IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

A Secure Blind Path Energy Aware Geographical Routing Protocol for Wireless Sensor Networks

Manjunath D R[1*], Thimmaraju S N[2]

[1]Visvesvaraya Technological University, Belagavi, India

[2]Dept. of MCA, Visvesvaraya Technological University, Centre for Post Graduate Studies, Mysore

[*]*Corresponding Author:manjunathdrcs@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 14/Jan/2019, Published: 31/Jan/2019

***Abstract*—**Wireless Sensor Networks (WSNs) are rapidly becoming popular due to they are low cost solutions for various real-world challenges. It is widely used in military surveillance, transportation management, health care, etc. Prolonging a wireless sensor network's lifetime is closely related to energy consumption. Furthermore, secure data transfer is a great challenge for WSNs, especially for applications that use important data such as military applications. The main objective is not only to design a new routing protocol that ensures network lifetime efficiency, but the balance between these security threats and energy efficiency. For that reason, we have designed the standard framework and simplify the process of building a novel geographical routing sensor networks that introduce location privacy, data privacy and energy awareness routing. Firstly, the whole network is divided into multiple grids with randomly distributed sensor nodes and all sensor nodes only communicates with their neighbor grids. Each grid selects the grid head based on the maximum energy level and minimum distance of the destination node in each grid .The data transmitter node identifies the neighbor grid with the grid head having maximum energy level and minimum distance of the destination node among its neighbor grids for data transmission. Further Hybrid AES-DES algorithm is applied to provide data privacy and location privacy. The proposed protocol provides a good trade-off between balancing energy, security and routing efficiency, and in all cases the lifespan of sensory networks can be significantly expanded.

***Keywords*—**Wireless Sensor Networks, Geographic Routing, Location privacy preserving, Data privacy preserving, Energy aware, blind path approach**.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) ,With their inherent computation and communication capabilities can expand human senses to areas that are not normally accessible and do not work for quite a while, thus opening up numerous new applications capabilities.Wireless sensor networks are unstable and have many notorious properties in a crucial and dangerous real-time environment. WSNs have been utilized for many long-lived monitoring applications such as water quality monitoring, underground railway supervision, Great Wall Monitoring and vehicle monitoring [1-6]. Effective routing technique is important for monitoring these applications because it provides plenty of real-time data.

Practitioners and Researchers allow them to evaluate and optimize the development of real-world WSN applications by understanding how energy consumes from sensor nodes. WSN efficiency of energy increases the life of the WSN, which is the making of new hardware platforms, new routing algorithms for complex topologies, development stock network protocols and new algorithms to develop media access.On the other hand, smaller devices are usually supplied with smaller batteries; As they are wireless, they generally operate in the absence of infrastructure, so their limited batteries depend on the power to supply and are expected to work for a long time and are unbearable and expensive to restore or recharge the batteries, once sensor nodes are assigned. They also need to manage the mobility of the nodes in the network. And most importantly, it reduces the impact of attacks on the routing protocol designed for such networks. In fact, due to the nature of the wireless channel's broadcast, the attackers are expected to participate in each node packet on the network, while the node's communications range to tweak traffic, correction, or drop packets forward Procedures' security.

There are three mainly routing protocols categories for wireless sensor networks: hierarchical routing, geographical routing and flat routing. In hierarchical routing, nodes are portioned into many clusters and each cluster is assigned with cluster head. An example of LEACH[10] sequencing routing protocols. Flat routing protocols include reactive routing protocols, like AODV [8], DSR [7], and DSDV[9]. In geographic routing protocols, location information of the nodes is used to transport packets towards the destination node. GPSR[11] is an example of geographic routing

protocols. Flat routing protocols are straight forward and every nodes are at the same level. When the network's size increases, they are poor for scalability because these protocols have a large amount of packet overhead, which uses more power. Hierarchical routers sort the network area into groups. In addition, one of the advantages of geographical approaches is that we can use "distributions" or "vector fields" defined in the geographical space to describe the states or operations of the network, and these distributions or vector spaces have very substantial properties in networks, such as variation or integrity, which allows many applications to be developed in classical mathematical analysis.Therefore, geographic routing protocols are viewed as progressively effective on IOT[12] because they minimize the size of the sensor node's storage, keeping only the information about direct neighbors for packet forwarding. Currently, hundreds of newly registered vehicles in the world have been installed with navigation systems and GPS receiver. As a result, geographical routing protocols are popular in VANETs[13] with the availability of their simplicity, low overhead, and GPS devices. Geographic routing protocols are suitable for scarce and dense traffic.

In this case, geographic routing is generally considered to be a smart forwarding mechanism, whereby each node packet will make the decision to pass to nearby neighbors or nodes near sync. Furthermore, such geographic routing protocols are effective, low-over-head modes have sufficient density, accurate localization and significant link reliability in sufficient sensor networks. Geographical routing protocols are based on the assumption that all packets in the network are considered trustworthy and have not taken into consideration the safety issue. However, compromised (malicious) nodes on the network may result in a decline in geographic routing displays in terms of distribution ratio (routing failures).

The forwarding node in geographic routing will select the location of the destination where the next hop is included in the forward message. Attackers can change or change this information to interrupt the routing plan. Attackers may disrupt the routing plan by creating a reduced message such as an encryption message or error message. For example, under animal supervision, supervision of network traffic flow and infecting backtracking, general sensor glands, or analyzing the data packets confidential information, the attacker can easily detect the actual position.

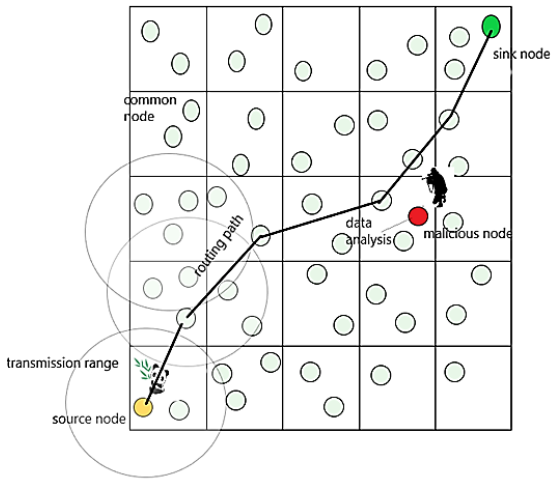


Fig1. Illustration of panda-hunter game model based on geographical routing protocol.

[14], The Panda hunter game originally intended to maintain location confidentiality, making it clear the location of the privacy situation. As shown in Figure 1, in the Panda-Hunter game format, many small sensor nodes are randomly supplied to pandas for residence. When the panda appears, monitor it quickly through synchronization or routing paths that are surrounded by sensor nodes (called root nodes) and transmit information quickly (e.g., panda position). Also, the hunter is a panda-hunter game that runs free on the network and controls local wireless communications. By monitoring network traffic and tracking the routing path, the hunter can find the exact location of the original nodes and eventually find the panda.

Furthermore, providing security at routing is an important step in improving the system's reliability as discussed in the previous section. Therefore, two important functions that can be used to improve the performance of network awareness are energy communication and security supplies.

The main contribution of our proposed work are first we develop an energy aware geographical routing protocol based choosing neighboring grid highest energy node and less distance from the sink node. Next we implement hash function generation for sensor nodes and grids using SHA 256 algorithm to provide location privacy for sensor nodes and finally we develop hybrid AES-DES algorithm to do data encryption and decryption to provide data privacy. In our proposed approach we are develop a novel energy aware secured geographical routing scheme that can protect both location privacy and data privacy.

The remainder of this paper is organized as follows. After introducing related work in Section 2, we briefly describe the proposed energy aware geographic routing scheme along with implemented security scheme in Section 3. Experimental results and performance analysis of proposed approach are

then discussed in Sections 4 .Finally, conclusions are drawn in Section 5.

II. RELATED WORKS

Geographic routing protocols provide basic-destination routes based on localization information of sensor nodes, which do not require path detection. Traditional geographical routing uses a greedy routing technique known to each node to know the location of the neighborhood, a hop distance, the position of the final location of a packet and the position of the candidates to advance further decisions. Geographic Routing Methods require a bit of computation in regular nodes and therefore it is very appropriate WSN Applications [15-16].Authors presents the routing protocol is based on the geographical location of the GAF[17] nodes. The protocol assumes that each node knows the location of the nodes in the entire monitoring area and in its own place. The protocol has two steps to execute. The first step is to divide the network area into many wireless cells according to the node and communication radius. The second stage is the choice of virtual cells CH nodes. Clustering from realistic particles Nodes make energy consumption more uniform. However, if the size of the network area is large, the GAF's inter-cluster communication costs will rise.

GPSR stands for most unified geography routing protocol, [18] which makes greedy forward decisions based on information about hop neighbors. This method broadens the location of the nodes of the network on the network while identifying the nearest neighbors near the destination. GPSR converts to peripheral mode, which uses the right-hand rule to cross the hole to cross the hole to reach the destination to restart the process through the GF technique. On the road, the Greedy Permit Routing Protocol (GPSR) does not use information from the map, which represents the algorithm based position. In particular, geographical routing can be made using natural planner graph streets and sections.

For a WSNs, a power efficient intra cluster transmission in the grid clustering protocol was proposed by Qasim et.al.[19]. The authors used mathematical analysis to provide a metric to define inter-cluster transmissions. The metric is an extreme distance used to determine the cluster's best size. The centralized energy-aware grid clustering protocol is based on the appropriate cluster size. However, the authors did not specify the implementation of multiple hop routing protocols on paper and only 225m * 225m network showed in a hop context Environment. This is not an algorithm that adapts to a large network area.

Most early works deal with only one type of attack but not by a variety of attacks that may start up against routing Protocol. At [20], the Geographical-based Safe and Effective Cost-Aware Safe Routing (CASER) protocol has been proposed. The network is divided into several small mesh, similar to the different groups. Each mesh node that has the maximum percentage of power is selected as a mesh head for packet transmission. Each mesh head has the location information known, the rest of its own power, Position information and the residual strength of the mesh beside it. To save energy consumption, low priority chooses to pass the packet with high priority. That is, the power of the next energy is closer to the base of the power and the next hop mesh is selected. Then, to protect the privacy of the original location, the random walk system Used to create a routing path instead of for less passage. The authors in [21] have proposed a scalable certification scheme based on ellipse curve cryptography (ECC) to prevent the attacker from obtaining the original node ID by analyzing the content of the cryptography and authentication mechanism message. The certification scheme proposed on the ECC, has a clear power over the computational and communications overhead compared to conventional messaging certification schemes. In addition, the ECC node is effective against compromise. Attackers cannot pretend to be the legal sensor node or add fake packets to the network; they do not modify the message content.

ID Analysis In contrast to attacks, pseudonyms is used instead of true IDs to maintain location confidentiality. However, specific nicknames can be monitored and tracked by even more powerful opponents. [22], the novel approach based on the symmetrical Bayesian-Nash Equilibrium (SBNE) is proposed to change the pseudoscience of mobile nodes in the ad hack network. However, this is not correct in dynamic changing pseudonyms to power limited WSNs. Random walking is easy and easily accomplished due to the need for any routing management. Also, nodes reduce the cost of storage and communication. However, in a random walk routing, the packet communication path becomes longer, introducing some long-term communication latency and higher power consumption. Cryptography method are used to ensure the node's anonymity. In some existing Works SBNe [22] is responsible for poor generalization, as opposed to attacks on ID analysis. Protocols like e.g. ECC [21] protects basic location confidentiality, hopes for node compatibility, traffic analysis and hop-by-hop backtracking provide id anonymity while providing some safeguards to attack.

III. PROPOSED WORK

In this section, we present complete discussion about proposed model which is mainly divided into two stages where first of all we develop energy aware routing protocol and later, security parameters are included to make the proposed routing scheme more efficient and robust. In this work, we focus on energy efficient and sensor node location privacy preserving scheme for geographical sensor network. The complete work is divided into multiple stages which are as follows.

A. Network Model

In this work *M* sensor nodes are non-uniformly deployed over a geographical grid region whose area of W xH. where W

and H represents width and height of network respectively considered with similar values. Each sensor has the node Very limited and re-restored energy resource. The only available destination to all sensor nodes is sink node to send messages. The network is split into small number of grids i.e. divided into $l \times l$ number of grids where l denotes the grid size, for random number of nodes. All sensor nodes are heterogeneous and have the different initial energy. Each node has a unique ID. Every sensor nodes knows their location by using GPS or some other localization systems. All nodes are aware of their retention power and have the transmission range and same transmission rate.

In our work, geographical routing based network architecture is adopted where the sensor nodes are deployed randomly and un-uniformly. Here, at the beginning, each node is assigned with random different power capability, which may change at the packet transmission stage. The complete process of our proposed work is depicted in figure 2.

Algorithm 1 : neighboring grid identification process

Step 1

1. Provide the input as current grid ID and grid size.
2. Initialize the each grid ID with 0// initially we assign all grid IDs as 0 which is updated later as any neighboring grid is identified.

Step 2

$$\boldsymbol{If}\ (grid_{id} + grid_{size}) \leq\ {grid_{size}}^2\ then\ neighbour_{up} = grid_{id} + grid_{size}\ \boldsymbol{end\ if}$$

$$\boldsymbol{If} (grid_{id}) > grid_{size} then\ neighbor_{down} = grid_{id} - grid_{size}\ \boldsymbol{end\ if}$$

$$\boldsymbol{If}\ mod(grid_{id}, grid_{size}) \neq 1\ then\ neighbor_{left} = grid_{size} - 1$$

$$neighbor_{left_{up}} = grid_{id} + (grid_{size} - 1)$$

$$neighbor_{left_{down}} =\ grid_{id} - (grid_{size} + 1)\ \boldsymbol{end\ if}$$

$$\boldsymbol{If}\ mod(grid_{id}, grid_{size}) \neq 0\ then\ neighbor_{right} = grid_{size} + 1$$

$$neighbor_{right_{up}} = grid_{id} + (grid_{size} + 1)$$

$$neighbor_{right_{down}} =\ grid_{id} - (grid_{size} - 1)\ \boldsymbol{end\ if}$$

$$\boldsymbol{if}(grid_{id} + grid_{size}) > {grid_{size}}^2\ then\ neighbor_{left_{up}} =\ 0\ and\ neighbor_{left_{down}} = 0\ \boldsymbol{end\ if}$$

$$\boldsymbol{If}(grid_{id}) \leq\ grid_{size} then\ neighbor_{right_{up}} =\ 0\ and\ neighbor_{right_{down}} = 0\ \boldsymbol{end\ if}$$

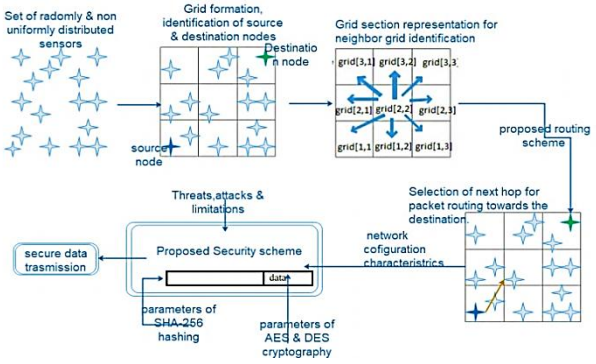


Fig2: Functionality diagram of our proposed approach.

To organize the network, the sensors are divided into grids where each grid is managed by a grid head. The grid head node can listen and communicate directly with all their grid members and all neighboring grid heads in the network. Also, we assume that the destination node can listen and communicate with all neighboring grid head in the network. Coordinates of the sensor node will be identified based on grid coordinates in the considered region as

$$Coord(x, y) = random(N, 2) \times W \qquad (1)$$

First of all, we identify the source and destination node id where the original node ID, like input, $Grid_{ID} = [i, j]$; It gives the grid space of the original node. Based on those coordinates, we identify the grid with the desired orbits by comparing the orbits of the original node and other observations. For example this provides the grid location in the deployed network area such as $Grid_{ID} = [1,3]$ in the current network scenario as depicted in figure. Based on these ID values, final grid where source node is present can be computed as:

$$Final_{Grid_{ID}} = l * \left(Grid_{ID(i)} - 1\right) + Grid_{ID(j)} \qquad (2)$$

Where l=4, $Grid_{ID(i)}$=1 and $Grid_{ID(j)}$=3 hence final grid ID is 3, next step using our proposed routing scheme we provide a solution for neighboring grid identification to pocket routing. Grid section representation for neighbor grid identification shown in the figure, based on the position network is divided into different section. The complete process of neighbor grid identification is shown in algorithm 1.

Even though multiple neighboring grids are eligible for data transmission for given source node we consider neighboring grid having grid head with highest energy when compare to grid heads of other neighboring grids so that energy consumption of all grids are equally distributed and to improve the total network lifetime. In order to select the most suitable node, we consider the neighbor grid head we use equation given below

$$Neighbor_{Grid_{Head}} = \begin{cases} E_{max}(Current\ Grid\ Nodes) > E_{threshold}, \\ \quad Select\ this\ node\ for\ next\ step \\ E_{max}(Current\ Grid\ Nodes) < E_{threshold}, \\ \quad discard\ this\ node \end{cases} \quad (3)$$

Where E_{max} represents the maximum remaining energy level of current grid nodes and $E_{threshold}$ Threshold energy level. We select $Neighbor_{Grid_{Head}}$ with E_{max} greater than the threshold energy level, which results in multiple neighboring grids are eligible for data transmission. In this case, we consider next hop from multiple neighboring grids for data transmission with minimum distance node from the sink. We use equation given below to find next hop. The minimum distance is calculated using Floyd-Warshall algorithm.

$$Next\_Neighbour\_Hop = \min(dist((D_x, D_y) - Neighbor_{Grid_{Head}}) \quad (4)$$

B. The location and data privacy scheme

To prevent the attacker from obtaining the source node's ID and data privacy by analyzing the message content, we proposed a scalable authentication scheme based on hybrid model of AES and DES encryption and decryption schemes. In our proposed geographical routing each node maintains several information includes its Node ID, its Current grid ID, Neighboring Node ID, Neighbor Grid ID, Distance between the nodes, Energy Level of communicating node along with data. Several information such as IDs of grids, nodes, neighboring grids and current grid are need to be secure in order to preserve the location privacy information. In our proposed security approach we apply SHA-256 hash function to the above information in the routing table to introduce the anonymity to the network and grid IDs. Distance between nodes and energy level of the communicating nodes are updated iteratively during a successful communication. Next to secure main information i.e. to provide data privacy the aggregated main information is encrypted and decrypted using hybrid model of AES and DES encryption and decryption scheme at sender and receiver node respectively. The working of hybrid model is shown in the figure 3.

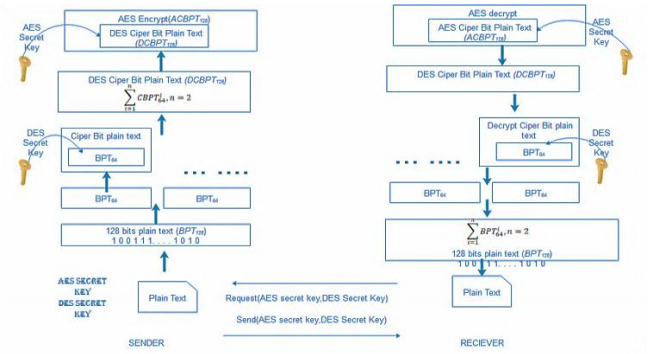


Fig 3. Proposed data privacy scheme

IV. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS.

Here first we discuss about our experimental results using our proposed routing scheme and then the performance was measured using throughput, network life time and the total energy consumption. In addition to above, we also furnish description about how our proposed security scheme prevents different variety of attack to provide location and data privacy.

We use MATLAB Simulation tool to experiment our proposed approach in windows environment. The simulation parameters are presented in table1.

Table 1. Experimental simulation parameters

Sensor field area	500 × 500
Sensor nodes Number	100
Sensor nodes position	static sensor nodes
Transmission range	20 meters
Initial nodes energy	random
Transmission energy consumption per bit	50 nJ/bit
Receiving energy consumption per bit	50 nJ/bit
Data aggregation energy	5 nJ/bit
Packet size	64 bytes
Data rate (kbps)	2,4,6,8

The proposed energy aware routing algorithm is tested for 50,100 sensor nodes and tested can be done for any number of nodes. We have taken at least the minimum values of the energy of sensor nodes, we can increase so that this does not affect the performance of the proposed routing algorithm.

In our current scenario, we have considered $grid_{size} = 3$ hence totally 9 grids are generated which contains either no node or multiple node distributed in the random manner. In this case, source node selection is based on highest remaining energy of grid {1, 1}.Totally 7 nodes are presented in the grid {1, 1}, where node id 12 with coordinates [0.80, 0.96] having highest energy of the current grid is elected as grid head and acts as source node with hash function d3304b33a18ad32b007011c1952401a2. The grid head selection process is presented in table 3 where grid name, coordinates, node ID, and corresponding energy levels are discussed. The coordinates of destination nodes are given as [2.34, 2.14] and Hash function is e09f99f2b3532e8ae417237659880d24.

The grid head selection process is presented in table 2 where grid name, coordinates, node ID, and corresponding energy levels are discussed. The next neighboring grids for grid{1,1} are grid{1,2},grid{2,1},grid{2,2} . First of all, we consider grid {1,2} where only 3 nodes with node id 24,37,45 are present with the energy value of 0.7688,05118,and 0.4547 respectively which is depicted in table 4, next neighbor grid identified as Grid{2,1} where total 7 nodes are present with node id 3,7,17,21,34,38 with energy values of 0.9394,0.5341,0.9397,0.9456,0.5835 and 0.0826 respectively

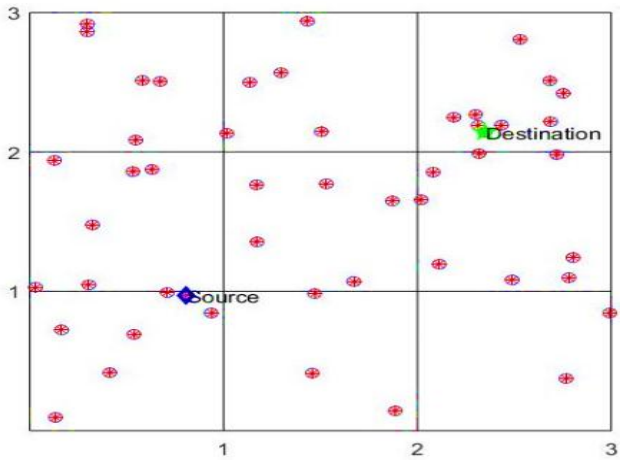
. Next neighbor grid identified as Grid{2,2} where total 5 nodes are present with node id 15,29,35,39,48 with energy values of 0.1609,0.6802,0.5518,0.9496,and 0.1257 respectively .In grid {1,1} node id 24 with highest energy level in the current grid is elected as grid head, likewise in grid{2,1} node id 21 with highest energy level is elected as grid head and in grid{2,2} node id 39 with highest energy level is elected as grid head. From table 3 the maximum energy nodes in each grid are obtained as 24, 21 and 49 whose energy levels are 0.7688, 0.9456 and 0.9496 and all are above $E_{threshold}$. Hence, for data transmission node id 39 belongs to neighbor grid {2, 2} is selected as next hop node for data transmission and it is show in the figure 4.

Table 2 : Next hop & grid selection process

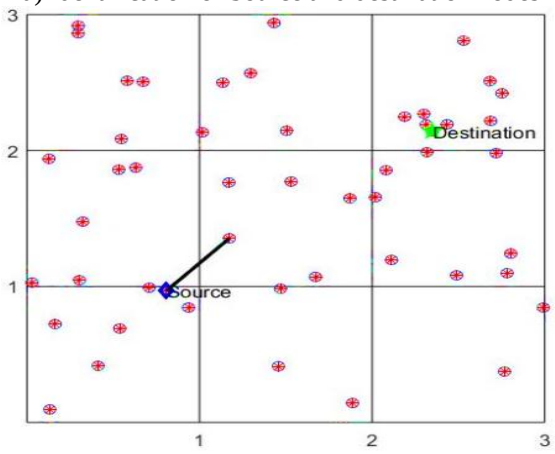
Grid name	*Nodes*	*Coordinates*		*Node Id*	*Energy Level*	Selected Head
G{1,2}	*3*	*1.46*	*0.98*	*Id=24*	*0.7688*	Node Id=39
		1.88	*0.14*	*Id=37*	*0.5118*	
		1.45	*0.41*	*Id=45*	*0.4547*	
G{2,1}	*7*	*0.02*	*1.02*	*Id=3*	*0.9394*	
		0.12	*1.93*	*Id=7*	*0.5341*	
		0.53	*1.85*	*Id=17*	*0.9397*	
		0.32	*1.47*	*Id=21*	*0.9456*	
		0.63	*1.87*	*Id=34*	*0.5835*	
		0.30	*1.04*	*Id=38*	*0.0826*	
G{2,1}	*5*	*1.87*	*1.64*	*Id=15*	*0.1609*	
		1.67	*1.07*	*id=29*	*0.6802*	
		1.53	*1.77*	*Id=35*	*0.5518*	
		1.17	*1.35*	*Id=39*	*0.9496*	
		1.17	*1.76*	*Id=48*	*0.1257*	

Performance analysis

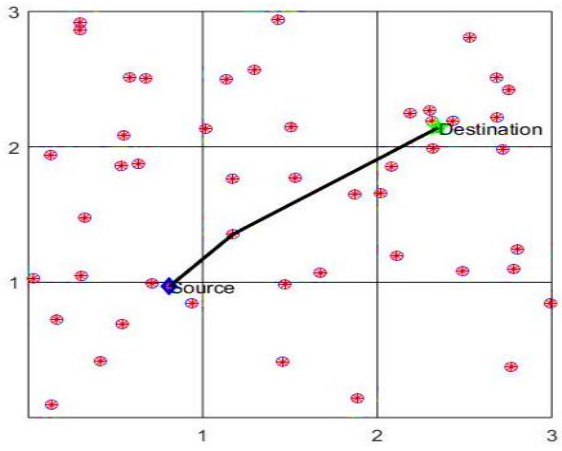
Based on the proposed routing plan, we analyze the network's performance based on network throughput, network lifetime, and power consumption. The performance of the proposed method is tested by changing the data rates as mentioned in the simulation parameter table1. Network throughput is referred as successfully distributed packets on the network during each simulation round are computed. The performance of the received end-to-throughput depicts in Figure 5, where data rates vary by 2, 4 and 8 kbps, indicating that higher data rates can achieve better throughput performance compared to lower data rates. The proposed method of performance for 8kbps is higher up to 50% for 2kbps data rate and 25% from 4kbps.



a) Identification of Source and destination nodes



b) Identified Neighbor grid{2,2} & grid head selection as next hop for data transmission



c) Packet route to destination

Fig 4: Routing steps

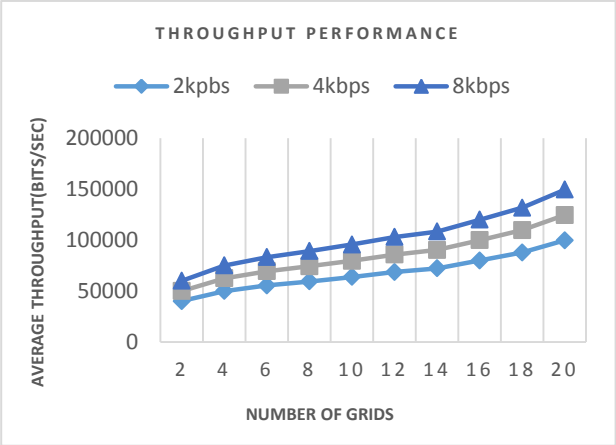


Fig 5: end-to-end throughput

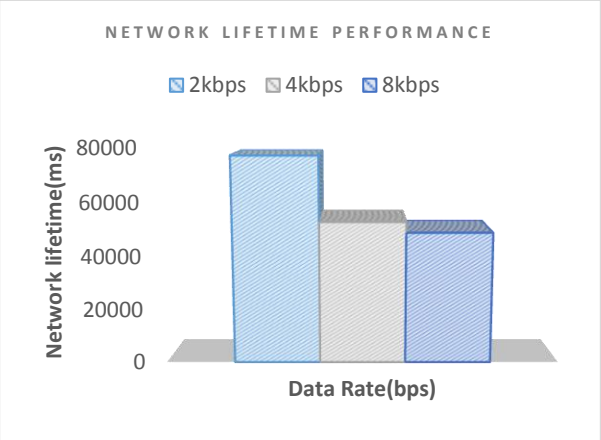


fig 6: Lifetime performance

Here, the number of grids through where data packets are sent to the destination. Likewise, in the current simulation scenario, we evaluate the performance of network life expectancy for various data rates, which often shows that network life expectancy rates for higher data rates decrease due to the frequent use of sensor nodes. Comparative analysis of network life depicted in Figure 6. It is analyzed by an energy consumption performance model in a network context for a different number of nodes nested in figure 7. Higher data communication rate requires more energy for data communication and storage, which can affect the efficiency of energy consumption, which affects the low network

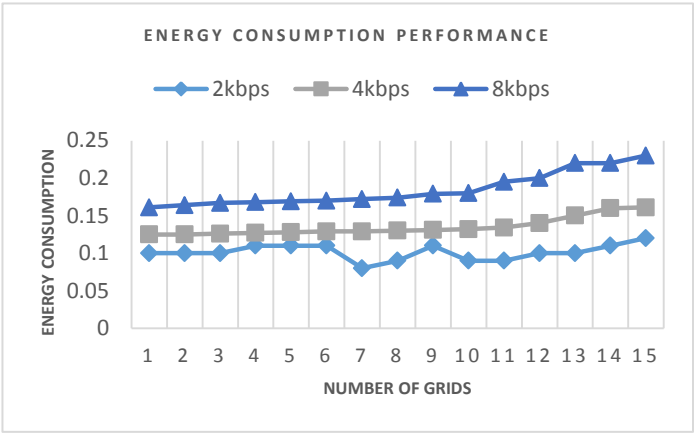


Fig 7: Energy consumption performance

lifetime. For this experiment, the average power consumption for 2kbps, 4kbps and 8 kbps is 0.099J, 0.1362J and 0.18162J.

Security analysis

Here we explain some important things of Security analysis results including, source location privacy, ID analysis attacks, passive Attack analysis, and compromised grid head attack analysis.

To prevent the attacker from getting the source node's ID by inspecting the message content, we used a hashing scheme based on SHA256 hashing. In order to introduce the anonymity to the network and grid IDs, we apply hash function operation during the node deployment phase where each node's corresponding hash ID is used for establishing the communication between two neighboring nodes so that attackers cannot pretend to be the legal sensor node or add fake packets to the network; they do not modify the message content. More importantly, attackers cannot create source nodes ID and location information by analyzing the message's contents or network. In the proposed protocol, comprehensible data is encrypted with hybrid AES DES encryption and decryption scheme and deals with all eavesdropping by the Homomorphic encryption algorithm. Thus, passive attackers cannot decrypt the message without decryption Key.

The compromised grid head attack is an attempt to demands combined data from neighboring grid head so that after receiving the message it can analyze the data and get or modify specific information.

In our proposed security Schema is that the role of all neighboring grid head is to forward the aggregated encrypted data from its neighboring grid heads and to the destination node without decrypting the message. In addition, our encryption process depends on many factors, that is node location, and the distance between the grid head node to the destination node; so for grid head attackers or any attackers requires this combination Information about network operations and network topology (To know the distance between node and grid head), and The secret key generated by the hybrid AES DES scheme.

V. CONCLUSION

Geographic routing protocols are considered more efficient on IOT, VANETS because they minimize the size of the sensor node's storage, keeping only the information about direct neighbors for packet forwarding. We focus on the geographic routing schemes on wireless sensor networks. Creating network grids is an effective way of improving Measurement and Longevity of WSN. With the goal of improving the lifespan of the entire network we introduce the novel path for safe and energy awareness geographical routing protocol for communication. According to our proposed work, complete networks are divided into multiple grids, where there are randomly distributed several nodes presents in the grid with different energy level. For next hop selection the source node only need to communicate with neighboring grid head with the highest energy and minimum distance between the destination node. This process will be repeated until the destination node is positioned. To protect location and data privacy, we apply the Hash Function generation during deployment to the nodes and grid IDs and enlist the data and transmit the hybrid of the AES-DES algorithm. Comparative performance is done by changing the data rate. Experimental studies show that more data-specific methods provide better throughput but low data rates communication can improve network life. Additionally this will provide both source location privacy, data privacy and also prevents id analysis attacks, passive attacks and compromised grid head attacks.

REFERENCES

[1] A. Milankovich , K. Klincsek , Wireless sensor network for water quality moni- toring, in: Proceedings of the European Project Space on Information and Com- munication Systems, 2015, pp. 28–47 .

[2] P. Mohit , R. Amin , G.P. Biswas , Design of authentication protocol for wireless sensor network-based smart vehicular system, Veh. Commun. 9 (2017) 64–71 .

[3] A. Odorizzi , G. Mazzini , M-geraf: A reliable random forwarding geographic routing protocol in multisink ad hoc and sensor networks, in: Proceedings of the International Symposium on Intelligent Signal Processing and Communica- tion Systems, 2008, pp. 416–419 .

[4] K. Oe , A. Koyama , L. Barolli , Proposal and performance evaluation of a multi- cast routing protocol for wireless mesh networks based on network load, Mo- bil. Inf. Syst. 2015 (2015) 1–10

[5] K. Oe , A. Koyama , L. Barolli , Proposal and performance evaluation of a multi- cast routing protocol for wireless mesh networks based on network load, Mo- bil. Inf. Syst. 2015 (2015) 1–10

[6] B. O'Flynn , R. Martinezcatala , S. Harte , C. O'Mathuna , J. Cleary , C. Slater , F. Re- gan , D. Diamond , H. Murphy , Smartcoast: a wireless sensor network for water quality monitoring, in: Proceedings of the IEEE Conference on Local Computer Networks, 2007, pp. 815–816

[7] Boukerche, A., Turgut, B., Aydin, N., Ahmad, M.Z., Boloni, L., Turgut, D., 2011. Routing protocols in ad hoc networks: a survey. Comput. Netw. 55, 3032–3080.

[8] Mulert, J., Welch, I., Seah, W.K.G., 2012. Security threats and solutions in manets: a case study using aodv and saodv. J. Netw. Comput. Appl. 35 (4), 1249–1259.

[9] Ade, S.A., Tijare, P.A., 2010. Performance comparison of aodv, dsdv, olsr and dsr routing protocols in mobile ad hoc networks. Int. J. Inf. Technol. Knowl. Manag. 2 (2),545–548.

[10] Tyagi, S., Kumar, N., 2013. A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. J. Netw. Comput. Appl. 36(2), 623–645.

[11] Karp, B., Kung, H., 2000. GPSR: Greedy perimeter stateless routing for wireless networks. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. ACM Press, pp. 243–254

[12] F. M. Al-Turjman and H. S. Hassanein, ``Enhanced data delivery framework for dynamic information-centric networks (ICNs)," in *Proc. IEEE 38th Conf. Local Comput. Netw. (LCN)*, Oct. 2013, pp. 810_817.9

[13] Silva, C. M., Masini, B. M., Ferrari, G., & Thibault, I. (2017). A survey on infrastructure-based vehicular networks. Mobile Information Systems, 2017.

[14] C. Ozturk, Y. Zhang, W. Trappe. Source-Location privacy in energy-constrained sensor network routing. In: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004). pp. 88-93, 2004.

[15] E.Park, D. Bae, H. Choo, Energy efficient geographic routing for prolonging network lifetime in wireless sensor networks, in: Proceedings of the 2010 International Conference on Computational Science and Its Applications, ICCSA '10, IEEE Computer Society, Washington, DC, USA, 2010, pp. 285–288

[16] C. Petrioli, M. Nati, P. Casari, M. Zorzi, S. Basagni, Alba-r: Load-balancing geographic routing around connectivity holes in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 25 (3) (2014)529–539.

[17] Xu, Y., Heidemann, J., Estrin, D.: Geograph-informed energy conservation for Ad hoc routing. In: 7th Annual International Conference on Mobile Computing and Networking, 2001, pp. 70–84.

[18] Brad Karp, H. T. Kung GPSR: greedy perimeter stateless routing for wireless networks MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking Pages 243-254

[19] A.A. Qasem, A.E. Fawzy, M. Shokair, W. Saad, S. El-Halafawy, A. Elkorany, Energy Efficient Intra Cluster Transmission in Grid Clustering Protocol for Wireless Sensor Networks, Wirel. Pers. Commun. 97 (2017) pp. 915–932.

[20] D. Tang, T. Li, J. Ren, J. Wu. Cost-Aware SEcure Routing (CASER) Protocol Design for
Wireless Sensor Networks. IEEE Transactions on Parallel & Distributed Systems, 2015, 26(4):960-973.

[21] J. Li, Y. Li, J. Ren, J. Wu. Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks. IEEE Transactions on Parallel & Distributed Systems, 2014, 25(5): 1223-1232.

[22] J. Freudiger, M.H. Manshaei, J.P. Hubaux, D.C. Parkes. Non-Cooperative Location Privacy. IEEE Transactions on Dependable & Secure Computing, 2013, 10(2):84-98.

Authors Profile

Manjunath D R is currently working as assistant Professor in Dept. of CSE , Dayananda Sagar Academy of Technology and Management, Bangalore, received B.E and M.Tech in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, Karnataka, India, 2007 and 2013, and he is currently pursuing the PhD in Computer Science and Engineering from Visvesvaraya Technological University.

Dr. Thimmaraju S N is a Professor in Dept. of Masters of Computer Applications, Visvesvaraya Technological University, and Centre for Post Graduate Studies, Mysore, India. His research interests lie in the areas of computer networking, graph theory and big data.

