A Secure Communication and Location Privacy in WSN Using Grey Wolf Optimization

N. Padmapriya¹, S. Subathra²

¹Associate Professor, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram.
²UG Scholar, Department of Computer Science and Engineering, IFET College of Engineering, Villupuram.

¹priyasifetcse@gmail.com, ²subathrasakti@gmail.com

Abstract. Wireless Computing draws in huge speculations, while simultaneously client necessities are ceaselessly expanded. Additionally development in remote advancements should stay up with aforementioned fields, so as to encourage the mix of imaginative administrations and applications in ordinary correspondence of the system. In the proposed framework we upgrade the security instrument for every sensor node by utilizing GWO(Grey wolf optimization) algorithm, and then the dummy sources are created to deceive the adversary and thus the original source is secured.

1. Introduction

A Wireless device Network consolidates a few gadget hubs and protocols that is the basis of service like information validation, event awareness, and hub charging. These hubs assume the job of PC and square measure dispersed in shifted situations. There square measure ton of information transmission and communication between the device nodes, therefore the nodes square measure secured from the mortal.

Security of WSNs involves several aspects, like information Privacy and site privacy. information privacy will be protected by victimization algorithms whereas location privacy can not be protected to the intense. Time correlation in information transmission between 2 nodes, the person will collect location info through analysis. From a time correlation point of view, privacy of the location comprises of location privacy of the source and the sink. Given the significance of the supply, we tend to specialize in the supply location privacy that is Associate in nursing outstanding analysis topic within the field of privacy. Many units of techniques are there, like secure routing, dummy sources, phantom nodes, fake cloud, and cluster which can be applied to safeguard the location privacy of the sink.

The proposed PSLP has exhibited a higher performance than other recent schemes in our simulations with regard to increasing the safety time even as balancing the energy consumption. The main contributions of this paper are:

1) The proposed PSLP is a combination of phantom nodes and fake assets, which strengthen the security of the location privacy.
2) Hidden Markov Model is used by the nearby enemy to calculate the domain of the supply.
3). Based on the distance among the supply and the sink, Two facts transmission modes are built up which further strengthen the privacy of the source area.
Figure 1: Panda-Hunter model

In the existing system securing the source location was the only aim. GPS tracking based system is possibly used in existing system. Also sensor based and camera based tracking system are used in existing system. The disadvantage in the existing system is GPS system was not accessed by all the time. And also hidden markov model is used it only prevent the source location so the sink node is easy hacked by the adversary. Larger number of sensor nodes is used to cover the region it may lead to overlapping of sensor nodes. The intruder normally starts from sink node and calculate the angel between each sensor node. The intruder starts the time and waits to receive the packets. If the intruder isn't capable of hear a new message and the timer is expired, the attacker needs to roll lower back to the preceding node and delete the preceding node from memory. Adversary record the information about the current sensor node to avoid repeating in their path. In the proposed system the GWO algorithm will be used to create fake sources and redirect the adversary to the wrong path. And using this algorithm it increase the time duration by directing adversary to longest path. The system focuses on the problem of finding the Intruder to source state vector. A huge number of sensor nodes are distributed over the network. The distribution of the sensor nodes is uniform for obtaining maximum coverage of the entire network. This method will be more efficient and the availability of the network will be increased by the optimization process.

2. Related Works

J.Koh, D.Leong, G.Peters and W.Wong 2017[1]. Proposed that initially duplicate energy will be dynamically supplied and it will be deployed among the sink. Based on the flooding concepts the sink chooses the false resources. A good location privacy is supplied with an enormous amount of energy is consumed in these set of rules. To cope with this, every other set of rules referred to as dynamic single route routing set of rules (DynamicSPR) changed into proposed. By using directed random walk, the nodes which are away from the energy supply will be selected as a false node, which greatly decreases the power consumption.
R.Manjula and D.Raja 2018[2]. Two-segment routing approach the usage of multiple digital resources to offer enhanced supply location privateness in WSNs. The concept of escape- attitude and random walks are based on the potential power. The packets are directed to the bottom station via various digital assets which are placed at various positions in the network. The major idea of this work is to make use of the excess power in the non- hotspot regions in the network community which helps in generating dispersive path between the source node and the digital assets. Without obstructing the network lifetime the safety period can be extended. Mathematical models are used to determine the overall energy consumption that sustain at each node

Yiting Wang 1, Liang Liu , and Wenzhao Gao 2019[3] proposed an algorithm that is primarily based upon Circular Trap (CT), which combines the MAC layer and routing layer to supply SLP safety for Wireless Sensor Networks. With the help of Time Division Multiple Access it assigns time slots for every node that are present inside the community, which avoids the loss of records due to channel collisions.

Aparna Gurjar, A.R.Bhagat Patil 2013[4]. Context primarily based privateness safety in WSN to hide the location data of the sensor nodes. Using cluster based totally anonymization the scheme hides the real node identities during communication, by way of replacing them with random identities generated by way of the cluster heads. The diploma of privateness of WSN is analyzed the use of entropy based totally method.

S.Sivashankari, M. Mohamed Raseen 2013[5]. Proposed a method similar to k-anonymity and personal data retrieval. In Ubiquitous computing the location privacy of the users’ may be weakened by an alert from the wireless signals form users’ device. To overcome these issues random delay and dummy traffic are directed. In our device networks the location privacy falls in addition to the final framework of location privacy.

Pandurang Kamat, Yanyong Zhang, Wade Trappe 2005[6]. In the panda-tracker model, the point of securing source area is to keep the enemy from assaulting the objective. For example, endangered pandas in the natural life assurance consistently have persuasive market value. WSNs see the data which is connected the panda's life propensities and other significant logical proof. The tracker may utilize traffic examination method to follow the source hub.

Jian Wang, Fengyu Wang, Zhenzhong Cao, Fengbo Lin 2017[7]. A scheme based on a directed random walk becomes adopted. The direction records of the actual packet rely upon on exceptional phantom nodes. This paper proposed the EDWOW scheme to transmit packets with random hops across the ring. A plan dependent on a coordinated arbitrary walk is adopted. The bearing records of the actual packets depend upon on exceptional phantom nodes. EDWOW scheme to transmit packets with random hops across the ring is proposed.

A. Gupta 2017[8]. The key idea is to allow sensor coverage areas to overlap and to reduce the number of sensors head. Wide area is used to prevent the source location privacy.

R. Mayank, K. Sajal Das 2017[9]. Traditional security mechanisms, like encryption, have been proven to be ineffective as the location of the source can also be revealed by analyzing the traffic flow in the network. In this two modifications is proposed MSS, Mule-Saving-Source-Shortest Path (MSS-SP) and Mule-Saving-Source-Two Level (MSS-TL)

L. Mutalemwa and S. Shin 2018[10]. The scheme makes use of a hard and speedy of fake supply nodes to behave as actual resources. The dummy sources generate packets to model the community site visitors in a manner that confuses an adversary thru diverting interest far from the actual supply. Fake packets are of the same length as the actual packets, and they're encrypted with a purpose to make it difficult for adversaries to tell the difference between dummy and actual packets. Several
variations of dummy deliver routing exist, along with short-lived fake supply routing, persistent dummy supply routing, dynamic dummy deliver routing, and a allotted answer that combines dummy supply routing and phantom routing.

3. Framework methodology

Our proposed method overcomes the disadvantages present in the existing method. Tracking Source by Intruder (Attacker) involves detection and localization of the source of interest by processing the information provided by the sensing relay nodes along with their location. First analyse whether any nodes are attacked by the adversary if detection is confirmed then prevent that particular node before the hacker is reaching to the sink node because each sensor node has information about the neighboring nodes so the information may gained through the attacked neighbours node. So it is prevented by blocking the particular node using the algorithm. The Sink node does not send any information or path to reach the destination part to the attacked node. Suppose before identifying that the sink node is attacked then the adversary reaches to the sink node easily and reach to the source location. So to prevent that source from the adversary fake sources are created to confuse them and mislead them to the wrong path. To create a fake sources GWO (Grey Wolf Optimization) algorithm is used. In proposed system longest path is selected to create a fake source so that the time duration of misleading the adversary is increased. Using less number of sensor node it covers a wide area by using the optimal random placement. Our proposed method gives a better solution to evaluate the state parameters of the intruder. It also tracks and safeguard the source and the same is associated with the location in the border of WSN.

**Network Initialization:** Network initialization is used to find how many nodes are used and where to place the each node for the wireless communication. Distribute the nodes to cover a maximum area to secure the source location.

**Optimal Random Placement:** Optimal Random Placement is used to locate the sensor in 90° distance. First node is placed and then with the 90° distance another sensor node is placed and then another node so on in triangular based so that we can minimize the overlapping. By using this we can cover larger area with minimum node

**Triangular Based Sensor Deployment:** In Triangular based sensor, if any node is placed in random place without the triangulation and tri-lateration the sensor nodes placed are reset to align the sensor node in a triangular so that we can avoid overlapping. Using this triangular based sensor method it adjust the sensor distribution and predict the distance between each sensor nodes. We can estimate the number of sensor nodes used to cover the desired area. The trilateration is used for tracking the objects. If any movement is identified calculate the distance between closest nodes. The detection is held only at the second intervals.

![Triangular based Deployment](image.png)

Figure 2: Triangular based Deployment.
Intruder tracking:

When the adversary reached the any of the sensor node, he can easily reach the sink node. When the sink node is reached, they call the emergency protocol and hide the activated source and create the fake source to deceive the adversary. This intruder tracking gather the information from the sensor nodes and generate to the base station for preventing the original location source. The major role of this intruder tracking is to detect the adversary and track the objects and report the directions and speed of the tracker to the base station.

Figure 3: Information passing among neighbours

The information gathered from the neighbours sensor nodes are forwarded through multiple nodes and a gateway. Each node communicate with other node wirelessly.

Figure 4: Managing conflicting resources

Figure 5: Track Generation.

Track generation is one of the most important application in which sensor nodes reveal and report the positions of moving items to the application's person with a minimal latency. In the above given figure sensor nodes are placed and the information passes among the neighbours node. When the attacker try to reach the source fake sources are created and deceive to the dummy sources. And keep away the attacker from the original source.
The data which are tracked by the adversary are sent to the sink node for further process. The following are the components used by the adversary to track the applications are:

- **Node Localization**: It is used to permit the sensor nodes to determine their place.
- **Intruder Localization**: It determines the Intruder's vicinity at regular durations of instances using strategies together with triangulation and tri-lateralization.
- **Timing Synchronization**: Synchronization in time domain among node and Intruder.

The intruder starts to gather information from the sink node, if there are no messages from nodes and intruder has to wait until the messages receive. Flooding is created to blast ring. The original sink node is within the ring. The purpose of this ring is to consume the energy. Backtracking to the previous node the intruder realizes that the packets are transmitted from all the nodes. In location privacy forward the packets by using the scheme FRW (forward random walk) to the neighbouring nodes.

**GWO ALGORITHM:**

GWO (Grey wolf Optimization) algorithm is mainly used for security purpose of each node. Each and every node contains information about the neighbour node so that the data are transmitted to another node. This is simulated by categorizing the search agents; it is responsible for decision making. This algorithm is based on the hunting mechanism that has alpha, beta and delta. First it analyse information from the sensor nodes and then decide the path to transfer the information to the sink node. Using this algorithm block the sensor nodes to stop the leaking of data to the adversary. The alpha produce the best path to transmit the data packets and second is beta and then the third far most place is delta. Using this algorithm it updates the position of each and every sensor nodes with the help of alpha, beta and delta towards adversary.

**Low Cost Localization Protocol:**

Using this algorithm the attacker is misled to the wrong path. When the attacker tracks any one of the sensor he can easily reach the sink node. So to prevent the source first search which node is cracked and then neighbouring nodes are blocked to avoid getting the information about the source node. In case if the sink node is reached by the attacker then using this algorithm fake sources are created and mislead in that way. Information transformed by one sensor node to the nodes is encrypted.

GWO algorithm is incorporated to spot the precise role of unknown nodes, as a way to manage the node localization problem. Minimal localization is applied to analyse the efficiency of GWO rule. This hunting mechanism consists of alpha, beta, delta and omega. The looking and searching manner is usually governed through the alpha, the beta plays a less essential role, and the delta plays a far less role. All of the other grey wolves switch their role to the alpha if intruder receives the excellent. It ought to be stated that, in real searching and looking procedures, the fine position is nearest to the prey, even as in optimization for a global premiere of a given problem, the satisfactory role is the maximum or minimum of the health value underneath given restrictions.

**Advantages of proposed system:**

1. Difficult to identify the source nodes.
2. Increase the time duration to reach fake sources by showing the longest path.
3. Overlapping can be reduced in the sensor node by using the triangular based deployment.

**Performance Metrics**

This process is executed by NS 2 tool. By the usage of this language we will execute the security for the each and every node. And the longest path algorithm can be used to mislead them in maximum distance to prevent the source location privacy.
Figure 6: WSN environment

Here the node4 act as a sink node and node 0 act as a target node i.e. intruder. At very first node 15 act as original source when the intruder tries to reach the original source location dummy sources are created to deceive the intruder. Here the created dummy sources are the node 20, node 13 and node 24. The alternative paths are longer than the original path.

**Packet Delivery Ratio:**

The packet delivery is increased in the proposed system when compared to existing system. It is defined as the ratio of the number of the number of packets sent by the source to the packets received at the destination.

Figure 7: Packet Delivery Ratio

There are lots of challenges regarding this detection process. First the number of nodes used in coverage area. Second optimize the nodes in particular area uses diverse platform and difficult to find security solution for them. Third now threats are become more and more complex and used various obfuscation techniques to bypass detection techniques. This is a simple parametric model for binary classification where examples are classified based on their distance from a hyper plane decision boundary.
Energy Consumption:

The sensor node lifetime is increased so that energy consumption of each sensor is reduced when it is not in use. A WSN consists of many sensor nodes which sense physical phenomena or collect data from an environment. Depending on a predefined application of a network, sensor nodes can be located in fixed places or distributed randomly over a large geographical area.

Average End to End Delay:

The delay is reduced in the proposed system when compared to existing system. It is well-defined as the average time taken for a packet to be transmitted from the source to the destination.

Throughput:
The throughput is increased in the proposed system when compared to existing system. It is defined as the total amount of data, that the destination receives them from the source which is divided by the time it takes for the destination to get the final packet.

5. Conclusion

We Proposed a Grey Wolf Optimization (GWO) algorithm. A powerful adversary which utilizes source privacy protection is considered in this project. To deal with it, phantom nodes, dummy sources, and weight are adopted to change the packets transmission directions. Considering the space between the supply and the sink, two forms of routing modes are designed.

References:

[1]. J.Koh,D.Leong,G.Peters, and W.Wong, Preserving Probabilistic Routing for Wireless Network,“IEEE paper 2017.

[2]. R. Manjula and D. Raja, “A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs,”Pervasive and Mobile Computing,vol.44,pp.58-73,Feb.2018.

[3]. Yiting Wang , Liang Liu and Wenzhao Gao, Efficient SLP algorithm based on circular trap,2019.

[4]. Aparna Gurjar , A.R. Bhagat Patil “cluster based ananomization for source location privacy in WSN “,978-1-4673-5603-9/IEEE-2013.

[5]. S.Sivashankari, M.Mohamed Raseen,Trust management on location privacy and minimising
the error rate in WSN".978-1-4799-0935-3@2013 IEEE.

[6]. Pandurang Kamat, Yanyong Zhang, Wade Trappe, Celal Ozturk, Enhancing Source-Location Privacy in Sensor Network Routing, @IEEE 2005.

[7]. Jian Wang, Fengyu Wang, Zhenzhong Cao, Fengbo Lin, Jiayan Wu, Sink location privacy protection under direction attack in wireless sensor networks, Wireless Networks, Vol. 23, No.2, pp: 579-591, Feb. 2017.

[8]. A. Gupta, C. Gui, and P. Mohapatra, —Mobile Intruder tracking using sensor networks, in Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Direction, R. Shorey and A. Ananda, Eds. Wiley, 2006.

[9]. R. Mayank, and K. Sajal Das, “Using datamules to preserve source location privacy in Wireless Sensor Networks,”Pervasive and Mobile Computing, vol. 11, pp. 244-260, Apr. 2014.

[10]. L. Mutalemwa and S. Shin, “Strategic Location-Based Random Routing for Source Location Privacy in Wireless Sensor Networks,”10.3390/s18072291 @2018IEEE.