PROCEEDINGS OF SCIENCE

Lightweight Security Trust Model for Wireless Sensor Network with Mobile Sink

Hongling Wang[1][2]
China University of Geosciences, Wuhan, 430074, China
East China University of Technology, Nanchang, 330013, China
E-mail: `whl9win@163.com`
Yueshun He[2a]**, Gang Zheng**[2b]**, Lin Liu**[2c]
East China University of Technology, Nanchang, 330013, China
E-mail: [a]`heys@ecit.cn`; [b]`gzheng@ecit.cn`;[c]`lliu@ecit.cn`

Each sensor node in Wireless Sensor Network (WSN) can gather and monitor data in real time with a cooperative mode, and then routes data to the base station in the way of wireless communication after sensing and processing multi-source information. However, owing to the limitation of computing power, energy consumption and their own security condition, sensor nodes often face problems such as the transmission data redundancy, long routing path, failure nodes and malicious node identification and other security issues. According to the characteristics of the Wireless Sensor Network, a lightweight security trust framework was proposed to reduce the communication and calculation workload. The lightweight framework of the Wireless Sensor Network with a mobile Sink node mainly consists of three levels: the routing model of mobile Sink, data redundancy detection model and bidirectional authentication model. In the first place, we present an optimizing node routing mechanism based on the Firefly algorithm. The next, we introduce Simhash method to improve data gathering efficiency. Finally, authentication node trust management mechanism makes the WSN have a low communication risk. This lightweight security model can ensure the Wireless Sensor Network working in high speed and safe operation from a new perspective.

CENet2017
22-23 July 2017
Shanghai, China

[1] Corresponding Author

[2] This study is supported by Science and Technology Foundation of Jiangxi Province Education Department (GJJ150594),Key Research Development Foundation of Jiangxi Province Technology Department (20161BBE50063), Science and Technology Foundation of Jiangxi Province Education Department (GJJ160555)

1.Introduction

Wireless Sensor Network (WSN) is composed of a large number of micro sensor nodes deployed randomly in sensing fields, which aims to evaluate and make decision according to specialized application[1]. The lower cost and better communication capabilities contribute to wide application in medical, military and environmental monitoring fields[2].

Most application fields place a great demand on the security of WSN. As the nodes in WSN are limited to their energy, communication capability, computing capability and own security condition, this is a time of great challenges for WSN. Security trust requirement is stricter in high efficiency, reliability and security, with which the nodes can transmit data to the aggregator real-timely and reliably. For the traditional WSN, nodes around aggregator not only need to transmit their own data to aggregator, but also transfer data to other nodes. Therefore, the workload of nodes around aggregator is much higher than the remote nodes. This unbalanced data transmission mode is easy to result in energy hole and network congestion. Furthermore, owing to the limited energy consumption and storage capacity of sensor nodes, failure nodes may appear after working for some time, which results in transmission interruption and data loss. At the same time, if WSN works in remote or dangerous environment, sensor nodes are vulnerable to be attacked by the malicious nodes that always disseminate false information or steal confidential information from internal or external. Therefore, the security of the entire network is threatened. Fortunately, by introducing mobile Sink which continues to move and select an appropriate mobile path for data communication, the network load of WSN gets balanced and energy hole phenomenon is also reduced.

The mobile Sink can not only sense, communicate, compute but also shift. It can communicate with other nodes directly, distract nodes from high data consumption area, and improve data transmission and data gathering performance. However, the movement of nodes always makes the established communication link failure, data gathering delay and data loss. So, designing a security trust model should take into account for the dynamic characteristic of WSN. The author proposes a lightweight security framework from micro and macro level, which aims to achieve efficient and secure data transmission. The rest of paper is structured as follows. The second section reviews related works in security model. In the third section, we construct a security trust model for WSN from moving model of the mobile Sink, bidirectional authentication mechanism and data redundancy calculation. Finally, in the fourth section we conclude our study with some discussion.

2. Related Work

The security model has been drawn a large body of research in past few years. Efficient data gathering, data aggregation and trust mechanism are all hot topics for study.

For data gathering problem, Durmaz proposed a minimum delay method based on time slice scheduling mechanism which focused on the relationship between scheduling and energy control to avoid the conflict in the scheduling and communication process[4]. A coding compression algorithm NADPCMC was introduced by Kasirajan et al. that can effectively reduce energy consumption of source nodes and fusion nodes[5]. To solve the problem of aggregation nodes can’t ensure the data confidentiality in the process of data gathering, Chien-Min et al. put forward a new protocol[6].

As a very important protocol proposed by Heinzelman W, the LEACH protocol not only can search for a minimum energy consumption routing but also support data aggregation operation. The Directed Diffusion protocol performs aggregation in aggregator node using information gradient method. Wang Leichun et al. performed data aggregation according to spatial location and data characteristics. Dilip K et al. analyzed the establishment of the cluster and data transmission path in heterogeneous condition[7]. Liu Ming took into account the node coverage and used the least node to transmit the most comprehensive information[8]. Carlos Guestrin introduced linear regression model to fuse the data to reduce the amount of data transmission[9]. Torsha Banerjee et al. applied binary tree topology structure and regression model with approximation function to aggregate data. Chen H.F et al. put forward an adaptive data fusion method based on cluster, which made use of the spatial and temporal correlation of data to realize the adaptive fusion of sensor nodes[10]. In order to prevent failure of the cluster head, Necchi L. et al. proposed EERINA protocol, which can reduce the transmission data by introducing Gossip algorithm and the broadcast characteristic of wireless channel.

Many trust models for Ad Hoc were not suitable for WSN because of the special characteristics.Ganeriwal et al. proposed a trust evaluation framework based on node reputation[11]. Tanachaiwiwat et al. introduced a method based on location center for separating malicious nodes[12]. The credit value was evaluated by the security capabilities of the nodes. If the trust value was below a certain threshold, the node would be considered unsafe and the packet would bypass it. Tao et al. put forward trust evaluation rules based on statistics method for self-organizing network and also proved the convergence of rules. PET was a personalized trust model proposed by Liang et al., in which every node can change the parameters of trust model, according to environment and customize the trust value[13]. Sun et al. proposed a trust evaluation framework based on distributed network, in which the trust value was spread by the third party. Crosby et al. presented a voting mechanism for cluster head based on node reputation, by which the malicious nodes were not possible to become cluster heads. Guang Yang et al. proposed a malicious behavior recognition model based on MA&TP-BRSN, which introduced a concept of evaluation trust value to denote the reliability of nodes[14].

The above analysis shows that current researches on data aggregation and node trust evaluation are mainly for static WSN that can't satisfy certain extensible requirements of the large scale of dynamic WSN owing to low efficiency and performance of data gathering. The security mechanism of traditional network can't play an effective role in WSN and reach the lightweight goal because of the restriction of computing capability and energy consumption. Therefore, construction of a lightweight security trust model for dynamic WSN by introducing mobile Sink has theoretical and practical significance in promoting the safety of WSN. The lightweight security trust system of WSN should be able to satisfy the following aspects. First of all, dynamically adjust network structure, transmit less redundant data, balance energy consumption and maximize the lifetime of network meanwhile keeping the best data gathering performance. Secondly, build an optimal data transmission system and take into account of computing complexity and time delay to ensure the high efficiency and reliability. Finally, optimize the current trust model and reduce the resource cost of algorithm without changing the trust evaluation precision.

3.Building Security Trust Model

Mobile Sink can reduce coverage vulnerability, track detected events or support more precise measurement when they need to be aggregated in the detection area. Meanwhile, mobile Sink can move to the event area or a node that can't be reached by multi hop transmission, in order to shorten communication distance and balance the workload of other sensor nodes especially the entire energy consumption of WSN. This paper constructs a hierarchical framework of security trust model, in which a new swarm intelligent optimization algorithm named Firefly algorithm is introduced to optimize the moving trajectory. Furthermore, to prevent malicious nodes from stealing important information, it is very necessary to verify the identity of nodes. So, we propose a bidirectional low risk node authentication method which can provide the basis for reliable communication of WSN. As for the efficient data transmission, in order to solve the data redundancy problem caused by the random distribution of nodes, this paper uses the Simhash algorithm to detect the similarity between data. The security trust framework is presented as figure 1.

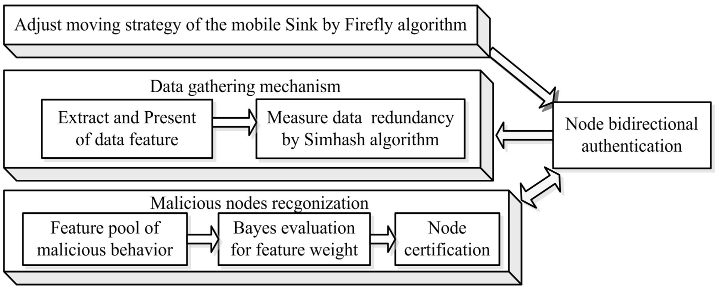
Adjust moving strategy of the mobile Sink by Firefly algorithm
Data gathering mechanism
Extract and Present of data feature
Measure data redundancy by Simhash algorithm
Node bidirectional authentication
Malicious nodes recgonization
Feature pool of malicious behavior
Bayes evaluation for feature weight
Node certification

Figure 1: Security Trust Model of WSN

3.1 Construction the Moving Model for Mobile Sink

The moving strategy of mobile Sink mainly includes random moving, predictable moving, controlled moving and adaptive moving. Random moving strategy makes the node has greater autonomy and blindness when selecting the next hop node, which may result in much more data storage and affect the effectiveness of data transmission. In predictable moving strategy, mobile Sink shifts according to the predefined routing.The low uncertainty of moving trajectory can reduce the communication consumption between different nodes, while it lacks flexibility to adjust the location of the mobile Sink in term of the varied and unexpected network circumstances. Meanwhile, malicious nodes are easy to detect the successor node and then destroy the network connectivity deliberately. Similar to predictable moving strategy, in controlled moving strategy mobile Sink transfers in the light of the predefined path and also changes its transfer speed according to the network environment, but even then it can't fundamentally solve the problem of unbalanced energy consumption. As for the adaptive moving strategy, the transfer path of mobile Sink is unknown. The mobile Sink depends on the current network status and its own location to compute and select the successor shifting location, which has great flexibility and can alleviate the energy consumption pressure of WSN.

The Firefly algorithm is a new Swarm intelligence optimization algorithm proposed by Yang Xin-she scholar of University of Cambridge in 2008, which depicts the search and transfer process of firefly on the basis of the brightness and attraction of peers. A large number of experiments show that Firefly algorithm is better than the genetic algorithm and particle swarm algorithm in global optimization capability and optimization speed[15].To reduce the node load and build lightweight security trust architecture, this paper adopts adaptive moving strategy for mobile Sink and introduces the Firefly algorithm to update and optimize its moving trajectory dynamically based on network environment of WSN. Furthermore, by introducing an inertia factor $\delta \in (0.5, 0.9)$, it makes the mobile Sink leave the visited node or return to the detection area quickly, which can reduce the transmission cost and enhance the moving randomness of mobile Sink. Suppose the mobile Sink starts from an initial node s_0 and goes along with a dynamic path through each sensor node (the sensor node visited by the mobile Sink at time i refers to p_i) to complete a round of data gathering, and then returns to initial node. So, the path model of the mobile Sink is described as follows:

$$min\left(\sum_{i=0}^{N}\sum_{j=0}^{N} X_{ij} d_{ij} + d_{N0}\right) \tag{3.1}$$

In formula(3.1), x_{ij} presents the mobile Sink transfers from node i to node j , d_{ij} presents the transfer distance of the mobile Sink.In formula(3.1), x_{ij} presents the mobile Sink transfers from node i to node j , d_{ij} presents the transfer distance of the mobile Sink.

Brightness and attraction are two key factors in the Firefly algorithm. The fitness value is proportional to the brightness and the attraction. Fireflies with low brightness always move to the others with high brightness. The brightness of firefly is determined by the fitness value of individual firefly and the fitness value is determined by the optimization function. In Firefly algorithm, the brightness of firefly denotes its location. By calculating the fitness value of the sensor nodes according to formula(3.2), we can get the brightness of nodes.

$$f(x) = \frac{1}{min\left(\sum_{i=0}^{N}\sum_{j=0}^{N} X_{ij} d_{ij} + d_{N0}\right)} \tag{3.2}$$

The attraction function is defined as the formula(3.3), in which β is attraction, γ is optical attenuation coefficient, X_i and X_j are the locations of firefly i and j in solution space.

$$\beta = \frac{1}{1 + \gamma \|X_j - X_i\|^2} \tag{3.3}$$

The mobile Sink selects the moving direction by the brightness of other nodes. Then, it updates its location according to formula (3.4) after moving.

$$X_i = \delta X_i + \beta (X_j - X_i) + (1-\delta)(X_j - X_i)^2 + \alpha \tag{3.4}$$

In formula(3.4), δ is inertia factor, α is a random parameter and its value between 0 and 1. The first part of this formula presents the current location of firefly and the second part presents the variation in position caused by the attraction that reflects the global optimization capability. The third part presents variation in leaving from the visited firefly and the last part presents local random transfer of firefly.The mobile Sink moves to other nodes to communicate with each other by using the Firefly algorithm. Its moving speed can be automatically adjusted by the distance between nodes. Easy to implement and low moving cost contribute to reduce the communication consumption of WSN dramatically.

3.2 Bidirectional Authentication Mechanism

Complicate security authentication methods of tradition network can't be effectively applied into WSN because of the limited resources of sensor nodes. In addition to encryption, secure routing and other defense mechanism are essential to cope with attacks from external. And also, WSN must respond to any attacks from internal malicious nodes.

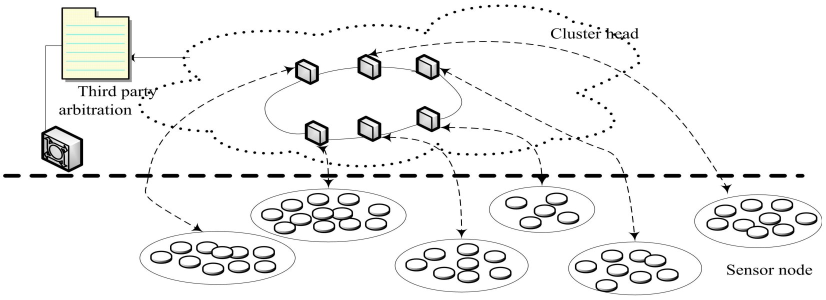

Figure 2: Bidirectional Node Authentications Model

Based on cluster network architecture, this paper constructs a bidirectional authentication model as shown in Figure 2. Nodes in this model can monitor each other, gather the behavior characteristics of nodes and evaluate the credit value by bringing together current and historical situation. In additional, nodes share the gathered credit information with cluster head. In a certain period of time, an optimal node is selected as the cluster head in light of the credit value, residual energy and the location of node. And then, the cluster head evaluates on the other nodes and assigns a local immutable certificate to the node. At the same time, the authentication certificate of cluster head and mobile Sink is maintained by the arbitrable third party authentication node.

For internal active defensive security, the nodes in the detection area are divided into several clusters according to their adjacency degree, and select a suitable cluster head for each cluster. This paper proposes a hybrid cluster algorithm to select the cluster head. By using hierarchical cluster method, the sensor nodes are divided into serval areas according to their distribution density and the initial cluster heads are selected. Then, getting the final cluster heads from candidate nodes by using k–means cluster method on the division result. Selecting the optimal cluster head in each area should consider these aspects such as the residual energy of nodes, the distance between one node and others in the same area and the historical records of this node being a cluster head. Let E_i present the distance between this node and other nodes in the same region. So, we can get an optimal cluster head according to formula (3.5).

$$f(x) = \bar{T} * max\{E_i\} + min\{D_i\} \qquad (i=1,2,\cdots,n) \tag{3.5}$$

After getting the cluster head, it makes a credit evaluation to the nodes in the same region at regular intervals t and gives the node a certificate mark. We need to construct a feature pool in light of malicious attack behavior such as activity, packet loss rate, data transmission delay and data transfer rate. It constructs a sample model vector for each node according to the predefined malicious behavior model in the evaluation process. The whole sample nodes are

present as $S=\{X,Y\}$, in which X presents the nodes that have been marked, Y presents other nodes. Also, we describe X as $X=\{x_i, r_i\}$, if x_i matches with the malicious attack behavior feature, r_i equals to1; otherwise, r_i equals to 0.

Limited in computing and communication capability, the much implicated computing model is not suitable to apply into WSN. Owing to the excellent mathematical characteristics, the Bayes model is introduced to evaluate the node credit. The probability of malicious nodes can be computed by formula(3.6).

$$P(bad|d_x)=P(bad)P(d_x|bad)/\sum(d_x)P(d_x|bad) \tag{3.6}$$

To improve the identification result, this paper introduces the characteristic weight coefficient W_t , $W^t=c_{v1}/c_{v2}$. It can lightweight the key role of some behavior features in enhancing the recognition accuracy, because not all abnormal behaviors have the same effect on identifying malicious nodes. c_{v1} is the number of instances with ith property equals to v . c_{v2} is total number of instances. Formula(3.6) can also be expressed as formula(3.7).

$$P(bad|d_x)=W^t P(bad)P(d_x|bad)/\sum(d_x)P(d_x|bad) \tag{3.7}$$

After the cluster head and ordinary node mutually evaluate each other, the cluster head allocates a local unmodifiable authentication certificate to the node and pass its own certificate to the third party arbitration. When the mobile Sink moves to the node along a certain path, it can check the identity legitimacy of the communication node, which prevents the mobile Sink from connecting and communicating with malicious nodes. In additional, the ordinary nodes can also validate the identity legitimacy of the mobile Sink by the third party arbitration.

3.3 Data Redundancy Detection

Sensor nodes in WSN always randomly distribute and the distribution density is not possible to be homogenized. Furthermore, for most of WSN, the nodes work together to complete a variety of tasks, in which sensor nodes inevitably generate a lot of redundant data that takes a large amount of communication bandwidth and sensor energy. Thus, it is necessary to check the information redundancy between communication nodes before data transmission. Considering the computing ability and limited power of node, we need to use a low complexity method to calculate the data similarity.

At present, the commonly used methods such as information entropy, Euclidean distance and Jaccard similarity show excellent performance in calculating small scale data similarity. However, for the WSN, the data collected by the sensor node is very large. So, the WSN inevitably encounters computing bottleneck with the traditional method. The Locality Sensitive Hashing is an effective method to calculate similarity by narrowing similarity calculation range or reducing the dimension of calculating data. The basic idea is that two adjacent data in the high dimensional data space has a great probability of being adjacent after the data is mapped into a low dimensional data space. And, the two nonadjacent data will also has a great probability of be nonadjacent. By mapping, we can find the adjacent data in the low dimensional data space to reduce searching workload and searching time in high dimensional space. So, this paper introduces Locality Sensitive Hashing to calculate the data similarity between the sensor nodes for solving large scale data redundancy problem. Simhash is a kind of Locality Sensitive Hashing, which is first proposed by Moses Charikar. The essence of Simhash is that the high dimensional feature vector is mapped into a f-bit fingerprint, and then compares the hamming distance of the f-bit fingerprints of the data. The closer the hamming distance is, the more similar the data is. The method can reduce the dimensionality meanwhile comparing the data similarity. Taking into account of storage cost of sensor nodes, we specify Simhash with 32 bits, and then initialize every bit of Simhash to 0. Extract and calculate the feature value of data gathered by n sensor nodes in a period of time, and then calculate the hashcode of every feature value using traditional hash function for each sensor node. After that, accumulate the hash code of every feature value into a sequence of f. Finally, reduce the dimension of each bit for f that is, if a bit is greater than 1, the value of this bit is 1, otherwise is 0. We get the final simhash fingerprint of feature value by mean of the above reducing dimension operation. When the mobile Sink gathers data, it can detect the similarity degree of data by calculating the Hamming Distance between n simhash fingerprints. If the Hamming Distance is less than the predifined threshold, we consider the data is almost similar.The sensor nodes in WSN contain mass redundant or duplicate data which takes up a large amount of network resources. Data de-duplication will help storage and communication efficiency for the WSN. Introducing Simhash method in this paper can realize the accurate detection of extensive data de-duplication for sensor nodes and also balance the time and space complexity.

4.Conclusion

The characteristics of WSN determine that its security trust model is much different with traditional network. The paper presents a lightweight security trust model for WSN with the mobile Sink considering the features of WSN. Bidirectional authentication process based on Bayes evaluation method is simple and efficient for ensuring the robustness of cluster head, in which the cluster heads are selected by the hybrid cluster algorithm, meanwhile it guarantees the communication security between mobile Sink with cluster head and cluster head with ordinary sensor node. The routing mechanism of mobile Sink optimized by the Firefly algorithm with faster convergence speed can select the next node with short distance and enough energy for the mobile Sink in a large searching space and less time cost. Data redundancy detection method based on Simhash algorithm makes the WSN quickly determine the data similarity, reduce data redundancy, energy consumption and communication bandwidth occupied by redundant data transmission and interaction under the large scale of data application. In a word, the paper builds a lightweight security trust model for WSN from a new perspective, which provides a theoretical framework for the research of WSN.

References

[1]F.L.Lewis. Wireless sensor networks[J]. *Smart Environments: Technologies, Protocols, and Applications*.11-16(2004)

[2]J.Yick, B.mukherjee, D.Ghosal. *Wireless sensor network survey*[J].Computer Networks. 12(52):2292-2330(2008)

[3]O.D.Incel, A.Ghosh, B. Krishnamachari. *Fast Data Collection in Tree-based Wireless Sensor Networks*[J]. IEEE Transactions on Mobile Computing. 1(11):86-99(2012)

[4]P.Kasirajan,C.Larsen,S.Jagannathan. *A New Data Aggregation Scheme via Adaptive Compression for Wireless Sensor Networks*[J].ACM Transactions on Sensor Networks. 1(9):1-26(2012)

[5]C.C.Ming, L.Y.Hsun, Y.C.Lin. *RCDA:Recoverable Concealed Data Aggregation for Data Integrity in wireless Sensor Networks*[J]. IEEE Transactions on Parallel and Distributed Systems. 4(23):727-734(2012)

[6]D.Kumar, T.C.Aseri, R.B.Patel. *EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks*[J].Computer communications.4(32):662-667(2009)

[7]C.Guestrin, P.Bodix, R.Thibaux. *Distributed regression: an efficient framework for modeling sensor network data*[C].Proc The 3th international processing in sensor networks.1-10(2004)

[8]T.Banerjee, K.Chowdhury, D.P.Agrawal.*Tree based data aggregation in sensor networks using polynomial regression*[C].Proc the 8th international conference on information fusion.1146-1153(2005)

[9]H.F.Chen, H.Mineno, T.Mizuno. *Adaptive data aggregation scheme in clustered wireless sensor networks*[J].Computer Communication. 25(31):3579-3585(2008)

[10]S.Ganeriwal, M.Srivastava. *Reputation-based Framework for High Integrity Sensor Networks*[J]. ACM Transactions on Sensor Networks.3(4):63-66(2008)

[11]T.Sapon, D.Pinalkuniar, B. Rohan. *Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks*[J].IEEE International Performance, Computing, and Communications Conference. 463-470(2004)

[12]Z.Q.Liang, W.S.Shi. *PET: A personalized trust model with reputation and risk evaluation for P2P resource sharing*[C].Proc the 38th Annural Hawaii International Conference on System Science. 256-264(2005)

[13]G.Yang, G.S.Yin. *Reputation framework for sensor networks*[J]. Communications Journal. 3(29):47-53(2008)

[14]S.Zhu,S.Jajodia,P.Ning.*An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks*[C].Proc IEEE Symposium Security and Privacy.259-271(2004)

[15]X.S.Yang. *Firefly algorithms for multimodal optimization*[C]. Proc the 5th International Conference on Stochastic Algorithms: Foundations and Applications.169-178(2009).