IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

Dynamic Probabilistic Source Location Privacy Protection Scheme Based on Brother Node in Wireless Sensor Network

Dr.R.Srividhya, K.Geethalakshmi,

Assistant Professor, Department of Computer Science, Dr.G.R.Damodaran College of Science, Coimbatore, Tamilnadu, India

Research Scholar, Department of Computer Science, Dr.G.R.Damodaran College of Science, Coimbatore, Tamilnadu, India

ABSTRACT---Source location privacy problem in WSNs is an important research topic in the industry. We propose a probabilistic source location privacy protection scheme based on brother node (PSLPBN) for WSNs. A more powerful adversary, which can use Hidden Markov Model (HMM) to estimate the state of the source, is considered in this thesis. To cope with this type of adversary, phantom nodes and fake sources, which are responsible to mimic the behaviour of the source, are utilized to diversify the routing path. Then, the weight of each node is calculated as a criterion to select the next-hop candidate. In addition, two transmission modes are designed to transmit real packets. To improve security and preserve source location privacy in wireless sensor networks, a strategy called Dynamic Multi-node Selection based on Phantom Routing Protocol is proposed. The protocol enables the selected phantom node to maintain certain angle and the distance that is well enough to evenly get distributed around the source node.The routing path is also diversified through multi-node selection, which greatly reduces the possibility of overlapping paths capability. Simulation experiment results and theoretical analysis show that: on one hand, the proposed protocol can effectively resist source location privacy attacks with the ability to intercept the entire network; on the other hand, it can balance and optimize network energy consumption and delay, and extend the network life cycle.

KEYWORDS: Internet of Things, Wireless Sensor Networks, Location-Based Service Process

I.INTRODUCTION

The Development of Internet of Things, Wireless Sensor Networks (WSNs, wireless sensor networks) have been widely used as an important part of the Internet of Things. It is widely used in the fields of national defense and military, industrial and agricultural production, smart cities and environmental monitoring. Wireless sensor network is an information collection system that processes the integrated information of the system with transmission function which can obtain target information in real time. This is to realize the interaction details of the system, and used in military, environmental monitoring and forecasting. Many fields such as health care have very broad application prospects. The wireless sensor network is affected by the wireless communication method and its own resources. It is vulnerable to various security threats due to limitations, etc., among which the location of the source node privacy issue has become the main obstacle restricting its actual deployment on the applications. Wireless sensor networks have uncontrollable environmental factors. In recent years, Wireless Sensor Networks (WSN) have become more widely used, and its security issues have become more and more.

1.1WSN Data Privacy Protection Method

Wireless sensor network can be realized from end to end data aggregation privacy protection, which allows direct manipulation of ciphertext encryption transformation technology that can realize multiplication and homomorphic calculation. To improve further, Domingo-Ferrer algorithm can be implemented in addition. Using homomorphic encryption algorithm to guarantee homomorphism allows users to operate on sensitive data without revealing data information. In the data aggregation process of WSN, the system can realize end-to-end encryption of data using homomorphic encryption technology, where intermediate nodes can directly aggregate encrypted data under its premise avoiding the disclosure of privacy during the decryption.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

1.2WSN Data Privacy Protection Method Based on Clustering Technology

Two methods are proposed for data aggregation privacy protection. Cluster-based Privacy Data Protection (CPDA) and Shard-based Converged Privacy Protection (SMART), these two methods are to achieve data "and" aggregate calculation.

The realization of CPDA method includes 3 steps.

(1) **Build a cluster:** The sensor nodes are randomly divided into multiple clusters using a distributedprotocol.

(2) **Data aggregation in the cluster:** The nodes in each cluster share a non-zero number as the seed; the cluster head node point uses the additive nature of polynomials to exchange data between nodes to achieve the data aggregation of nodes in the cluster. In the realization of the cluster aggregation, it will ensure that every node can obtain the private data of othernodes.

(3) **Data aggregation between clusters:** Each cluster head node uses the aggregated data to use the routing tree protocol.

1.3DesignIdeas

Typical location service scenarios based on information cache have high information value, frequent user query requests, and query requests in the same area that have characteristics of dense mass, etc. By analyzing the above characteristics, you can find that the user's movement trajectory is easy for leakages, and the service provider is untrusted which could lead to security hazards and defects (such as low server efficiency). To solve the above problems, the system use caching mechanism to reduce the interaction between users and untrusted service providers considering the background information in the area where the user is located assuming that the untrusted service provider is attacker A. Interchanging the frequency will significantly reduce the risk of privacy leakage.

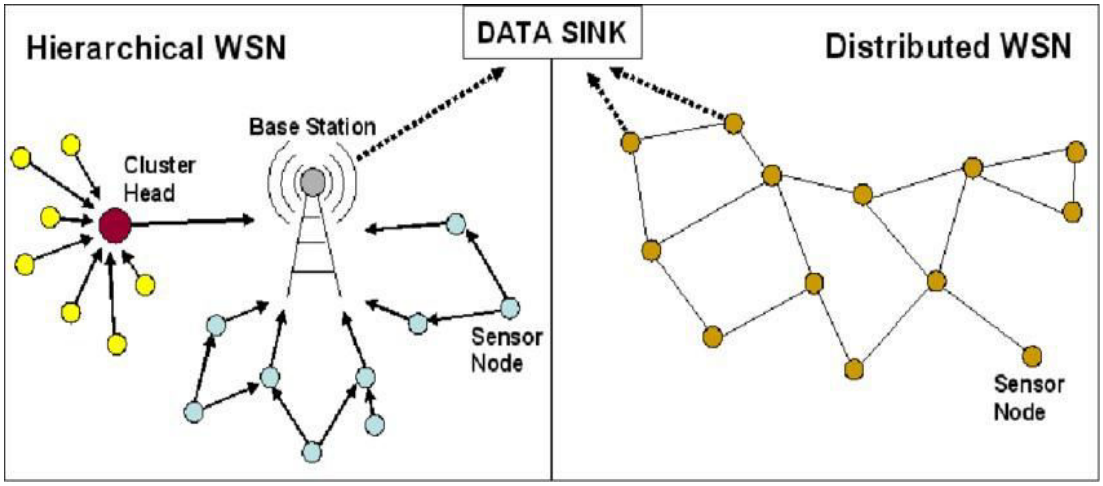

Figure 1. Wireless Sensor Network Attack Model

According to the characteristics of wireless sensor network, in wireless sensor network attack model shown in figure 1, the following assumptions are made in the protection of network location privacy.

1) There are enough sensor nodes and evenly distributed in the network, that is, the node density is equal in each area. Two nodes adjacent to each other can achieve direct communication between them, and communication between non-adjacent nodes can be forwarded through an intermediate node and completed in a multi-hopmanner.

2) There is only one base station and multiple aggregations in the network node. The source node can directly collect information and collect data, and the data packet is sent from the source node to the sink node and finally reaches the base station. Base stations usually have strong communication and computing storagecapabilities.

3) Except for the base station, other nodes are identical, that is, they have the same limited power consumption, initial energy, computing power, storage capacity, Communication capability, and nodes can replace eachother.

4) The location of the base station and each node is completely random and in the network, the location can change, the network topology can change, and the new nodes can be added at any time, and failed nodes can be removed at the same time. There may be multiple source nodes simultaneously transmitting information. In wireless sensor network location protection, according to the attacker, the attack method can be divided into ordinary attack model and complex attack model. In the ordinary attack model, the attacker only uses eavesdropping and hop-by-hop passive attack methods such as backtracking [Kido *et al.,*, Li *et al.,*] and traffic analysis [Kamat*et al.,*]. This way

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

analyses the nodes in the network without exerting additional influence on the network. The location of the point and the base station is private and not easilydetected.

To improve security and preserve source location privacy in wireless sensor networks, a strategy called Dynamic Multi-node Selection based on Phantom Routing Protocol is proposed. The protocol enables the selected phantom node to maintain a certain angle and the distance that is well enough to evenly get distributed around the source node and the routing path is diversified through multi-node selection, which greatly reduces the possibility of overlapping paths capability**.** The source location privacy protection protocol is to resist global traffic attackers. The existing research work mainly forwards data packets from the phantom node to the base station through the shortest path, and the routing path is relatively simple and easy and cause overlap on the path.

The further organization of the paper is as follows. Section 1 describes the detailed information about wireless sensor networks and its privacy issues, source Location privacy, scope and motivation of this research work. Section 2 presents the previous research in the area of source Location privacy in wireless sensor networks and their advantages and disadvantages. Section 3 describes the protocol called Phantom routing protocol for single path selection and presents a new approach called DMNSPRPBN. Section 4 describes the performance comparison of the proposed method with the existing routing mechanism. Section 5 concludes the work with cited references.

II. LITERATURE SURVEY

Kao *et al.*, proposed the phantom routing protocol for the first time, which uses flooding. The method will greatly increase communication overhead and energy consumption, and the phantom nodes generated by the phantom routing protocol that walks completely random and cannot be well far away the data source node. Kao *et al.*, proposed a directional random step protocol based on area or hop count based on the panda hunter model. The main idea of the agreement is made assuming thateach node in the network puts the number of hops greater than itself in the set (Smax) according to the number of hops from the neighboring node to the base station, and puts the number of hops less than itself in the set (Smax).{Smin}, each time the source node sends a data packet, the node in s0 or s1 is randomly selected as the forwarding node for the first h hops. This method can make the number data packets sent away from or close to the base station every time. However, the phantom source nodes generated by this strategy are concentrated in certain areas and do not have a good dispersibility. Liu *et al.,* proposed a location-based phantom routing protocol (PRLA, a source location privacy protocol in WSN. The PRLA protocol determines the forwarding probability according to the offset angle of neighboring nodes, and selects the next hop sending node according to the forwarding probability. So as to avoid the attacker's visible area as much as possible, and reduce the failure path, but the loss of the path cannot be completely avoided. Liu *et al.,* proposed based on the source node's enhanced limited flooding source location privacy protection protocol (EPUSBRF, a source-location privacy preservation protocol in Wireless sensor networks using source- based derestricted flooding), In the hop limited flooding stage of source node h, the mark of the node is in the view area, the source node h hops after the limited flooding ends, the base station performs a network-wide broadcast avoiding the view area, and in the shortest path routing stage segment, data packets are always forwarded to the base station along the shortest path avoiding the visible area. However, once the detection target moves to a new position, the protocol the entire network will be flooded multiple times, which greatly increases the network energy consumption. At the same time, data packets are transmitted from the phantom node to the base station across the shortest path. Since the distance between each node and the base station is fixed, it increases the possibility of the attacker to track the source nodequickly.

Mahmoud *et al.,*proposed a method based on phantom single-path routing source Location Privacy Protection Strategy (PSRMPN, strategy of source-location privacy preservation in WSNs based on phantom single-path routing), this strategy increases the number of hops in the h-hop limited flooding phase and increases the number of phantom nodes. However, the maximum jump value of this strategy is relatively fixed, and the distance between the phantom node and the source node is extended by increasing the minimum jump value, which can reduce efficiency of the phantom node and increases the energy consumption and also causes delay in the network. The work proposed by Mehta et al.,, PSRMPN transfers data packets from the phantom node through the shortest path sent to the base station. Ouyang et al., proposed the method of periodic acquisition and source simulation to protect the privacy of the source location, but this method will generate huge energy overhead, real- time performance islow.

From the above works, it can be seen that source location privacy protection has experienced a great improvement; techniques like fake sources, phantom nodes, random walk, and the weight have been developed. However, these techniques are only used in a simple way, but give us an inspiration.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

III. PROPOSED RESEARCH METHODOLOGY

Previously, out focus was on the source location privacy problem in WSNs, a hot research topic in security, and propose A Probabilistic Source Location Privacy Protection Scheme (PSLP) for WSNs. A more powerful adversary, which can use Hidden Markov Model (HMM) to estimate the state of the source, is considered in this study. To cope with this type of adversary, phantom nodes and fake sources, which are responsible to mimic the behaviour of the source, are utilized to diversify the routing path. Then, the weight of each node is calculated as a criteria to select the next-hop candidate. In addition, two transmission modes are designed to transmit real packets. Source location privacy protection strategy based on phantom single-path routing strategy is proposed in this paper, and it is divided into two parts:

3.1Phantom single-path source location protection protocol for multiple phantom nodes Similar to PUSBRF, this routing protocol is divided into two stages. In the first stage, first the source node performs h_{walk} hop finite flooding, and then the node i within the h_{walk} hop from the source node divides its neighboring nodes into two sets: *parent* and *child* , where the node in *parent* is away from the source node The minimum number of hops is greater than the minimum number of hops from *i to the* source node; the minimum number of hops from a node in *child* to the source node is equal to or less than the minimum number of hops from ito the source node. Then, the source node and each subsequent node randomly select a node from the set *parent* of its neighboring nodes as the forwarding node of the next hop, and perform random directional routing to the phantom node, so as to ensure that the phantom node can try its best Stay away from the source node. It would not be effective for the previously built trust-based packet filter to work in such a collaborative environment, since the process of trust computation can be easily compromised by insider attacks and low energy efficiency because of more routing and route selection.

3.2Proposed Dynamic Multi-node Selection based on Phantom Routing Protocol

In this paper proposed a strategy for Dynamic Multi-node Selection based on Phantom Routing Protocol (DMSPRP). The protocol enables the selected phantom node to maintain a certain angle and the distance that is well enough to evenly get distributed around the source node, and the routing path is diversified through multi-node selection, which greatly reduces the possibility of overlapping paths capability. Phantom routing strategy is depicted in Figure 2. Taking into account attackers with stronger visual capabilities, this protocol reduces unnecessary flooding by shielding the routing selection of nodes in the visible area. And restore the node state after the detection target leaves. The simulation results show that the protocol can provide better security performance and consume less energy.

The DMNPRP strategy proposed in this research is mainly divided into three phases: 1) limited flooding phase, 2) directed routing phase and 3) multi-node selection forwarding path by stage. In the above 3 steps, unnecessary flooding is reduced in the limited flood reduction stage, which saves energy and reduces the probability of source node being discovered. Directed routing and multinode routing increase the difficulty of reverse tracking by the attacker and prolong the security time, effectively protecting the location of privatenodes.

3.3Routing Protocol Description

The routing algorithm flow in this paper mainly includes has 4 stages; network initialization, selection of phantom nodes, shortest distance routing from real source nodes to phantom nodes, and the probabilistic forwarding route from the phantom node to the base station. In this paper, the phantom node adopts a probabilistic forwarding route to the base station, so the attacker cannot use the influence of the visible area on the routing path.

3.3.1Modified Network Initialization for Phantom Routing Protocol

As shown in Figure 2, the dark shaded area in the figure is PSA divide the entire PSA into μ parts evenly, and each part has an angle of $\varphi=2\pi/\mu$, which are defined separately, namely area1, area2,...,area μ. When the source node performs data packet transmission, first select an area areaλi, λi obeys [1, μ] with then generate the angle β, β obeys [(λi-1)φ, λiφ] random distribution; then produce the distance d, d obey [Rmin, Rmax] random distribution.

The relative position of the determined phantom source node is (Source.xd+dcos(β), Source.yd+dsin(β)). Because the location of the phantom source node is randomly selected, there may not be a node in the desired area.

If there are no nodes in the desired area, then the last hop node on the route to the selected location will become the phantom source node. In order to make the generated phantom source nodes more evenly divided at the same time, multiple phantom source nodes generated continuously and they will not be concentrated in a certain area,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

when the real source node selects the area in a data packet transmission the nodes within area λi (λi=1, 2,...,μ) they are used as phantom source nodes, so the neighboring area of area λi will not be selected in the next packet transmission. The nodes within the selected are used as the phantom source nodes, and the subsequent k (k≤(μ/4)) data packet transmissions will not select the nodes in the area areaλi as Phantom source node. In other words, the integer λi is randomly generated during the i^{th} packet transmission not only satisfies |λi−λi-1|>1, but also the subsequent i+j.

The second data packet transmission satisfies λi≠λi + j, j = 1, 2, 3... k. when the interval of [Rmin, Rmax] is set to be larger, the phantom area is larger, that is, the distribution of phantom nodes is more dispersed, and the distance from the true source node will be farther. Therefore, the phantom nodes generated in this paper can be distributed almost uniformly and randomly throughout the monitoring network; greatly increasing added the difficulty for the attacker to trace the true source node.

3.3.2Analysis of PrivacyProtection

In the WSN source location privacy protection strategy using phantom routing, the distribution of phantom nodes is very important. If the phantom nodes generated by the algorithm have the lesser proximity to the real node, the attack can easily locate the real node. In addition, the length of the packet routing path and random mechanism also affects privacy protection performance and communication performance. The distribution of phantom nodes in the WSN source location privacy protection protocol will be based on phantom routing. If the phantom node is too close to the source node or the distribution of phantom nodes unevenness will reduce the difficulty of backtracking, and the attacker can easily obtain the location of the true source node. In this article, take random angles and distances select the algorithm, the generated phantom nodes are distributed outside the circular area centered on the source node and the radius is Rmin, and the time-series adjacent data packets aregenerated.

Phantom nodes are separated by a certain distance. During the i^{th} packet transmission, the random integer λi generated not only satisfies |λi-λi-1|>1, but and in the subsequent $i+j^{th}$ data packet transmission satisfies λi≠λi+j, j=1, 2, 3...k. Therefore, the phantom festival of the selection of two sequentially adjacent packets the minimum angle between the points is Δφmin= 2×(2π/μ), then the minimum distance of the generated phantom nodes in the ground.

In different application environments, by selecting appropriate parameter values μ, RminsandRmax, the distribution of phantom nodes can be effectively controlled. Each node divides the neighboring nodes into 3 sets according to the minimum hop value from the base station: i.parent, i.brother, and i.child.

3.3.3Limited Flooding

The source node hw hop limited flooding is the basis of hxhop directed routing. In this protocol, hw =hmax, hmax is the maximum number of hops from the phantom node to the source node. At the end of the source node's limited flooding, each node i within hw hops from the source node obtains the distance between itself and its neighbors from the source node minimum jump value and angle. As shown in Figure 2, the angle is from the source node to the phantom node and the source node to the angle between the straight lines and the base stations. By comparing withthenumber of hops of the source node, the minimum hop value of the node in is _child from the source node is greater than the node i from the source node the minimum number of hops.

$$\alpha i = \arccos\frac{H^2+h_{i.s}^2-h_{i.b}^2}{2\times H\times h_{i.s}^2}$$

When the target is detected in the nearby area, the data source node jumps to the node within its hw range. The process of broadcasting message is similar to the flooding process of the whole network. Including messages type, node ID, angle αi, hs represent the hop count of the message, and the initial value is 0. The message arrives when each forwarding node adds 1 and counts to hw, the node no longer broadcasts the message. When node i connects when a broadcast message is received, it records the value of αi in the message, and calculate the value of its own angle αi according to formula (1), and then forward it to neighboring nodes. If hs≤r in the received message, then look up the node information in the set i.parent according to the ID number in the message. If found in i.parent then mark the node. All nodes marked in i.parent cannot be selected as the next in the multi-node selection forwarding stage jump to send nodes, so nodes in the visible area are shielded by nodes outside the visible area. If the monitored object leaves the monitoring range of the source node, the source node point to send a broadcast message with a hop count of r+1. After receiving the message, the node unmarks the message sending node in i.parent.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

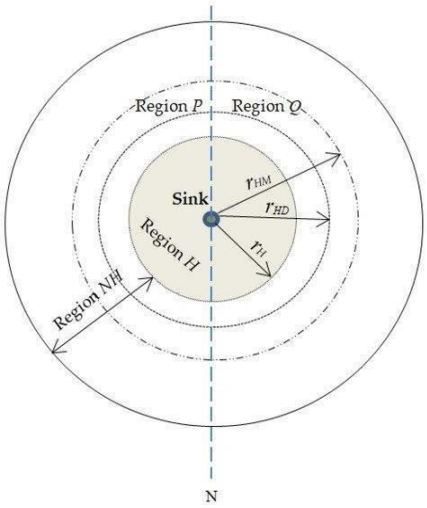

Figure 2. Regional Division

3.3.4Directional Routing

After the finite flooding ends, it divides the area around the source node into n parts, where n is an even number, and the angle of each part is θ=2π/n, and these areas are defined separately.

The domains are A1, A2, A3,...,An, A1 is adjacent to An. The source node selects an area Ai when sending data packets and decides based on the currently selected area. The selection range of the next sending area, the number of selection areas is the number of intervals between the current area and the selectedarea.

The minimum interval angle is Δβ =(k+1)×θ, and the selection range of the sending area is {Ai+k, Ai+k+1, Ai+k+2,..., Ai+k+m-1}. If the source node sends a data packet for the first time, it randomly selects one of the n areas as the send area. The data packet sent by the source node contains the forwarding hop number hx and the angle range [(i-1)θ,iθ], and hx obeys [hmin, hmax] random distribution. If node i receives a data packet, i randomly selects a node from _child, and the angle α of the node is within the angle range of the data packet and then forward the data packet to the node. Repeat this process until the packet is forwarded h times. As shown in Figure 2, the area around the source node is divided.

There are 8 copies, the minimum interval angle is π/2, and A2 which is the current area, then the selection range of the next data packet sending area is {A4, A5,..., A8}. It can be obtained when n tends to infinity, the minimum interval angle $\Delta\theta\min = \frac{\pi}{2}$

$$\lim_{n} \infty \left(\frac{\frac{n}{2}+\propto}{2}\right) . \frac{2\pi}{n} = \frac{\pi}{2} , \alpha \epsilon \{0,1\}.$$

Selecting the transmission area of the next hop data packet from the selection area can ensure that the angle of the transmission interval between adjacent data packets is at least π/2. This makes the number of neighboring phantom nodes generated by the packets are separated by a certain distance, which increases the difficulty of the attacker's reverse tracking and prolongs the security time.

Algorithm 1. Global Flooding Algorithm

1: Case global flooding:
2: if (node i receives the message for the first time) then
3: Record the information contained in the message and broadcast it; 4: else records the information contained in the message and then discards it. 5: Each node in the network can divide its neighboring nodes into 2 sets.

Algorithm 2. Local Flooding Algorithm

1: Local flooding of case:
2: if(hs<=hw)
3: if (node i receives the message for the first time) then
4: Record neighbor node information;
5: hs=hs+1;
6: Calculate the angle αi;

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

```
7: Broadcast the revised message;
8: else records the neighbor node information and discards the message;
9: if(hs<=r)then
10: Search for neighbor node information in the set i.parent;
11: if (find neighbor node) then
12: Mark neighboring nodes in the routing list;
13: else stop flooding;
14: Each node in the random walk area can get a set i.child
```

Algorithm 3. Directed Routing Algorithm

```
1: Case directed routing:
2: Select the sending area from the available areas;
3: Random number hs⊆[hopmin,…,hopmax];
4: if(hi,s<hx) then
5: if(i.child≠⌀) then
6: Select a neighbor from i.child in the angle range
7: Else sends the message to the receiver through the brother selection routing algorithm
```

Algorithm 4. Brother Routing Algorithm

```
1: case brother routing:
2: Select a node i from the set i.parent and i.brother;
3: if (nodei∈i, brother) then
4: if (hl≠0) then
5: if (equal==1) then
6: Check whether the vector satisfies formula (a.b>0);
7: if (vector cannot satisfy formula (a.b>0)) then
8: Select another node;
9: Else is set equal to 1 and sends a message to node i;
10: else sends a message to node i;
11: else select another node from the set i.parent and i.brother
```

Most of the existing wireless sensor network source anonymity protocols cannot take the source location anonymity, delay and life cycle into account at the same time. In response to this problem, this work proposes an energy-balanced and efficient source location privacy protection protocol. The confusion loop is dynamically adjusted to balance the distribution of network energy consumption and maximize the network life cycle.

IV. SIMULATION RESULTS

The strategy proposed by the research were simulated on Network Simulator 2 under Linux environment and compared with EPUSBRF and PSRMPN strategies. For convenience comparing the performance of each strategy, the following simulation scenarios are designed. Suppose there are 10,000 nodes evenly distributed in an area of 6000m×6000m. The communication radius of each node is 100m. Average per the number of neighbours of each node is 8.64. The number of neighbours of a small number of nodes is 3. The attacker's listening radius is equivalent to the node communication radius. View area of the radius is 600m. The limit hop count hl is 10, and the limited flood hop count hw belongs to the set {10, 20, 30, 40, 50}. Directional routing hops hx service Distribute uniformly from [hw-3, hw+3]. Perform 50 simulations for each parameter.

4.1Safety time

The security time is used to evaluate the privacy protection performance of the strategy and is defined as the number of data packets sent by the source node when the attacker finds the source node. Figure 3 and Figure 4 show the safety time brought by different number of directional walking hops when the source node is 60 hops away from the base station. The results show safe time as the number of directional walking hops increases, this is because the distance between the phantom node and the base station is getting longer and longer, the transmission path becomes more complicated, and the attack takes more time to find the location of the source node. At the same time, more phantom nodes are produced,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

which can reduce the possibility of overlapping paths. The safety time of PRABNS increased by 34.7% and 21.7% on average compared with the other two strategies. This is because PRABNS can make magic as the shadow nodes are more evenly distributed around the source node, so that the adjacent phantom nodes are kept a certain distance, and the path is made through the selection of sibling nodes. The path is more diverse. As shown in Figure 4, the safetytimeofthese strategies increases as H increases, because the routing path becomes longer as H increases Now, the attacker needs more time to track down. Compared with the other two strategies, PRABNS increased the safety time by 58.6% and 36.8% on average. So, this strategy can provide better security.

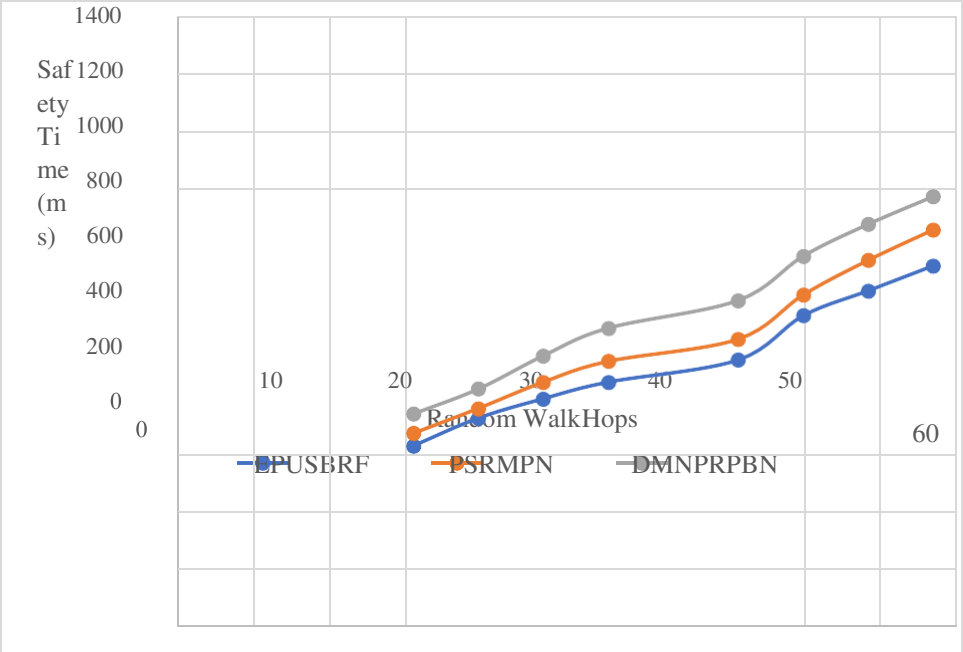

Figure 3. The Safe Time of Different Random Walk Hops

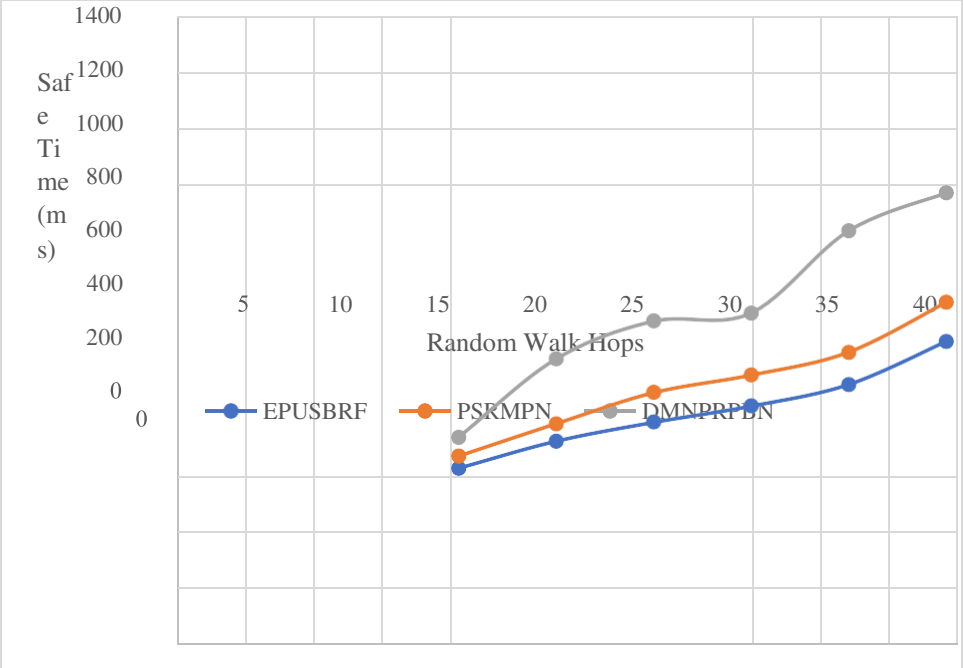

Figure 4. Safe Time of Jumping from Different Source Nodes to Destination Nodes

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

4.2EnergyConsumption

Conventional energy analysis to theoretically obtained energy consumption data **o**r energy of nodes and networks based on theoretical models of system components. It is said to depend on consumption. General energy from the point of nodes Considering that there are deficiencies from the examination of the consumption, in this study, on energy consumption of components in their different states and transitions between states processors, including RF (Radio Frequency) modules and sensors of nodes an energy model is presented for the basic components of the nodes and in the same study, the researchers found that between the energy consumption of the node components it also reveals the relationships and then creates a knot depending on the triggering events.

Finally, the researchers simulated the energy models of the node components. Network protocols based on the node energy model they calculate the consumption. Energy consumption is defined as the number of hops that a data packet is forwarded from the source node to the base station. Figure 5 and Figure 6 show the energy consumption under different H and hw. The energy consumption increases with the increase of H and hw, because the routing path becomes longer with the increase of these two parameters. DMNPRPBN at H = 60, When hw=25, the energy consumption increases by 9.6% and 13%, because the choice of brother nodes increases part of the energy consumption overhead, but this results in longer safety time. While analysing consumption and evaluating communication protocols, nodes it can be used in deployment and also to the developing of different applications they indicated.

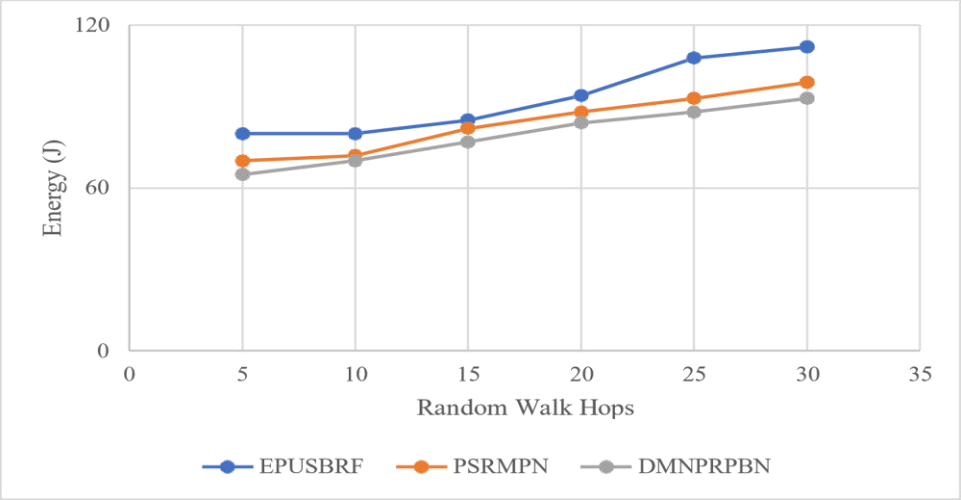

Figure 5. Energy Consumption of Different Random Walk Hops

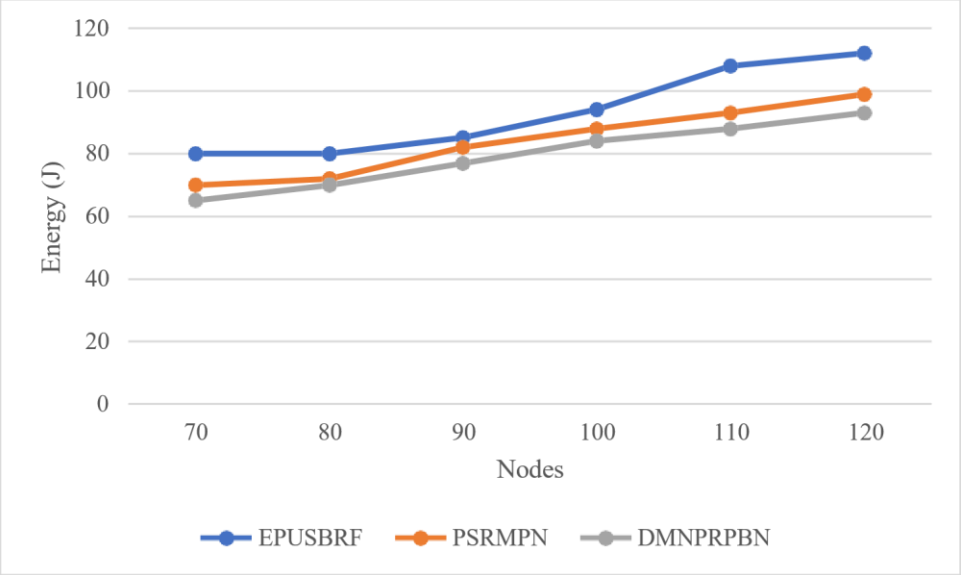

Figure 6. Energy Consumption of Hops from Different Source Nodes to Destination Nodes

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

V. CONCLUSION

Simulation experiment results and theoretical analysis show that: on one hand, the proposed protocol can effectively resist source location privacy attacks with the ability to intercept the entire network; on the other hand, it can balance and optimize network energy consumption and delay, and extend the network life cycle.Considering that the attacker has stronger visual ability, propose phantom routing strategy based on region and sibling node selection. This strategy increases the attacker's the difficulty of point reverse chasing, and extends the security time of the source node, and effectively protects the location privacy of the source node; limited flooding reduces the source node issue. Unnecessary flooding messages save the energy of the node and reduce the probability of the source node being tracked. Overall, the strategy effectively protects privacy of the source node. The goal of protecting the location information of the source node can be achieved, and it does not have any effect on the current routing. The system can be applied flexibly for practical applications (close to the sink and in the source node). As the attacker's ability increases, the network security performance will decrease.

REFERENCES

1. Agir, B., Papaioannou, T. G., Narendula, R., Aberer, K., &Hubaux, J. P. (2014). User-side adaptive protection of location privacy in participatory sensing. *GeoInformatica*, *18*(1),165-191.
2. Chen, H., & Lou, W. (2010, December). From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks. In *International Performance Computing and Communications Conference* (pp. 1-8).IEEE.
3. Chen, H., & Lou, W. (2015). On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. *Pervasive and Mobile Computing*, *16*,36-50.
4. Conti, M., Willemsen, J., &Crispo, B. (2013). Providing source location privacy in wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials*, *15*(3),1238-1280.
5. Du, S., Zhu, H., Li, X., Ota, K., &Dong, M. (2013). MixZone in motion: achieving dynamically cooperative location privacy protection in delay-tolerant networks. *IEEE transactions on vehicular technology*, *62*(9),45654575.
6. Gao, S., Ma, J., Shi, W., & Zhan, G. (2015). LTPPM: a location and trajectory privacy protection mechanism in participatory sensing. *Wireless Communications and Mobile Computing*, *15*(1),155-169.
7. Jia, B., Zhou, T., Li, W., Liu, Z., &Zhang, J. (2018). A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. *Sensors*, *18*(11),3894.
8. Kamat, P., Xu, W., Trappe, W., Zhang, Y.: Temporal privacy in wireless sensor networks. In: Proc. 27th Int. Conf. Distributed Computing Systems (ICDCS) (June2007)
9. Kamat, P., Zhang, Y., Trappe, W., Ozturk, C.: Enhancing source-location privacy in sensor network routing. In: Proc. 25th Int. Conf. Distributed Computing Systems (ICDCS) (June2005)
10. Kido H, YangisawaY, Satoh T. An anonymous communication technique using dummies for location-based services[C]//The 2nd IEEE International Conference on Pervasive Services(ICPS'05). 2015:88-97.
11. Li, Y., Lightfoot, L., & Ren, J. (2009, June).Routing-based source-location privacy protection in wireless sensor networks. In *2009 IEEE International Conference on Electro/Information Technology* (pp. 29-34).IEEE.
12. Li, Y., McCune, J.M., Perrig, A.: SBAP: Software-based attestation for peripherals. In: Proc. 3rd Int. Conf. Trust and Trustworthy Computing (Trust) (2010) 13. Li, Y., Ren, J.: Preserving source- location privacy in wireless sensor networks. In: Proc. 6th Annual IEEE Communications Society Conf. Sensor, Mesh and Ad Hoc Communication and Networks (SECON) (June2009)
13. Li, Y., Ren, J.: Source-location privacy through dynamic routing in wireless sensor networks. In: Proc. 29th IEEE Conf. Computer Communications (INFOCOM) (March2010)
14. Liu, D., Ning, P., Li, R.: Establishing pairwise keys in distributed sensor networks. ACM Trans. Information and System Security 8(1), 41–77 (February2005)
15. Mahmoud, M. E., & Shen, X. (2012, June). Secure and efficient source location privacy- preserving scheme for wireless sensor networks. In *2012 IEEE International Conference on Communications (ICC)* (pp. 11231127).IEEE.
16. Mahmoud, M. M., &Shen, X. (2011). A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, *23*(10),1805-1818.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006210|

17. Mehta, K., Liu, D., Wright, M.: Location privacy in sensor networks against a global eavesdropper. In: Proc. IEEE Int. Conf. Network Protocols (ICNP) (October2007)
18. Mehta, K., Liu, D., Wright, M.: Protecting location privacy in sensor networks against a global eavesdropper. IEEE Trans. Mobile Computing 11(2), 320–336(2012)
19. Ngai, E. C. H., &Rodhe, I. (2013). On providing location privacy for mobile sinks in wireless sensor networks. *Wireless networks*, *19*(1),115-130.
20. Ouyang, Y., Le, Z., Chen, G., Ford, J., Makedon, F.: Entrapping adversaries for source protection in sensor networks. In: Proc. Int. Symp. World of Wireless, Mobile and Multimedia Network (WOWMOM)(2006)
21. Ouyang, Y., Le, Z., Liu, D., Ford, J., Makedon, F.: Source location privacy against laptop- class attacks in sensor networks. In: Proc. 4th Int. Conf. Security and Privacy for Emerging Areas in Communications Networks (SecureComm) (September2008)
22. Ozturk, C., Zhang, Y., Trappe, W.: Source-location privacy in energy-constrained sensor network routing. In: Proc. 2nd ACM Workshop Security of Ad Hoc and Sensor Networks (SASN) (October2004).
23. Rios, R., &Lopez, J. (2011). Analysis of location privacy solutions in wireless sensor networks. *Iet Communications*, *5*(17),2518-2532.
24. Song, J. H., Wong, V. W., &Leung, V. C. (2010). Wireless location privacy protection in vehicular ad-hoc networks. *Mobile Networks and Applications*, *15*(1),160-171.
25. Tan, W., Xu, K., &Wang, D. (2014). An anti-tracking source-location privacy protection protocol in WSNs based on path extension. *IEEE internet of things journal*, *1*(5),461-471.
26. Yin, C., Xi, J., Sun, R., & Wang, J. (2017). Location privacy protection based on differential privacy strategy for big data in industrial internet of things. *IEEE Transactions on Industrial Informatics*, *14*(8),36283636.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details