Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 3, No. 3, 2023

Research on Application of Neural Network Model in Location Privacy Protection of Wireless Sensor Networks

Jintao Liu

Qingdao Academy, Qingdao, China

Abstract: Due to the characteristics of WSN (Wireless sensor network), attackers can easily eavesdrop on data packets transmitted between single or even multiple communication links, and separate sensitive data from multiple sensor information, which poses a great threat to location privacy. Therefore, it is very important to effectively protect the privacy of training sample data while using WSN. Neural network is an important research hotspot in AI field, and it is a model close to biological neural network in machine learning algorithm. In this paper, an application of neural network model in WSN location privacy protection is given. A CNN (Convolutional Neural Network) location privacy protection prediction protocol based solely on additive homomorphisms is proposed, which can effectively ensure that input features, model parameters, and intermediate values are not leaked during the prediction process. The experimental results show that the proposed method has good robustness and can effectively protect the private location of the source node.

Keywords: Neural Network; WSN; Location Privacy Protection.

1. Introduction

WSN (Wireless sensor network) is an integrated information system with the functions of information collection, processing and transmission, which can obtain the target information in real time and realize the information interaction. It has a very broad application prospect in many fields such as military affairs, environmental monitoring and forecasting, health care and so on [1-2]. The characteristics of WSN's own openness and ad hoc network determine its inherent security defects and are vulnerable to various attacks. Once the location privacy information is leaked, the attacker can further destroy or capture the corresponding nodes, thus destroying the whole network; Therefore, it is very important to effectively protect the privacy of training sample data while using WSN. In WSN, according to the different characteristics of source location privacy attacks, they can be divided into the following categories: attack behavior, attack source, attack scale and network information obtained by attackers [3-4]. Neural network is an important research hotspot in AI field, and it is a model close to biological neural network in machine learning algorithm. Neural network constructs a network structure by simulating the structure and function of neurons, simulates the memory function by setting the weights between neurons, and sets the activation function to simulate the stimulation and inhibition function of neurons. In this paper, the source location privacy protection protocol is described by using neural network model, and then an application of neural network model in WSN location privacy protection is given.

2. Research Method

2.1. Source Location Privacy Protection Protocol Foundation

Because of the characteristics of WSN, attackers can easily eavesdrop on data packets transmitted between single or even multiple communication links, and separate sensitive data from multiple sensor information, which poses a great threat to location privacy. For example, an attacker can crack the encryption key to obtain plaintext. If the key of the key node in the network is cracked, the privacy of the whole network may be exposed [5]. Examples of cryptanalysis attacks include ciphertext-only attacks, plaintext-only attacks, plaintext-selected attacks, adaptive plaintext attacks, ciphertext-selected attacks and so on. By eavesdropping on the sensor packets in the whole network or local area, the attacker can analyze the network traffic in WSN, thus analyzing the position and function of sensor nodes, and even locating the key nodes in the network.

The monitoring range of a global attacker is much larger than that of a local attacker, and it can obtain the traffic distribution information of the whole network. The attacker usually uses his own network to monitor the communication in WSN [6]. This type of attacker can accurately draw the path map of message delivery. It is worth noting that, in general, the protection strategy against local attackers cannot effectively resist the attacks launched by global attackers, but the protection methods designed for global attackers can usually effectively deal with the threats of local attackers. In the random walk mechanism, the data forwarding path becomes longer, which leads to long waiting time and high energy consumption. In the face of backtracking attack, the attacker may walk along the random packet closer to the source. Therefore, the random walk mechanism is usually not used alone.

The WSN model used in this paper is composed of a large number of sensor nodes and base stations deployed in a certain area to monitor the activities and positions of designated targets. Once the monitoring target appears in a certain position in the network, the node closest to the target immediately becomes the source node, and the sensed and collected data is periodically sent to the base station by multi-hop. The base station has enough energy and powerful computing and storage capabilities, and we think it is safe enough to be captured by attackers.

2.2. Problem Analysis and Security Strategy

In WSN, the location privacy of the source node is very important. WSN monitoring applications have two main requirements for routing protocols. First, security requirements: routing protocols need to have a long security period to ensure that the monitoring target is not captured by attackers. Second, the delay requirement: the data packet collection delay is small to ensure the freshness and availability of the monitoring data [7-8]. Therefore, for delay-sensitive WSN applications, it is necessary not only to ensure the safety of the monitoring target, but also to ensure that the monitoring information can be quickly transmitted to the base station. Aiming at the problem that the existing source location privacy protection scheme is not effective when the source node appears around the base station, a source location privacy routing algorithm based on neural network model is proposed, which uses constrained selection of intermediate nodes to increase the diversity of paths, and the forwarding of data packets on irregular rings increases the angle of transmission paths, thus improving the security cycle of the network.

Sensor network has the ability of attacker intrusion detection. When an attacker tries to maliciously destroy sensor nodes or tamper with data content and routing information, the detection mechanism can find out its location and remove it. Although the attacker can't crack the specific content of the data packet, the attacker is equipped with advanced equipment and technology that can be used to launch attacks of different intensities to the sensor network [9]. Therefore, the research on attack model is also an important part of the source location privacy protection research. Data fusion is a very effective technical means to reduce data communication between sensor nodes, reduce energy consumption and prolong network life in WSN. Neural network and data fusion have a common basic feature, that is, a large number of data can be calculated and processed to get conclusive results that can reflect these data characteristics. Therefore, neural network can be used to realize and solve the problem of data fusion.

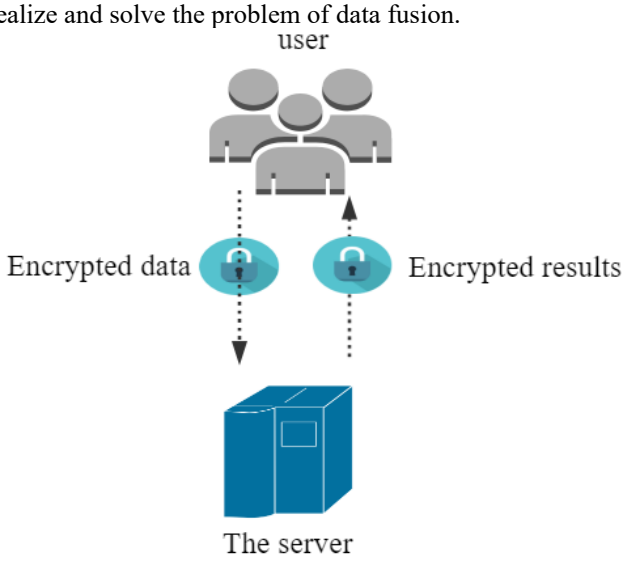

Figure 1. System model

CNN (Convolutional Neural Network) is characterized by parameter sharing and local connection. Compared with the fully connected neural network, CNN has better offset and fewer parameters in the capture position, which can effectively reduce the over-fitting of the fully connected neural network. For the prediction of CNN, this project plans to design an algorithm of CNN location privacy protection prediction protocol based on additive homomorphism to ensure that the input characteristics, model parameters and median value of CNN will not be leaked during the prediction of CNN.

The location privacy protocol of CNN proposed in this paper includes two subjects: user and server, as show in fig 1. In this project, each participant will follow the principle of "semi-honesty" in the process of fulfilling the agreement, but will obtain private information from the agreement.

Having the characteristic matrix $\vec{x}(x_{111},\cdots)$ wants to use its own characteristic vector to make prediction. $[\vec{x}]=([x_{111}],\cdots)$ is obtained by encrypting $\vec{x}$ with its own public key PK, and the ciphertext $[\vec{x}]=([x_{111}],\cdots)$ is sent to the server for prediction. After receiving the ciphertext of the prediction result sent back by the server, it is decrypted to obtain the prediction result.

Have CNN model $(\vec{w},b)$. Based on the ciphertext $[\vec{x}]$ of the user's characteristic matrix and the model parameter $\vec{w},b$ owned by the user, the location privacy protection prediction of CNN is made, and the ciphertext of the prediction result is sent to the user after the prediction is completed.

Because WSN nodes are in various complex environments, self-organized and have limited processing resources, and the security problems are serious [10], WSN nodes are complex systems, and it is difficult to describe WSN nodes with a unified model. Suppose the neuron is static, that is, $H(s)=1$. Then the neuron can be expressed as:

$$\begin{cases} X(t)=AY(t)+BU(t)+W \\ Y(t)=g(X(t)) \end{cases} \tag{1}$$

X is an n-dimensional vector, $g(\cdot)$ is a nonlinear function, and A,B is a connection matrix.

Pre-training model, statistical gradient information, pre-defining threshold parameter C, and then cutting the gradient based on C to ensure that the gradient values of all parameters do not exceed C:

$$\vec{g}_i(x_t)=\frac{g_t(x_t)}{\max\left(1,\frac{\|g_t(x_t)\|}{C}\right)} \tag{2}$$

Security time is the time taken by the attacker to track the location of the source node from the base station, and it is also an important basis to measure the security of the protocol. The base station node is the target node of all data packets, and the data of each data packet is confidential, so the attacker cannot directly obtain the location information of the source node from the eavesdropped data packet.

Therefore, the concept of privacy loss accumulation function is put forward to calculate the privacy loss of accessing training data in each iteration process and the cumulative privacy loss with the progress of training.

In order not to lose generality,

$$\sigma=\frac{\sqrt{2\log\left(\frac{1.25}{\delta}\right)}}{\varepsilon} \tag{3}$$

The algorithm in this paper can greatly reduce the value of ε under the same iterative steps, and protect the privacy of data more.

3. Result Analysis

In order to effectively protect the user's privacy location information in WSN, a model experiment of source node location privacy protection based on WSN is constructed. Assume that 10000 nodes are evenly distributed in the range of 4000m * 4000m, and the communication radius of each node is 100m. The listening range of the attacker is the same as the communication range of the node. In order to train CNN, we adopted Python on a 64-bit Windows system and a tensor stream architecture. Finally, five trained CNN networks are tested with 100 experimental samples.

The amount of transmission in the protocol is determined by the number of interactions and the amount of data per interaction. For the number of interactions in the protocol, in order to protect the activation value and the output of the last layer, each activation layer requires the user to interact with the server once, and each argmax layer requires the user to interact with the server 10 times.

As can be seen in fig. 2, when the activation layer is increased, the number of interactions correspondingly increases, and the transmitted information also increases, and the transmitted information also increases when the number of interacting data increases.

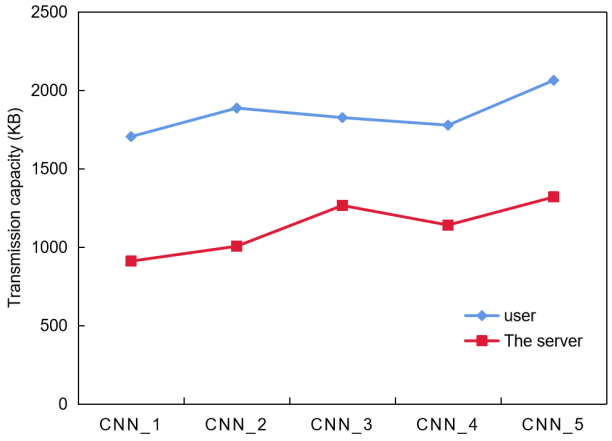

Figure 2. Transmission capacity of location privacy protection protocol

Fig. 3 shows the change of safety time formed by different methods when the number of hops from the source node to the target node changes.

It can be seen that the safety time will increase with the increase of hop count, and the safety time of this method is improved compared with the traditional method, and the effect is obvious, which proves that this method is more practical.

Because the distance between the nodes in the network and the base station is far away, the transmission path in the network becomes more complicated, which makes it take longer for the attacker to find the source point, and the overlapping paths in the network become less. The simulation results show that the algorithm is robust and private to the source node.

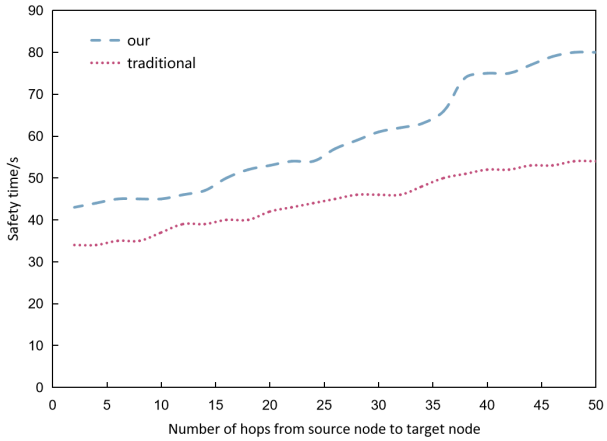

Figure 3. Safe time of different hop counts from source node to target node

4. Conclusion

The open and self-organized nature of WSN determines its inherent security flaws and susceptibility to various attacks. Once location privacy information is leaked, attackers can further damage or capture the corresponding nodes, thereby disrupting the entire network. Neural network constructs a network structure by simulating the structure and function of neurons, simulates the memory function by setting the weights between neurons, and sets the activation function to simulate the stimulation and inhibition function of neurons. In this paper, the source location privacy protection protocol is described by using neural network model, and then an application of neural network model in WSN location privacy protection is given. Experimental results show that this method has good robustness and can effectively protect the privacy position of the source node.

References

[1] Wang H, Han G, Zhang W, et al. A Probabilistic Source Location Privacy Protection Scheme in Wireless Sensor Networks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(6):5917-5927.

[2] He H. Privacy Protection of Node Location and Data in Wireless Sensor Networks[J]. International Journal of Online Engineering, 2016, 12(11):34.

[3] Han G, Miao X, Wang H, et al. CPSLP: A Cloud-Based Scheme for Protecting Source-Location Privacy in Wireless Sensor Networks Using Multi-Sinks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3):2739-2750.

[4] Xue D, Wu L F, Li H B, et al. A novel destination prediction attack and corresponding location privacy protection method in geo-social networks[J]. International Journal of Distributed Sensor Networks, 2017, 13(1):142.

[5] Ye H, Li Z, Liu W, et al. A location privacy protection algorithm based on differential privacy in sensor network[J]. International Journal of Embedded Systems, 2021, 14(5):432.

[6] Huang C, Ma M, Liu Y, et al. Preserving Source Location Privacy for Energy Harvesting WSNs[J]. Sensors, 2017, 17 (4): 724.

[7] Ubaid S, Shafeeq M F, Hussain M, et al. SCOUT: a sink camouflage and concealed data delivery paradigm for circumvention of sink-targeted cyber threats in wireless sensor networks[J]. Journal of Supercomputing, 2018, 74(10):5022-5040.

[8] Jiang S, Li M, Tang Z. A New Scheme for Source-location Privacy in Wireless Sensor Networks[J]. International Journal of Network Security, 2018, 20(5):879-888.

[9] Hudson S M, Taylor J T, Bowen C R. Energy harvesting of cathodic protection currents in subsea and marine structures for wireless sensor power and communication[J]. Applied energy, 2022(15):316.

[10] Wang H, Han G, Zhang Y, et al. A Push-based Probabilistic Method for Source Location Privacy Protection in Underwater Acoustic Sensor Networks[J]. IEEE Internet of Things Journal, 2021, (99):1-1.