A Novel Wireless Sensor Networks Malicious Node Detection Method

Hongyu Yang(✉), Xugao Zhang, and Fang Cheng

School of Computer Science and Technology,
Civil Aviation University of China, Tianjin 300300, China
hyyang@cauc.edu.cn

Abstract. This paper proposed a malicious node detection model based on reputation with enhanced low energy adaptive clustering hierarchy (Enhanced LEACH) routing protocol (MNDREL). MNDREL is a novel algorithm, which is aimed at identifying malicious nodes in the wireless sensor network (WSN) more efficiently. Cluster-head nodes are first selected based on the enhanced LEACH routing protocol. Other nodes in WSN then form different clusters by selecting corresponding cluster-head nodes and determine the packets delivery paths. Each node then adds its node number and reputation evaluation value to the packet before sending it to the sink node. A list of suspicious nodes is then formed by comparing the node numbers, obtained through parsing with the packets by the sink node, with the source node numbers. To determine the malicious nodes in the network, the ratio of the suspect value to the trusted value of each node is further calculated and compared with a predefined threshold. The simulation experiments show that the proposed algorithm in this paper is more efficient in detecting malicious nodes in WSN with lower false alarm rate than other state-of-the-art methods.

Keywords: Wireless sensor network · Network security · Malicious node · Reputation evaluation · Cluster-head node

1 Introduction

In recent years, Wireless Sensor Networks (WSN) [1, 2, 10] has been widely used in surveillance of military operations, medical secure, construction and other fields. Due to the special working environment, WSN is vulnerable to threats as the internal nodes of it may be controlled as malicious nodes. Therefore, the detection of the malicious nodes in the Wireless Sensor Networks (WSN) has become a research hotspot.

This section addresses the existing related literatures on wireless sensor malicious node detection. Prathap et al. [3] have presented a scheme of Catching Packet Modifiers with Trust Support (CPMTS). In CPMTS scheme, the identity of the node and the reputation value of the parent node were added into the packet, which was encrypted and transferred to the base station, as a tag and the reputation value obtained by analyzing the information decrypted from the packet which was received by the base station was compared with the threshold to identify the malicious node. Though the scheme improved the detection rate of malicious nodes to an extent, the consumption of

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 697–706, 2019.
https://doi.org/10.1007/978-3-030-21373-2_59

the node energy was too excessive during data transmission. Althunibat et al. [4] have proposed an algorithm for detecting the malicious nodes in wireless sensor networks regardless of the type and the number of the nodes. To identify malicious nodes in networks, the algorithm used the real report of the node to master the intelligent behavior of malicious nodes. With the high complexity of the algorithm, the detection effect is unsatisfactory when there are more malicious nodes. Cui et al. [5] have presented a detection method based on reputation with a voting mechanism for wireless networks. The method gave suspect voting on neighbor nodes by analyzing the behavior of neighbour nodes forwarding packets and the malicious node was judged according to the suspect value. However, when the bad mouthing attack frequently comes to the same normal node, the method will fail.

Though research into malicious nodes detection has achieved some results, the efficiency of above methods is still unsatisfactory. Further research needs to be carried on. Thus, the major contribution of our work will be:

- We proposed a Malicious Node Detection algorithm based on Reputation with Enhanced LEACH [6], MNDREL. To improve the detection efficiency, the model will combine the Enhanced LEACH routing protocol with a reputation evaluation mechanism and identify the malicious nodes in WSN effectively.
- We compared the efficiency of MNDREL, FMATM and HRTM methods through a series of simulation experiments and demonstrated that the proposed method in this paper stands out with higher detection rate and lower false alarm rate.

The remainder of the paper is organized as follows. Section 2 discusses the related work on malicious node detection. Section 3 shows the whole structure of the MNDREL model. In Sects. 4, 5 and 6, the sub-modules, which are the cluster construction module, the packet forwarding module and the malicious node detection module, are illustrated separately. The proposed model is compared with other two methods through the experiment in Sect. 7. Finally, Sect. 8 summarizes the conclusion.

2 Related Work

2.1 Fuzzy Logic Based Multi-attribute Trust Model

Because of the uncertainty of the decision taken according to some specific behavior of a node, a fuzzy logic based multi-attribute trust model (FMATM) [9] was proposed to improve the trust based security model. The final trust value of a node is calculated with fuzzy computational theory based on four trust metrics: message success rate (MSR), elapsed time at node (ETN), correctness (CS) and fairness (FS). The final trust value is classified as low (l), medium (m) and high (h). According to the simulation results, the FMATM model is more efficient in detecting malicious nodes than the Hierarchical Trust Management Protocol (HTMP).

2.2 High-Reliability Trust Evaluation Model

Gong et al. proposed a high-reliability trust evaluation model (HRTM) [1] for secure routing to refine the trust evaluation result of a node and improve the related routing trust evaluation model. The HRTM evaluated the trust of routing nodes according to the inner states of a node and the outside interaction behaviors between nodes. With high detection efficiency and fast responding, the HRTM was able to defense internal and external attacks on a router.

The above two methods are relatively efficient in identifying the behavior of a node, however, the information of a node considered is not enough, so we utilize the FMATM and the HRTM to detect malicious nodes in WSN and compare the simulation results with the model proposed in this paper. Details of the comparison are discussed in Sect. 7.

3 Model Structure Design

The MNDREL model consists of a Clusters Construction (CC) module, a Packets Forwarding (PF) module, and a Malicious Nodes Decision (MND) module, which contains two sub-modules, the packet analysis sub-module and the integrated decision sub-module (as shown in Fig. 1).

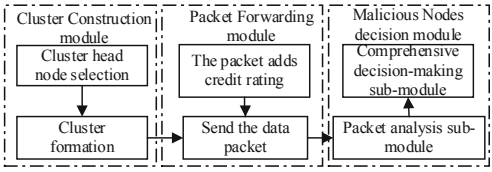


Fig. 1. MNDREL model structure

Firstly, the CC module determines the Cluster-Head node (CH) and divides the network into clusters to form a transmission path of packets; Secondly, the PF module transmits the packet containing the reputation value of the parent node evaluated by the current node to the Sink Node (SN); Finally, the MND module analyses the reputation value in the packet to determine the malicious node.

In the MNDREL model, the detection steps for the malicious nodes of the network are designed as follows:

Step 1. According to the remaining capacity of the node, the distance to the sink point, the signal strength and other conditions, a number of cluster heads from the network nodes are selected;

Step 2. The selection results of the cluster-head are broadcast by each cluster-head to notify the remaining nodes. With the distance of each node to each cluster-head calculated separately, one round of clustering is completed after the nodes join the cluster with the minimum distance;

Step 3. In way of sharing the key with the sink node, each node adds the reputation evaluation value of its parent node to the data packet and encrypts the data information;
Step 4. The packet is transmitted from the cluster nodes to the cluster-head by one or several hops, thus forwarded to the sink node by the cluster-head.
Step 5. After the sink point receives the data packet, the data packet analysis sub-module of the MND module will extract parameters such as the node number and the reputation value of the parent node in the packet. The suspicious node list is constructed by comparing the node number and the source node number and the reputation value from the packet and the reputation value calculated by other nodes are combined as the input of the integrated decision sub-module;
Step 6. The reputation value of various nodes is calculated by the integrated decision sub-module and it is compared with the threshold to determine whether there are malicious nodes in the network.

4 Cluster Construction Module

4.1 Cluster Head Node Selection

The approach of cluster-head selection is defined as follows:

$$RB_{avg} = \frac{\sum_{i=1}^{n} RB_i}{n} \tag{1}$$

$$DB_{avg} = \frac{\sum_{i=1}^{n} DB_i}{n} \tag{2}$$

$$P_i = w \times \frac{RB_i}{RB_{avg}} \times \frac{DB_{avg}}{DB_i} \tag{3}$$

where RB_{avg} represents the remaining power of all nodes, DB_{avg} represents the average distance of each node and the sink node in WSN, RB_i denotes the current remaining power of node i, DB_i represents the distance of node i and the sink node, n represents the number of live nodes at present time, P_i represents the probability that node i becomes a cluster-head.

Formula (3) satisfies the condition $(RB_i/RB_{avg}) > 1$, $(DB_{avg}/DB_i) > 1$ and $SB_i > SB_{Th}$. SB_i is the quantized value of the signal strength of node i; SB_{Th} is the critical value of the signal strength, which is assigned as the value of the weakest intensity of signal strength of the nodes that the sink node could sense. w is a fixed constant greater than 1.

4.2 Clustering Process

The clustering process is as follows:

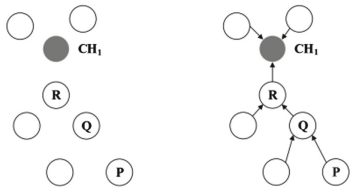
Step 1. The cluster-head node notifies other nodes of Head_Msg;
Step 2. After receiving the Head_Msg, the non-cluster-head node chooses the cluster in which it expects to join. According to the distance from different cluster-head and the received signal strength of a cluster-head, the non-cluster-head node sends the Join_Clu_Msg to the cluster-head. The Join_Clu_Msg includes the number of the node that sends the application and the number of the specified cluster-head number.
Step 3. Each cluster-head summarizes the Join_Clu_Msg and determines the nodes that can join the corresponding cluster based on the maximum transceiver capacity of the cluster-head, thus forming different clusters of WSN;
Step 4. The packet is transmitted from the cluster nodes to the cluster-head by one or several hops, thus forwarded to the sink node by the cluster-head, thereby determining the routing path of the packet in the network.

5 Packet Forwarding Module

5.1 Packet Delivery

With the division of clusters in WSN finished, the sink node sets the time slice length of the packet transmission and notifies other nodes in the network and the nodes in each cluster forward the packet to the cluster-head within the specified time slice.

The process of packet transmission is shown in Fig. 2. When the source node P sends data, P creates the packet $m_1 = <P_{id}, M_{id}, T_Q, D>$, and the packet m_1' is then generated by encrypting m_1 using the key P_{key} shared between the packet and the cluster-head node CH_1. Where P_{id} is the number of node P, M_{id} is the number of packet m_1, T_Q is the reputation value evaluated by node P for its parent node Q and D is the data get by source node P.



(a) Cluster node deployment (b) Intra-cluster data transfer

Fig. 2. Process of packet transmission

Node Q generates packet m_2 by adding the node number, the packet number and the reputation evaluation value of the parent node R into packet m_1' and it generates packet m_2' by encrypting m_2 with the shared Q_{key} of node Q and CH_1. Following the similar process, CH_1 finally gets the packet, encrypts it and sends it to the sink node within the specified time slice.

5.2 Reputation Evaluation

The process of reputation evaluation is designed as follows:

Step 1. Each node records the number of the parent node to which it forwards the packet. The sink point establishes a tree topology including all parent-child node relationships according to the information collected from each node and decrypts the data packet based on the topology to detect the malicious node in the network;
Step 2. After the network node is deployed, each node adds a reputation evaluation table to the parent node in the data packet, and the reputation evaluation value for the parent node calculated by the child node includes the credibility evaluation value and the suspicion evaluation value (as shown in Table 1), the credibility evaluation value and the suspicion evaluation value are initialized to 0. k represents the node number in the network, $k = 1, 2, \ldots, n$; n represents the number of nodes participating in the packet transmission;

Table 1. Parent node reputation evaluation table

Parent node number	k
Credible evaluation value	0 or 1
Suspect evaluation value	0 or 1

Step 3. After the parent node receives the packet from the child, the behavior of the packet forwarding by the parent node within the pre-set time slice will determine the credibility evaluation value and the suspicion evaluation value of the parent node. If malicious behaviors such as the packet dropping, packet modification, packet misrouting or packet delay appear in the parent node, the child node sets the suspicion evaluation value to 1 and the credibility evaluation value to 0. Conversely, the credibility evaluation value is set to 1 and the suspicion evaluation value is set to 0;
Step 4. After a round of packet delivery, the child node can perform corresponding operations according to the behavior of the parent node: If the parent node is not the cluster-head and malicious behaviors appear in its packet forwarding process, the child node notifies the neighbor one-hop node of the malicious behavior by broadcast. If the parent node is the cluster-head and malicious behaviors appear in its packet forwarding process, the child node joins other clusters in the next round of selection and deletes the original parent node number from the node number list.

6 Malicious Node Decision Module

The malicious node decision module is combined of two parts: the packet analysis sub-module and the integrated decision sub-module.

6.1 Packet Analysis Sub-module

When packet m is passed to the sink point, the analyzing step for m is designed as follows (the packet analysis process is shown in Fig. 3):

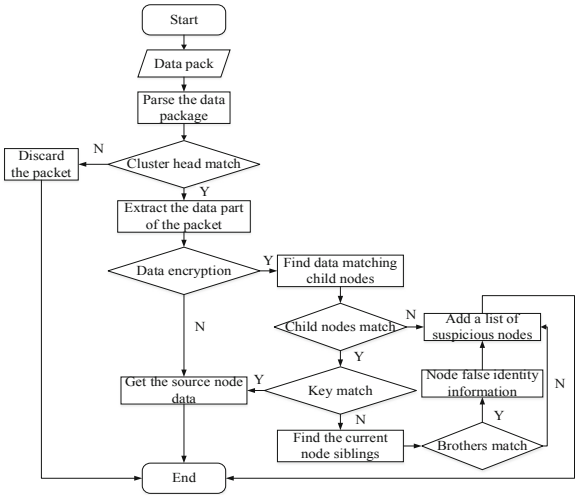


Fig. 3. Packet analysis flowchart

Step 1. The sink point encrypts packet m on the basis of the key shared with the cluster-head and produces packet m';
Step 2. Parse packet m' and remove the node number, packet number and the reputation evaluation value of the cluster-head, if other data in the packet is unencrypted, then m' is from the source node;
Step 3. If the data of packet m' is partly encrypted, then backtrack the upstream node according to the routing path of packet m', and decrypt the data packet through the upper layer shared key until the data of the source node is obtained;
Step 4. If the information of all the child nodes of a parent node does not match the packet information, illustrating that malicious packet modification appears in the parent node or any corresponding child node, then the parent node and all the child nodes are added to the suspicious node list;
Step 5. If the node number in the packet does not match the decryption key number in the decryption process, check the sibling node of the current node to see if there is a matching one and determine whether the identity of the sibling node is impersonated by the current node. If the impersonation exits, add the current node to the suspicious node list.

6.2 Integrated Decision Sub-module

Node Reputation Value

When the data packet has been delivered, the sink point parses the packet, gets the reputation value of the parent node evaluated by the child node and generates the reputation value of each node in WSN (as shown in Table 2).

Table 2. Network reputation table for each node

Node number	1	2	3	…	k	…	n
Trusted value (T_k)	T_1	T_2	T_3	…	T_k	…	T_n
Suspect value (S_k)	S_1	S_2	S_3	…	S_k	…	S_n

In Table 2, the trusted value T_k represents the sum of the credibility evaluation value of node k, that is, the sum of all the numbers for the node's credibility evaluation value of 1; similarly, the suspect value S_k represents the sum of the suspect evaluations of the node k; n is the number of nodes participating in the packet transfer.

Reputation Decision Algorithm

In order to determine the malicious node based on the trusted value of the node and the behavior of the node in the process of data packet transmission, this paper proposes a reputation decision algorithm. The algorithm determines the malicious node by analyzing the suspect value and the trusted value of each node and comparison with the detection threshold.

According to the literature [4], the detection rate is higher and the false alarm rate is lower with the detection threshold set as 1.2. Therefore, the detection threshold R_{Th} is set to 1.2 in this paper. Calculate the ratio R_k (k is the node number, $k = 1, 2, \ldots, n$) of suspect value to trusted values for all nodes:

$R_k \geq R_{Th}$, if node k is in the suspicious node list, determine k as a malicious node; if node k is not in the suspicious node list and no impersonation of the identity of other nodes appears, node k will be added to the suspicious node list, waiting for the next round of detection.

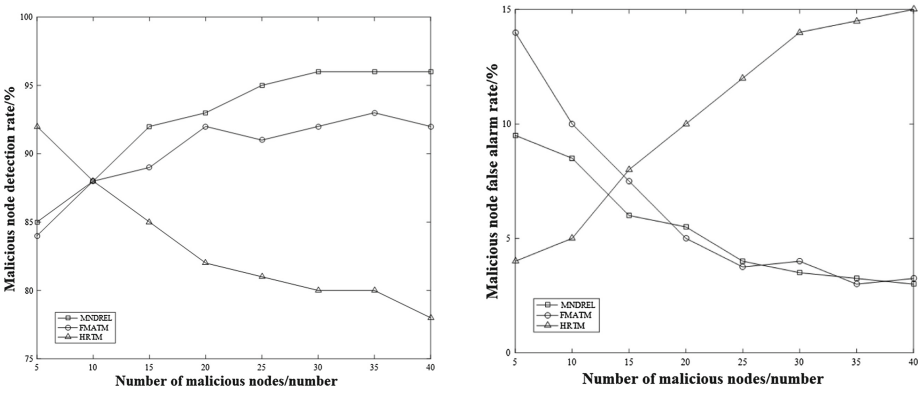
$R_k < R_{Th}$, if node k is in the suspicious node list, retain it and wait for the next round of detection; if node k is not in the suspicious node list and no impersonation of the identity of other nodes appears, then k is determined as a normal node.

In the above process: If node k is determined to be malicious, the sink node will broadcast its number and the nodes with a forwarding relationship with it will delete its number from the parent node list. If node k is added into the suspicious node list after a round of detection, however, it satisfies the relation of $R_k < R_{Th}$ in several other rounds of detection, then move it out of the suspicious node list and use it as a normal node in packet delivery activity.

7 Experiment and Analysis

The experiment was conducted on the OPNET (opnet-14.5) platform. The MAC layer adopts the 802.11 wireless communication protocol, and the network layer adopts the Enhanced LEACH routing protocol. The number of nodes in the network simulation experiment is 50, 100, …, 400, and the number of malicious nodes generated randomly is 5, 10, …, 40. The source node generates a data packet of 4000B every 100 ms to be transmitted to the cluster-head through the parent node, and then sent to the sink node by the cluster-head. Based on the experimental conclusions of [7] and [8], the network simulation time of this experiment is set to 50 s, and the time slice length of data packet transmission is set to t = 2 s. After the OPNET sends the packet based on the Enhanced LEACH routing protocol, the experimental data is processed through MATLAB programming by which the algorithm and the module function mentioned above are realized.

In the same environment, we compared efficacy of the MNDREL detection model, the Fuzzy logic based Multi-Attribute Trust Model (FMATM) [9] and the High-reliability Trust evaluation Model (HRTM) [1]. The number of nodes is set to 50, 100, …, 400, and the number of malicious nodes generated randomly is set to 5, 10, …, 40. The detection rate and the false alarm rate are shown separately in Fig. 4.



(a) Malicious node detection rate (b) Malicious node false alarm rate

Fig. 4. Detection comparison of MNDREL, FMATM and HRTM

It can be seen from Fig. 4(a) and (b) that with the increase of the number of malicious nodes, the detection rate of malicious nodes in HRTM method decreases, the false alarm rate increases while the detection rate of MNDREL model and FMATM model increases and the false alarm rate decreases. Compared with FMATM, the detection rate and the false alarm rate of the MNDREL model is more stable.

The experimental results show that the MNDREL model can maintain a high detection rate and a low false alarm rate when the number of malicious nodes in the network changes. The reason is that the MNDREL model is based on the Enhanced LEACH routing protocol. With the relatively fixed routing path of the packet, the malicious node in

the network is easier to be tracked and located, thus leading to high detection efficiency. In addition, the MNDREL model judges the suspicious node generated during the process of packet transmission and with the increasing of nodes and packets, the information extracted from the reputation evaluation is more, so the malicious node is easier to be found, thus leading to gradual rising of the detection rate and the gradual descending of the false alarm rate.

8 Conclusions

To improve the effect of malicious nodes detection, we proposed a novel algorithm, MNDREL. The malicious nodes can be effectively identified according to the suspect value and the trusted value evaluated by MNDREL. Simulation experiments proved that the MNDREL model outperformed in detecting malicious nodes in WSN with lower false alarm rate than FMATM and HRTM. However, the real time performance of the MNDREL model has to be improved. By adding time stamps into the model, we will monitor the dynamic changing situation of malicious nodes in WSN, moreover, the distribution of malicious nodes within a certain time can be predicted.

Acknowledgement. This research was funded by the Civil Aviation Joint Research Fund Project of National Natural Science Foundation of China under granted number U1833107.

References

1. Gong, L.Y., Wang, C.D., Yang, H.Y., et al.: Fine-grained trust-based routing algorithm for wireless sensor networks. Mob. Netw. Appl. (2018). https://doi.org/10.1007/s11036-018-1106-z
2. Zhang, Y.Q.: The Study on Security Problems of Wireless Sensor Networks. Shandong People's Publishing House, Jinan (2013)
3. Prathap, U., Shenoy, P.D., Venugopal, K.R.: CMNTS: catching malicious nodes with trust support in wireless sensor networks. In: IEEE Region 10 Symposium 2016, pp. 77–82. IEEE Press, Piscataway (2016)
4. Althunibat, S., Antonopoulos, A., Kartsakli, E., et al.: Countering intelligent-dependent malicious nodes in target detection wireless sensor networks. IEEE Sens. J. **16**(23), 8627–8639 (2016)
5. Cui, H., Pan, J., Yan, D.: Malicious node detection algorithm based on reputation with voting mechanism in wireless sensor networks. J. China Univ. Metrol. **24**(4), 353–359 (2013)
6. Das, S., Das, A.: An algorithm to detect malicious nodes in wireless sensor network using enhanced LEACH protocol. In: International Conference on Advances in Computer Engineering and Applications 2015, pp. 875–881. IEEE Press, Piscataway (2015)
7. Liu, H.B., Cui, J.M., Dai, H.J.: Multivariate classification-based malicious detection for wireless sensor network. Chin. J. Sens. Actuators **24**(5), 771–777 (2011)
8. Hui, L.L., Pan, J.L., Cui, H.: A reputation-based method for detecting malicious nodes in WSNs. J. China Univ. Metrol. **23**(1), 41–47 (2012)
9. Prabha, V.R., Latha, P.: Fuzzy trust protocol for malicious node detection in wireless sensor networks. Wirel. Pers. Commun. **94**(4), 1–11 (2016)
10. Belhajem, I., Maissa, Y.B., Tamtaoui, A.: Improving vehicle localization in a smart city with low cost sensor networks and support vector machines. Mob. Netw. Appl. **23**(4), 854–863 (2018)