ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 1, 2025

A Privacy Protection Strategy in Unguided Sensor Networks

*A Bhasha[1], Dr. N Krishnaiah[2], Dr B Laxmikantha[3], K Radha[4]

2Professor, St. Martin's Engineering College, Secunderabad, Telangana – 500100

1, 3, 4Assistant Professor, St. Martin's Engineering College, Secunderabad, Telangana – 500100

*Corresponding Author

Email: abhashait@smec.ac.in

ABSTRACT

Computing and communication have advanced dramatically as a result of recent developments in wireless sensor networks (WSNs). Security has not yet received the same priority to match these changes. In this study, we concentrate on the WSNs' source location secrecy problem, a current security development area, and provide a privacy and security technique in WSNs. This approach considers more powerful opponents who can evaluate the situation at the origin using a hidden Markov model. To deal with this sort of opponent, fake sources and phantom nodes are used to divert the transmission path by mimicking the actions of the origin. To choose the candidate for the next step, each access point's weight is employed as criteria. Moreover, transmitter and receiver modes are intended to send original packets. According to the computation results, the suggested privacy protection strategy increases safety while using less energy.

INTRODUCTION

Wireless Sensor Networks (WSNs) are made up of numerous protocols and sensor nodes that serve as the foundation for services such as Authentication of information, node charging, and event awareness. These nodes operate as distributed microcomputers in a variety of contexts. Many data flows and communication behaviours occur among nodes. Therefore, maintaining security is essential. The security of WSNs represents a variety of factors, including location and data privacy. While location secrecy cannot be completely secured, data privacy can be secured using encryption algorithms.When data transfer between two nodes has a timing correlation, the attacker might extract position information through analysis. In this work, we concentrate on source location secrecy, since it is a brand-new topic of study in the field of security, because of the importance of the source. A number of approaches, including as secure routing, phantom nodes, false clouds, fake sources, and clusters, can be utilized to safeguard the privacy of the source location. In order to diversify the routing path, we present a privacy protection Strategy (PPS) that uses fake sources and phantom nodes.

- Phantom nodes are selected in the vicinity of the source, taking into account the viewable region.
- To decide the next-hop possibility, each node computes and dynamically updates a weight value.
- To mislead the attacker, fake sources are established around the sink to transmit fake packets.

In the preceding techniques, the viewable region is a separate area. The opponent can quickly identify the source when they trace their steps towards this location. The transmission uses both fake and real packets, which are of two different types.The source generates actual packets, whereas fake sources

generate fake packets.To be able to safeguard the origin place, the source's real packets are first routed through a directed random walk to a phantom node. Two transmission possibilities are explored depending on the separation between source and sink. During the transmission of actual packets, fake packets with a predetermined duration are also sent to the sink. In our simulations, the proposed PPS performed better than two other recent approaches in terms of lengthening the safety window while balancing energy usage.

- The proposed PPS includes phantom nodes as well as fake sources, which increases source location secrecy.
- The state of the source is estimated using a Hidden Markov Model by a more effective local adversary.
- The two ways of data transfer those are produced depending upon the difference between the source and the sink increase the privacy of the source location even further.

RELATED WORK

Since Ozturk first put forward his proposal, several researchers have focused on location privacy. Location privacy has recently been the subject of much research in social networks, automobile ad hoc networks, cloud computing, industrial wireless sensor networks, and so on. Both the sink and source location are covered by location privacy. To keep the location of the source secret, Manjula et al. used virtual sources. A routing technique was recommended in their plan to increase the safety time. Nodes present in non-hotspot locations took part in the creation of several routing paths by incorporating random walk into the routing procedure. As a result, the safety time was increased but the network lifespan remained same. To safeguard the secrecy of the source location, Matthew et al. developed two techniques employing fictional sources. Fake sources were dynamically placed near the sink in the first algorithm. The sink then chose false sources by flooding. Good source location privacy can be obtained with this approach, despite the cost of significant consumption of energy. Another technique, the Dynamic Single Path Routing Algorithm (DynamicSPR), was presented to address this. The energy usage was greatly lowered by selecting nodes far from the source as false sources using directed random walk. However, because fake sourceswere dependent on where the source and drain were in relation to one another, sensor nodes nearby might use up all their energy. To protect location privacy, Jing et al. took into account a more potent adversary and proposed a routing method that enhances privacy. A worldwide opponent was discovered in their investigation that used a Bayesian maximum-a-posteriori (MAP) estimation approach to track node-to-node communication. Then, a framework for making decisions was proposed to lower the likelihood that the enemy would be discovered. The difficulty was finally transformed into a parameter adjustment.

To safeguard the source location secrecy, Chen et al. devised a constrained flooding approach and used phantom nodes.The source gathered information on the nodes in the restricted flooding area by using restricted flooding. The role of the source was then mimicked by choosing nodes to act as phantom nodes on the boundary of the constrained flooding area.Packets transmitted by a phantom node that remained behind the source would first avoid the visible region before taking the shortest path to the sink. Even though, limited flooding was used regularly, this may not be acceptable for a network of this scale. To protect the secrecy of the source location, Li et al. proposed a solution including a ring and random intermediary nodes. The authors first presented the standards form ensuring the quantitative information leakage from the source location. The routing path was then made dispersed by adding random intermediary nodes to lower the likelihood of leakage.Packets were transferred to an intermediate node and then forwarded to a node in the ring surrounding the sink. Before being sent to the sink, packets travelled on the ring for a random hop.

The entire network was separated into regions by Mutalemwa et al., who then developed a region-based transmission method. In this plan, the network's sink was in the middle, and regions were created all around it. A group of carefully chosen relay nodes carried out the transmission between the areas. These tactical relay nodes, which occupied two zones, were in charge of sending packets to the sink. Although being near to the sink, these nodes were dispersed. Too many packets would need a significant amount of energy to relay. As a result, average energy efficiency was low.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 1, 2025

Wang et al. examined the source location secrecy in the face of a novel opponent. The adversary model featured both global and local aspects. In typical circumstances, the attacker was a nearby adversary. The adversary transformed into a global opponent in this region when a plausible location for the source's residence was discovered.To deal with it, a message mapping sharing mechanism was proposed, and the position of the source was hidden by a cloud of numerous false packets. Random routing was used to send each message copy, providing the necessary source location secrecy. The data mule was employed by Mayank et al. to guarantee the source location's confidentiality, while accounting for time correlation during sensor node transfer.When the source was within the data mule's communication range it acted as the mobile data collection unit and gathered data. In this situation, the source location's privacy was moved to the mule's moving track's protection. The authors then put out three expanded angles-based schemes to safeguard the location of the source. Unfortunately, because the mule travelled grid by grid, the mule's safety was not adequately considered. A reduced time correlation research has plenty of room.

Proa et al. presented a traffic decorelation strategy to minimize the danger of an international attacker while also decreasing time correlation during transmission. The transmission delay and communication overhead were decreased by the suggested traffic normalization approach. A circular queue was also used to divide the whole network into a number of minimally linked zones, which may have reduced the number of active nodes during transmissions and the chance of an enemy eavesdropping.. The distance between the source's location and the adversary's expected location was used to calculate privacy in their work.

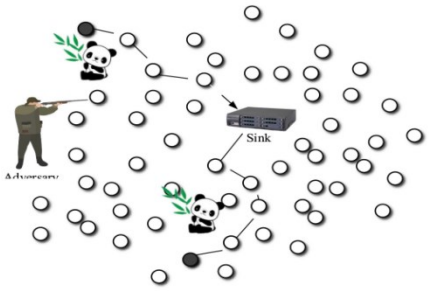

Fig 1. The Panda-Hunter model.

The preceding papers show how approaches such as phantom nodes, phoney sources, weight, and random walk have been developed to protect source location secrecy. The fact that these methods are simply applied in a straightforward manner serves as motivation.

SYSTEM MODEL AND ASSUMPTIONS

Assumptions are dotted across the adversary model and network models in this section, which provides the system model. The safeguarding of endangered wild animals is the background application. The placement of sensor nodes in the wild environment is random. These sensor nodes' placements remain constant after deployment. Then, sensor nodes keep an eye on how animals behave.

a. Model of Network:

The Panda Hunter model provides the foundation for the network model used in this investigation. A WSN made up of numerous sensor nodes is deployed to keep tabs on panda activity, as depicted in Fig. 1. When a panda is found, a sensor node switches to source mode and sends packets via several hops to the sink. Keeping the opponent from discovering the source location is a critical component of privacy protection. As a result, we assume the following:

b. Mode of Adversary:

Due of the source's potential value, the adversary begins at the sink and makes every effort to locate it. The enemy's surveillance range is equal to the sensor node's radius, indicating that it is a local adversary. The

communication range of a common node or somewhat more than it is the limited monitoring range of the local adversary. The local attacker can thus only keep an eye on specific areas of the network. To escape detection by the network administrator, the opponent typically employs passive tactics such as backtracking and listening. In this chapter, we look at a more formidable adversary. In addition to the passive attack, by examining each packet's header, we believe that the adversary is familiar with the kind of packets. Based on its observations, the opponent can then utilize the Hidden Markov Model (HMM) to deduce the possible state of the source for a particular period. The goal of employing HMM to infer the potential state of the source is to make it easier for the opponent to locate the source by using the estimate result rather than wandering throughout the network. This is so that the adversary's scope for locating the source can be reduced by the estimation of HMM.

On the other hand, the opponent is only aware of the source's current status and not its precise location. In this situation, we consider that if the opponent has sufficient network information, the likelihood that he will find the source from the anticipated source state is higher. The basic idea behind our suggested PPS is to broadcast both genuine and fake packets in opposite directions and with unique states. This draws the adversary's focus and diminishes the estimate's accuracy.

A PRIVACY PROTECTION STRATEGY IN WSN:

In this Section we aim to expand the source's potential locations because the opponent might be aware of the source's current status while the source's exact location is still a mystery. The PPS process consists of three steps: identifying phantom nodes in step one; identifying fake sources in step two; and path from the source to the sink in step three. In Fig. 2, a PPS overview is displayed. As stated in the adversary model, the opponent can utilize HMM to assess the present state of the source before undertaking a specific search. The source's potential states need to be expanded as much as possible. Fake sources and phantom nodes completely suit our requirements. The fake source and the phantom node both serve similar purposes, but they are defined differently. The term "phantom node" describes nodes that are close to or surrounding the source and mimics its operation. The term "fake source" can also apply to nodes that mimic the source's functionality.

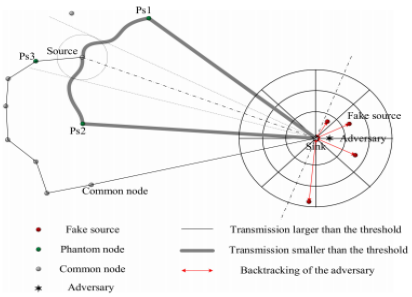

Fig. 2. Overview of PPS.

However, the fake source is located away from the source, towards the sink. The fake source and the phantom nodes are coupled to diversity the transmission routes. Both fake sources and phantom nodes are picked in non-hotspot zones that have no impact on network durability.

a. Phantom Node Determination

Phantom nodes, as previously described, are nodes positioned near to the source to simulate its operation. When we look at how phantom nodes work, we can see that the higher the privacy protection is the more away the phantom node is from the source. This setup's primary goal is to divert the attacker's attention from the true source. Therefore, we opt to choose the phantom nodes using a directed random walk. The direction of packet transmission is fixed in directed random walk. As a result, when the directed random walk ends, the chosen phantom node remains distant from the source. The current node transforms into a phantom node and sends packets given by the source when H hops equals 0. Each time a data transmission occurs, the phantom node is different. Also, the phantom node must remain outside of the viewable region. So the opponent may simply identify the source when it returns to the visible region. Also, during startup, packets are sent from

the source to the phantom node. As a result, it is assumed that the communication between the phantom node and the source is safe.

b. Fake Source Determination

As noted in the preceding description, around the sink, fake sources are created to improve packet direction. Each fake source should preferably remain in its own sector, ensuring that each fake packet travels in a separate route. Because at a particular time, the attacker is aware of the source state, it must study the packet flow to determine the source. As a consequence, source location privacy is protected by diversifying the source location using fake sources. For a set period of time, a node functions as a false source. After the countdown expires, another fake source emerges. During a predetermined amount of time, we think there is just one fake source in order to conserve energy.

C. The Path From the Source to the Sink

The transmission between the sink and true source occurs following the detection of fake sources and phantom nodes. When the sink shows up, the source sends a message to let it know. As soon as the sink receives this message, it chooses a fake source. Given that the source emerges at random, there is a chance that the separation between the sink and the source is minimal. Because the source's initial packet transmission to a phantom node, the significant differences are in phantom node selection and transmission to the sink from the phantom node.

IMPLEMENTATION

MODULES:

i. Service provider:

The service provider will examine the data file, configure the router nodes, and then deliver to the specified recipients. The router gets the data file from the service provider and determines the quickest path to the chosen recipient.

ii. Router:

The router manages many networks and provides data storage. The network has n nodes. The service provider of a router can see information about attacked nodes and node characteristics. The router gets the data file from the service provider and determines the quickest path to the chosen recipient. When a node identifies an attacker, the router connects to alternative node and forwards a message to that user.

iii. IDS Manager:

The IDS Controller in this module consists of two phases. The IDS controller is engaged if the router experiences data integrity issues or malicious activity. The objective is to identify every host that participates in IDS conversations on the monitored network. In order to eliminate network flows that are most likely to be produced by IDS software, we perform a pre-filtering step to the raw traffic we examine from the monitored network's edge in the first phase. The remaining data is then analyzed and a number of statistical characteristics are extracted in order to recognize flows made by IDS clients. Our system analyses IDS client traffic and classifies it as either valid IDS clients, or Malicious Data. There is Malicious Data detection or coarse-grained IDS Integrity in the second phase.

iv. Receiver (End User):

The data file may be obtained by the receiver from the router. A data file will be transmitted by the service provider to the router, which will subsequently deliver it to a designated receiver. The file is provided to the recipients without modification. Only particular data files may be obtained from the network by users.

v. Attacker:

Attacker is a person who injects harmful material into the appropriate node and changes the bandwidth of that specific node. The attacker can trick a node into using bogus bandwidth. After assaulting the nodes, a router will alter its bandwidth.

PERFORMANCE EVALUATION

The four simulation metrics that are assessed and completed efficiently are consumption of energy, safety time, transmission delay and lifetime of network. We begin with a definition for each measure. The time between the adversary determining the source's location and the initial packet transmission of sources is called the safety time. Being more precise, we represent the safety time using the adversary's backtracking hop count. The consumption of energy indicates the average energy cost for each simulation run. The network lifespan is the time between the inception of the network and the demise of the first node. The data processing time and average packet transmission for each simulation run is called the transmission delay.

CONCLUSION

The last ten years have seen a rise in the importance of WSN security research.We concentrated on source location privacy in this study since it is a hotspot for security research, and proposed a privacy protection Strategies technique (PPS) based on WSNs. In this study, a potent foe that makes use of Hidden Markov Models (HMM) is taken into account. The packets' transmission paths are changed using weight, phantom nodes, and fake sources as a solution. Two types of routing modes are generated based on the separation between the sink and the source. As compared to SLPE and DynamicSPR, The imitation results show that the suggested PPS balances the energy consumption of each node and has a better safety time. To safeguard the source location, future research will focus on protecting communication between nodes and minimizing the adversary's observation likelihood.

REFERENCES

[1] H. Lu and J. Li, “Privacy-preserving authentication schemes for vehicular ad hoc networks: A survey,” *Wireless Commun. Mobile Comput.*, vol. 16, no. 6, pp. 643–655, Apr. 2016.

[2] G. Han, H. Wang, J. Jiang, W. Zhang, and S. Chan, “CASLP: A confused arc-based source location privacy protection scheme in WSNs for IoT,” *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 42–47, Sep. 2018.

[3] H. Lu, J. Li, and M. Guinean, “Secure and effificient data transmission for cluster-based wireless sensor networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 750–761, Mar. 2014.

[4] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, “A source location protection protocol based on dynamic routing in WSNs for social internet of things,” *Future Gener. Comput. Syst.*, vol. 82, no. 5, pp. 689–697, Aug. 2018.

[5] H. Lu, J. Li, and H. Kameda, “A secure routing protocol for cluster-based wireless sensor networks using ID-based digital signature,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2010, pp. 1–5.