Secure Communication Mechanism Based on Key Management and Suspect Node Detection in Wireless Sensor Networks

Danyang Qin(✉), Songxiang Yang, Ping Ji, and Qun Ding

Key Lab of Electronic and Communication Engineering,
Heilongjiang University, Harbin, People's Republic of China
qindanyang@hlju.edu.cn

Abstract. The limitation of bandwidth, environment and multipath fading in wireless sensor network (WSN) cannot satisfy the need of users. Cooperative multiple-input-multiple-output (C-MIMO) technology is introduced to improve the communication performance, which brings in security problem as the same time. The key management technology may ensure the confidentiality with fewer keys but is unable to resist the compromised node attack. A new detection algorithm is proposed to sign the compromised node and recover the information during the transmission. Combining the key management and compromised node detection, a secure communication mechanism for WSN is proposed to resist the external and internal attack. Simulation results verify the advantages of security and performance by the proposed communication mechanism.

Keywords: WSN · Security · Routing protocol · Key management

1 Introduction

WSNs have been widely used in many fields with the rapid development of electronic information and wireless communication [1]. However, the WSN can hardly satisfy the need of users with the limitation of bandwidth, environment and multipath fading. So, researchers invent the MIMO communication system to break through the bottlenecks of wireless channel capacity, which can against multipath fading and improve channel capacity. MIMO technology can hardly be applied to the mobile terminal with the limited size and power. So C-MIMO communication is proposed, which can make use of mutual collaboration among the single antennas to form virtual multi-antenna matrix. Comparing with the single-input-single-output system, the C-MIMO system can enhance the transmission quality and the lifetime of the network without increasing the hardware complexity [2, 3]. However, the credibility of all nodes is a basis for cooperation mode, which provides an opportunity for attacker to destroy the network.

D. Qin—This work was supported in the part by the National Natural Science Foundation of China under Grant 61771186, University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province under Grant UNPYSCT-2017125, and Postdoctoral Research Foundation of Heilongjiang Province under Grant LBH-Q15121.

X. Gu et al. (Eds.): MLICOM 2017, Part I, LNICST 226, pp. 692–700, 2018.
https://doi.org/10.1007/978-3-319-73564-1_71

Generally, the attack in WSN can be divided into external attack and internal attack. The encryption technique can defense external attack but unable to resist the internal attack caused by the injured nodes, since they can encrypt and decrypt the information. Thus, suspect nodes may affect network security seriously [4, 5].

A detection model is designed for WSN to identify the suspect nodes by a few keys, based on which a cross-layer security communication mechanism is proposed to overcome the external attack and the internal attack caused by suspect nodes in the C-MIMO communication. Comparing with the similar schemes [6], the proposed mechanism can against the attack of the suspect nodes without increasing the system complexity. In addition, the user can achieve the balance among the power, the efficiency and the reliability of received data by adjusting the security level. It's a small probability event for intruder to break through the security authentication and infect the nodes in network, so this paper uses deterministic parameters as the model parameters of WSN nodes.

2 WSN Security Architecture Based on C-MIMO

2.1 Network System Model

Figure 1 shows a multi-hop cooperative WSN model which is composed of many single antenna sensor nodes, namely host nodes. These host nodes form clusters called MIMO nodes by a distributed clustering algorithm. The rest of the system is shown in the figure.

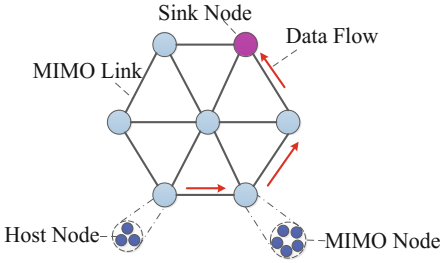

Fig. 1. System model

The most common collaborative communication strategies are Amplify-and-Forward (AF) and Decode-and-Forward (DF). AF amplifies and forwards the useful signal and the noise at the same time, which will directly affect the information transmission in network. DF can eliminate the noise and improve the reliability of system. Moreover, system needs to decode the data that aggregates in cluster head, so this paper adopts DF strategy.

Assuming that there are n_T and n_R nodes in the transmitting cluster and receiving cluster, respectively. The relationship between received signal $\boldsymbol{y}$ and sending signal $\boldsymbol{x}$ can be expressed as:

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{w} \tag{1}$$

$\boldsymbol{y} = [y_1, y_2, \ldots, y_{n_R}]^T, \boldsymbol{x} = [s_1, s_2, \ldots, s_{n_T}]^T$. $\boldsymbol{H}$ is $n_R \times n_T$ matrix of channel coefficients. $\boldsymbol{w} = [w_1, w_2, \ldots, w_{n_R}]^T$ represents Gaussian noise.

The channel matrix $\boldsymbol{H}$ is known to the receiving cluster instead of the transmitting cluster, which can enhance the security of MIMO network. $\boldsymbol{H}$ could be calculated by the known transmitting bit sequence and the corresponding received signal.

The proposed cross-layer secure communication mechanism for C-MIMO WSN is as follows: Each host node determines whether the suspect node needs to be identified. Normal cooperative data transmitting or forwarding will be performed if the detection is not required. Otherwise, suspect node detection will be performed. Normal data transmitting or forwarding will continue, if there is not any suspect node in the testing result. Otherwise, messy code will be eliminated by symbol filter. Then, the sink node will receive the test report, and the key management system will update key and re-build network.

2.2 C-MIMO Network Architecture

N denotes a network with many sensor nodes. d-cluster represents a disjoint part of N. There are two clusters with n_T and n_R nodes, namely A and B. This paper defines single-antenna wireless nodes as the host nodes, and calls d-cluster and C-MIMO transmission link as MIMO nodes and MIMO link, respectively. A C-MIMO network with given N and d can be formed by the following steps:

Step 1: The host nodes in N construct a C-MIMO network N_{CMIMO} through the distributed clustering algorithm.
Step 2: MIMO nodes form a multi-hop backbone tree in N_{CMIMO}.
Step 3: The backbone tree provides the routing which is used for data dissemination and data receiving.

After the C-MIMO network was formed, each cluster will obtain a ID. And each host node will contain the cluster's ID, all host nodes' IDs, the IDs and the size of neighbor clusters.

2.3 Secure Key Management Mechanism

Considering the limitation of energy and the correlated behaviors between MIMO nodes, this paper proposes a key management system, which requires a few preloading keys. This section establishes the key management system through the topology knowledge rather than the location knowledge which is more complex. Figure 2 shows two kinds of keys adopted in C-MIMO system, namely $C\_\text{key}(A)$ (for local communication) and $L\_\text{key}(A, B)$ (for long-haul communication between two clusters). The nodes in A encrypt transmitted signal by $L\_\text{key}(A, B)$, and the nodes in B decrypt the

received signal by the same key. Main components of the key management system are as follows:

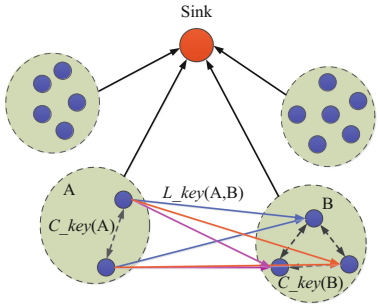

Fig. 2. Keys used in the proposed secured communication system

(1) Key pre-distribution: A shared secret key pre_key(b, m) is pre-distributed for b and m in WSN.
(2) Key establishment algorithm:
   Step 1: A host node m sends the plaintext message (IDs of m and b) and the encrypted message (ID of m and b, clusters list, neighbors of m) encrypted by pre_key(b, m) to b.
   Step 2: b decrypts the information by pre_key(b, m) after receiving a key request from m. And b would obtain the topology information of the whole C-MIMO network after receiving the key request from all nodes. Then, b generates C_key(A) and L_key(A, B) for A and link AB respectively, and responses to each x in A, which consists the plaintext message (IDs of b and x) and the encrypted message (IDs of b and x, C_key(A), L_key(A, B)) encrypted by pre_key(b, x).
   Step 3: x uses pre_key(b, x) to decode the message and then to obtain C_key and L_key, after receiving a key response.
(3) Secure communication link establishment:

The communication in A is encrypted by C_key(A), and the communication in link AB is encrypted by L_key(A, B). Only one pre-distributed key is required for each host node m in the proposed key management mechanism. Each host node m has one C_key and i L_keys, where i is the number of neighbor nodes of m in the backbone tree. The sum of C_keys and L_keys in the whole network is n (the number of clusters) and $n - 1$ (the number of links in the backbone tree), respectively.

3 Suspect Node Detection with Information and Network Recovery

Suspect nodes represent the physical or logical unsafe nodes which bring security issues that cannot be solved by encryption techniques. Moreover, the cooperative nature of C-MIMO makes the effect of suspect nodes on network security more serious.

So, this section proposes the suspect node detection algorithm, and insulates the suspect nodes by updating the key, which can eliminate the influence of suspect nodes on data transmission. Finally, network will be reconfigured to reduce the transmission delay caused by the isolation of key nodes.

3.1 Suspect Node Detection

Figure 3 shows a model of suspect node detection, where A is the transmitting cluster and D is the detecting cluster.

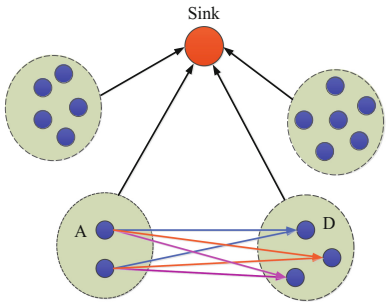

Fig. 3. Model for suspect nodes detection

Security enforcement is a challenging task in cooperative communication with multiple nodes and complex forwarding rules. To solve this problem, this paper proposes an identification method in physical layer, which can detect suspect nodes without increasing the transmission overhead.

Algorithm 1 is proposed to determine whether each cluster needs to detect the suspect node.

Algorithm 1.

1. generate s ($s \in [0,1]$) at node k randomly
2. compare s with l
3. **if** $s > l$ **then**
4. sends the detection signal to the other nodes
5. detect the suspect node before transmitting data
6. **else**
7. transmit the data
8. **end if**

The cluster will perform the detection, if there are suspect nodes. In the proposed mechanism, the detecting clusters cannot detect the transmitting cluster, since they are always the receiving side. The suspect nodes can be ignored which always send the correct message, because they do not influence the stability of the network.

In the proposed algorithm, all the transmitting nodes in cluster A transmit the same data stream to get the diversity gain. The host nodes in cluster A transmit the data flow $I_1 = I_2 = \cdots = I_{n_T}$ to the host node in D for detection. Every host node in D can obtain the complete data sequence R and detect the suspect node in cluster A by obtaining the received symbols form all other nodes. The suspect node detection algorithm at each host node in D is as follows.

Step 1: After receiving the complete data sequence R, each host node in D estimates the transmitted symbol I by the reverse channel detection, i.e. $\hat{I} = \boldsymbol{W}^{\boldsymbol{H}} R$, where $\boldsymbol{W}$ is $|D| \times n_T$ weighting matrix, $|D|$ is the number of nodes in D, and $(\cdot)^{\boldsymbol{H}}$ represents the conjugate transpose. Assume that the channel coefficients matrix $\boldsymbol{H}$ is known for the detecting cluster. $\boldsymbol{W}$ can be determined as:

$$W = \begin{cases} \boldsymbol{H}^{-1} & n_T = |D| \\ \left(\boldsymbol{H}^H \boldsymbol{H}\right)^{-1} \boldsymbol{H}^H, & |D| > n_T \end{cases} \tag{2}$$

Step 2: The detecting node can identify the suspect nodes x_i and record their IDs by checking the symbols, since the data flow sent by the normal nodes are identical. The nodes which send the same symbols are divided into one group to simplify the detection. The group with the most nodes is credible, and others may contain the suspect nodes.

Step 3: When the host node m detects the suspect node x, the cryptographic detection report with the plaintext message (ID of m and b) and the encrypted message (ID of m, b and x) which is encrypted by pre_key(m, b) will be transmitted to b by each detecting host node. The nodes are classified as a suspect node, if more than half of the host nodes in the cluster claim that node x is suspected.

Figure 4 shows a data forwarding path to describe the selection of detecting clusters and the upper limit of identifiable suspect nodes, where the *Pre_A* forwards data to A, and then A forwards the data to the *Post_A*. Let $|A|$, $|Pre\_A|$ and $|Post\_A|$ denote the number of nodes in A, *Pre_A* and *Post_A*, respectively. If $|A| \leq |Post\_A|$, the suspect node in A will be detected by the *Post_A*, and the upper limit of identifiable suspect nodes is $|A|/2 - 1$. If $|A| > |Post\_A|$ and $|A| \leq |Pre\_A|$, the suspect node in A will be detected by *Pre_A*, and the upper limit of identifiable suspect nodes is $|A|/2 - 1$. If $|A| > |Post\_A|$ and $|A| > |Pre\_A|$, the suspect node in A will be detected by a larger cluster between *Pre_A* and *Post_A*. The upper limit of detectable suspect nodes in A and the n_T can be determined by the following equation:

$$\begin{aligned} N_{\max} + n_T &= |D| \\ N_{\max} &= \tfrac{n_T}{2} - 1 \end{aligned} \tag{3}$$

$N_{\max}$ is the upper limit of suspect nodes in A, and $|D|$ represents the nodes in the detecting cluster. By solving (3), we can get

$$\begin{aligned} N_{\max} &= (|D|+1)\cdot\tfrac{1}{3}-1 \\ n_T &= (|D|+1)\cdot\tfrac{2}{3} \end{aligned} \tag{4}$$

$N_{\max}$ and n_T will be rounded to the nearest integer if they are not integers.

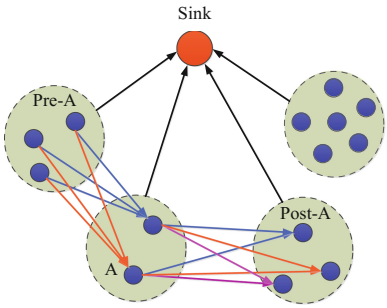

Fig. 4. Selection of cluster for detection

3.2 Key Update and Network Recovery

The sink node will update the key and recover the network if there is a suspect node in cluster A. This method could prevent the suspect nodes from obtaining information or sending false reports. Sink node b takes the following approach to update the key and recover the network:

Step 1: b sends a key update message including the plaintext message (IDs of b and u) and the encrypted message (IDs of b and u, new $C\_\text{key}(A)$, and the ID list of suspect node) which is encrypted by $\text{pre\_key}(b,u)$ to all nodes u in cluster A except for x.

Step 2: b sends a key update message that includes the plaintext message (IDs of b and u) and the encrypted message (IDs of b and u, new $L\_\text{key}(A,B)$) which is encrypted by $\text{pre\_key}(b,u)$ to each node u in every neighbor cluster B of A except x.

Step 3: After receiving the key update information from the above steps, u decrypts the message by $\text{pre\_key}(b,u)$ and obtains the new C_key and L_key. The suspect node x cannot obtain information from the network, since it does not have a new key.

The report will be sent to the sink node b layer by layer, if the suspect node in A is detected by its parent node. b may send a key revocation packet to A and its neighbor nodes via the reverse path of the transmission report, if each node maintains the record of the transmission path.

The suspect nodes are often deployed on the important transmission link in actual network. Screening out these nodes may affect the quality of the network transmission, and even lead to an island effect. So, network need to be rebuilt after the above work.

4 Implementation and Performance Analysis

4.1 Simulation Settings

The performance of the proposed algorithm and system is evaluated by MATLAB. The sink node sends a random signal on the premise of connected domain assurance. The fast Rayleigh fading channel is selected to imitate a multipath fading environment. The number of receiving symbol is 100, the modulation scheme is BPSK. This section evaluates the proposed detection algorithm by comparing with distributed compromised node detection algorithm.

4.2 Simulation Results

Figure 5 shows the accuracy of two detection algorithms with one suspect node in the transmitting cluster.

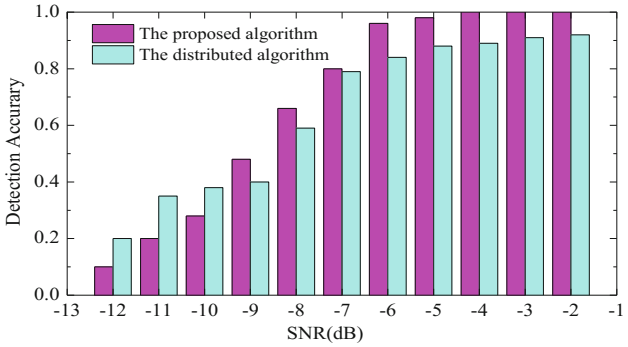

Fig. 5. Accuracy of two detection algorithms with one suspect node

There are four nodes in the transmitting cluster and five nodes in the detecting cluster in the simulation, since all the cases satisfy $|D| > n_T$. Figure 5 shows that the accuracy of distributed algorithm is higher than that of the proposed algorithm, when SNR is less than −9 dB. And the result is just the reverse when SNR is higher than −9 dB, which is the actual wireless channel environment. Moreover, the identification accuracy of proposed algorithm is close to 100% when SNR is greater than −4 dB. The simulation results suggest that the proposed algorithm has higher identification accuracy in the actual wireless channel environment.

Figure 6 shows the bit error rate of the proposed system and the traditional system, respectively. The case without any suspect node is simulated as a reference. Obviously, the proposed system can significantly improve the reliability of the communication

when the SNR is higher than −8 dB. It is clear that the proposed mechanism cannot only improve the suspect node detection accuracy and the performance of network security, but also ameliorate the quality of network information transmission.

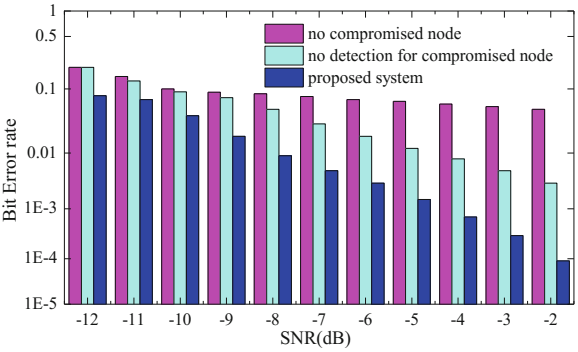

Fig. 6. Bit error rate of three systems

5 Conclusions

This paper proposes a cross-layer communication mechanism for C-MIMO communication to solve the security threat and improve the performance of the WSN. The mechanism contains a low cost key management system and a high-accuracy suspect node detection algorithm. The proposed mechanism may allow the network to transmit the data between authorized nodes, and it will update keys and recovery network if necessary. The simulation result indicates that the detection algorithm can identify the suspect nodes effectively, and the cross-layer communication mechanism may improve the stability and accuracy of the data transmission in the network.

References

1. Chang, F.C., Huang, H.C.: A survey on intelligent sensor network and its applications. J. Netw. Intell. **1**, 1–5 (2016)
2. Gao, Q., Zuo, Y., Zhang, J., Peng, X.H.: Improving energy efficiency in a wireless sensor network by combining cooperative MIMO with data aggregation. IEEE Trans. Veh. Technol. **59**, 3956–3965 (2010)
3. Islam, M.R., Kim, J.: On the cooperative MIMO communication for energy-efficient cluster-to-cluster transmission at wireless sensor network. Ann. Telecommun. **65**, 325–340 (2010)
4. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Netw. **1**, 293–315 (2003)
5. Choudhury, P.P., Bagchi, P., Sengupta, S., Ghosh, A.: On effect of compromised nodes on security of wireless sensor network. Ad. Hoc Sens. Wirel. Netw. **9**, 255–273 (2010)
6. Chen, X., Makki, K., Kang, Y., Pissinou, N.: Sensor network security: a survey. J. IEEE. Commun. Surv. Tutor. **11**, 52–73 (2009)