276-005-1766-z].

[12] Sungjin Lee & Sanghoon Lee, "Optimal transmission methodology for QoS provision of multi-hop cellular network," Wireless Netw., vol. 16, no. 5, pp. 1313-1327, 2010 [doi:10.1007/s11276-009-0205-y].

[13] Veena Safdar, Faisal Bashir, Zara Hamid, Hammad Afzal and Jae Young Pyun, "A hybrid routing protocol for wireless sensor networks with mobile sinks" in Proc. 7th Int. Symp. Wireless Pervasive Comput., 2012, pp. 1-5 [doi:10.1109/ISWPC.2012.6263665].

[14] Ioannis Chatzigiannakis, Athanasios Kinalis and Sotiris Nikoletseas , "Efficient data propagation strategies in wireless sensor networks using a single mobile sink", Computer Communications, vol. 31, no. 5, pp. 896914, 2008.[doi:10.1016/j.comcom.2007.12.011].

[15] Tian He, John A Stankovic, Chenyang Lu and Tarek Abdelzaher, "SPEED: A Stateless Protocol for Real-Time

Communication in Sensor Networks" in Proc. 23rd Int. Conf. Distributed Computing Systems, Jun 2003,Providence, RI, USA, .[doi:10.1109/ICDCS.2003.1203451].

[16] Amir Nader Shahbaz, Hamid Barati & Ali Barati, "Multipath routing through the firefly algorithm and fuzzy logic in wireless sensor networks," Peer-to-Peer Networking and Appl., vol. 14, no. 2, pp. 541-558, 2021 [doi:10.1007/s12083-020-01004-2].

[17] Zahra Hajipour & Hamid Barati, "EELRP: Energy efficient layered routing protocol in wireless sensor networks," Computing, vol. 103, no. 12, pp. 2789-2809, 2021 [doi:10.1007/s00607-021-00996-w].

[18] Isaac Sajan R and Jasper J, "A secure routing scheme to mitigate attack in wireless adhoc sensor network," Computers & Security, vol. 103, p. 102197, 2021 [doi:10.1016/j.cose.2021.102197].

[19] Nitin Mittal, Simrandeep Singh, Urvinder Singh and Rohit Salgotra, "Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks," Wireless Networks, vol. 27, no. 1, pp. 151-174, 2021 [doi:10.1007/s11276-020-02438-5].

[20] Weidong Fang, Wuxiong Zhang, Wei Yang, Zhannan Li, Weiwei Gao and Yinxuan Yang, "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks," Digital Communications and Networks, vol. 7, no. 4, pp. 470-478, 2021 [doi:10.1016/j.dcan.2021.03.005].

[21] Ali Shahidinejad and Saeid Barshandeh, "Sink selection and clustering using fuzzy-based controller for wireless sensor networks," Int. J. of Communication Systems, vol. 33, ~~no.~~ 15, p. e4557, 2020 [doi:10.1002/dac.4557].

[22] GULZAR MEHMOOD1, MUHAMMAD ZAHID KHAN, ABDUL WAHEED, MAHDI ZAREEI and EHAB MAHMOUD MOHAMED, "A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks," IEEE Access, vol. 8, pp. 131397-131413, 2020 [doi:10.1109/ACCESS.2020.3007405].

[23] Elham Hasheminejad & Hamid Barati, "A reliable tree-based data aggregation method in wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 14, no. 2, pp. 873-887, 2021 [doi:10.1007/s12083-020-01025-x].

[24] Maryam Naghibi & Hamid Barati, "SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 10769–10788, 2021.[doi: 10.1007/s12652-020-02751-z].

[25] Sedigheh Sadat Sharifi and Hamid Barati, "A method for routing and data aggregating in cluster-based wireless sensor networks," International Journal of Communication Systems, vol. 34, no. 7, p. e4754, 2021 [doi:10.1002/dac.4754].