International Journal of Safety and Security Engineering
Vol. 10, No. 3, June, 2020, pp. 397-402
Journal homepage: http://iieta.org/journals/ijsse

Security Analysis on Wireless Sensor Network in the Data Center for Energy Internet of Things

Shengjun Xie[1], Xiang Wang[1*], Hua Shang[2]

[1] Information and Educational Technology Center, Southwest Minzu University, Chengdu 610041, China
[2] Modern Educational Technology Center, Civil Aviation Flight University of China, Guanghan 618307, China

Corresponding Author Email: wangxiang@swun.edu.cn

https://doi.org/10.18280/ijsse.100312

Received: 30 January 2020
Accepted: 2 April 2020

Keywords:
Data Center (DC), Wireless Sensor Network (WSN), security analysis, information fusion, Low Energy Adaptive Clustering Hierarchy (LEACH)

ABSTRACT

In the Energy Internet of Things (EIoT), the sensors in the wireless sensor network (WSN) at the data center (DC) are prone to attacks, and easy to suffer from problems in information security management (ISM), such as poor real-time performance and high complexity. This paper clarifies the structure of the DC WSN for the EIoT, models the WSN under the LEACH, and predicts the possible types of attacks. On this basis, a real-time and dynamic ISM plan was developed for the WSN. In this plan, the structure and operations of LEACH are optimized, and amount of data transmission was reduced through information fusion. Simulation experiment shows that the proposed plan safeguards the communication between adjacent nodes and between upper and lower layers, ensures the durability of network security through real-time update of keys, and promotes the efficiency of data transmission through information fusion.

1. INTRODUCTION

The development of the Internet of Energy (IoE) has promoted the energy revolution in China. Under the Energy Internet of Things (EIoT), mass information is processed and computed by the powerful information devices in web-scale data centers (DCs) [1-5]. By 2015, the number of DCs in China has already surpassed 400,000. Data backup and disaster recovery are essential functions in DCs. These functions protect enterprise data from information loss or failure that arises from natural disasters, physical operating environment, etc. [6-9].

In a modern DC, numerous wireless sensors are deployed to form a network, which adopts various sensing techniques for environmental detection and equipment control [10]. However, the proliferation of the Internet of Things (IoT) has pushed up the security risk and energy cost of the wireless sensor network (WSN) [11-16]. The DC industry faces an urgent need to design an efficient strategy for information security management (ISM), and to reduce the energy consumption of the network.

In the EIoT, the sensors in the DC WSN are prone to attacks, and easy to suffer from ISM problems like poor real-time performance and high complexity. These problems generally come from the excessively large data flow [17-20]. In recent years, many ISM plans have been designed based on key management. To reduce computing and communication loads, Liu et al. [21] developed a layered key distribution method, but failed to analyze the security of the method. Based on low energy adaptive clustering hierarchy (LEACH), Ai et al. [22] proposed an elliptic curve cryptographic key management method, which ensures the security of multi-hop WSN in advanced measurement systems. Ai et al. [22] created a layered secure routing algorithm for attacks that target service terminals or inject fake packets. Yang et al. [23] introduced a key management method for broadcasting and multicasting under group identity mechanism, but the method consumes much energy due to the large number of message exchanges. Considering the limited storage of the DC WSN [24-25], the ISM models and algorithms must be capable of enhancing network security, reducing energy consumption, and improving dynamic performance.

This paper clarifies the structure of the DC WSN for the EIoT, models the WSN under the LEACH, and predicts the possible types of attacks. Then, the authors designed a real-time and dynamic ISM plan that optimizes the LEACH. The amount of data transmission was reduced through information fusion on the transmitted data. Simulation experiment shows that the proposed plan safeguards the communication between adjacent nodes and between upper and lower layers, and promotes the durability of network security and the efficiency of data transmission.

2. STRUCTURE OF THE DC WSN

Green computing, energy saving, and environmental protection are the only way for enterprises to realize sustainable development. During DC construction, it is a must to fully consider the energy consumption, and develop data backup facilities and disaster recovery systems that flexibly integrate centralized and decentralized modes.

As shown in Figure 1, the sensing objects, located at the bottom layer of the WSN, mainly include public electromechanical equipment, power and environmental equipment, switching signals of voltage and current transformers, temperature and humidity, water leakage and electric leakage, as well as intrusion.

The data of the above objects are collected by various sensors; processed and controlled by acquisition systems like building automatic control, power transformation and distribution, and power environment; integrated by common interfaces and protocols; displayed by the centralized monitoring system; and interacted with the operating system. In this way, the collected data serve the management of the entire DC.

The DC WSN can be viewed as a multilayer network with a large coverage. Each relatively independent area in the network collects and transmits data through its own sink node. The collected data are aggregated at multiple levels, before being reported to the integrated monitoring system, where the data are sorted and processed intelligently to support decision-making.

It is even more complex to access the DC WSN, in addition to the high degree of data integration. To safeguard intelligent terminals, users, information systems and data, it is imperative to build an intelligent network trust system that can be identified, trusted, and guaranteed, and explore deep into the research and application of secure access, transmission, and application. The ultimate goal is to realize trusted interactions and timely, secure connections between information systems, intelligent terminals and users.

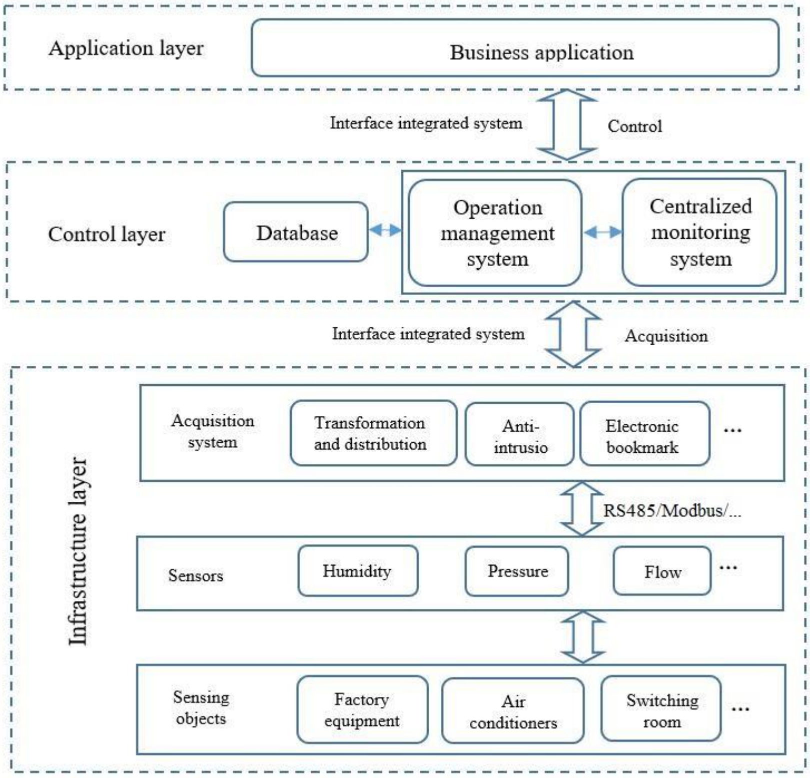


Figure 1. Structure of DC WSN

3. WSN MODEL AND ATTACK PREDICTION

This paper models the DC WSN based on LEACH, which has a discrete, uniform storage structure, and constantly adjusts its structure to optimize the next access. The BD WSN model is illustrated in Figure 2.

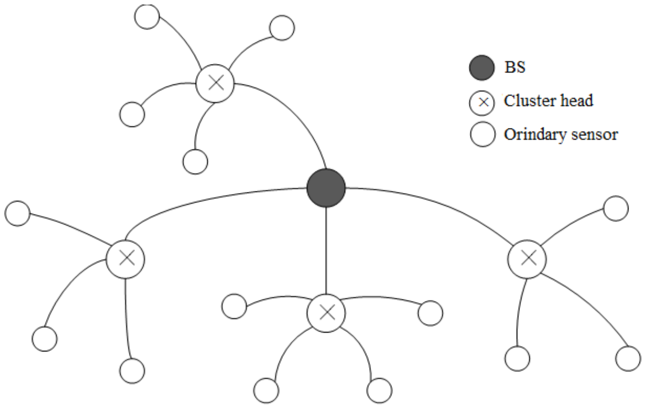


Figure 2. LEACH-based structure of BD WSN

In the sensing area A, the set of all sensors and the set of paths between the sensors can be denoted as $S=\{s_1, \ldots, s_{|S|}\}$ and $Path=\{p_1, \ldots, p_{|P|}\}$, respectively, where $|S|$ and $|P|$ are the number of sensors and paths. Each sensor in the WSN can be denoted as s_i, and the path between s_i and s_j as p_{ij}. If p_{ij} is one hop in length, then s_i and s_j can be referred to as neighbors.

Let cluster head s_{CHi} be a random sensor with relatively high energy in the WSN, that is, a physical host in the business, management or storage network in sensing area A. The s_{CHi} mainly collects and fuses the data from the ordinary sensors in its cluster, and transmits the fused data to the base station (BS).

In the WSN, each sensor is assigned a unique identification (ID) ID_x. Once the WSN structure is established, every ordinary sensor can receive/send data from/to its neighbors in the same cluster.

In the DC, the network key management aims to enhance the security and reliability of the IoT as well as the operation and maintenance network of information technology (IT). Therefore, it is of great importance to analyze the functions and model the possible attacks of the key management system. The attack model varies with the application environments.

The attacks against the DC WSN generally proceed in three steps:

(1) Decrypting the key system of the captured sensor;

(2) Deploying spy nodes to destroy or tamper with the data packets being transmitted in the network;

(3) Capturing and decrypting some data packets.

Once turned malicious, a sensor may act individually or collectively. The attack behaviors can be divided into direct malicious behaviors (dropping data packets, changing data content, and changing data packets), indirect malicious behaviors (reducing the credit of normal sensors and increasing the credit of malicious sensors), and disguised behaviors (replacing the ID of an existing sensor and trying to rejoin the WSN as a new sensor).

4. REAL-TIME DYNAMIC ISM PLAN

According to the proposed plan, the real-time dynamic key management includes four stags.

4.1 Neighbor verification

Once the WSN is deployed, the BS generates and assigns an initial key C_I to each sensor. Every sensor s_i produces its own basic master key $C_{si} = f_{CI}(ID_{si})$, using a one-way hash function *f*, and then broadcasts a message (ID_{si}, N_{si}) containing a random number *N*.

Upon receiving the message, neighbor s_j immediately replies s_i with a message (ID_{sj}, $MAC(f_{CI}(ID_{sj}), ID_{sj}|N_{si})$), where MAC is the message authentication code, and produces is master key $C_{sj} = f_{CI}(ID_{sj})$.

At this time, it is possible to obtain the pairwise master keys (PMKs) for effective communication between users, including the PMK for s_j to s_i $C_{sij} = f_{Csj}(ID_{si})$ and that for s_i to s_j $C_{sij} = f_{Csi}(ID_{sj})$. The workflow of this stage is shown in Figure 3.

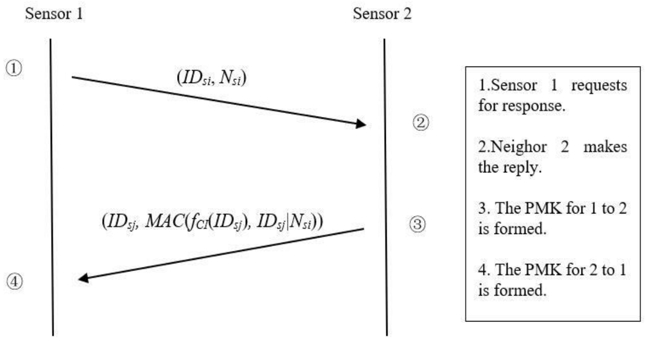

Sensor 1
Sensor 2
①
(ID_{si}, N_{si})
②
③
(ID_{sj}, $MAC(f_{CI}(ID_{sj}), ID_{sj}|N_{si})$)
④
1.Sensor 1 requests for response.
2.Neighor 2 makes the reply.
3. The PMK for 1 to 2 is formed.
4. The PMK for 2 to 1 is formed.

Figure 3. Workflow of neighbor verification

4.2 LEACH generation

The clusters of the initial LEACH are established simultaneously. Firstly, the cluster head s_{CHi} of cluster *i* broadcasts an encrypted message, which contains its ID ID_{sCHi} and master key C_{sCHi}, to the ordinary sensors $S_i = \{S_{ij}|S_{i1}, S_{i2}, \ldots S_{i|Si|}\}$ in its cluster.

Once S_i receives the message, each sensor s_{ij} computes its key with function *f*, decides which cluster to join, and adds the *ID*s of all its neighbors to the list of neighbors.

For the sensors that cannot exchange data under the protection of PMKs, their communication security needs to be maintained by creating the path key *PK* between each sensor s_{ij} and each cluster head:

$$PK_{sij-sCHi} = C_{sij} \oplus C_{E1} \oplus C_{E2} \oplus \cdots \oplus C_{Em} \oplus C_{sCHi}$$

There are *m* intermediate sensors between s_{ij} and s_{CHi}: $\{E1, E2, \ldots, Em\}$. Because the BS transmits keys via an intendent intermediate sensor, cluster head s_{CHi} will receive the MAC-protected *join* message from an ordinary sensor s_{ij}, decrypt the message, and send the *join-reply* message to that sensor. Then, the ordinary sensor will verify the legitimacy of the cluster head.

If no message is replied or the *join-reply* is wrong, ordinary sensor S_i will treat the cluster head as illegitimate, and will send an encrypted *alert* message to its neighbors for further verification. If the *join-reply* is correct, ordinary sensor S_i will work normally. The workflow of this stage is shown in Figure 4.

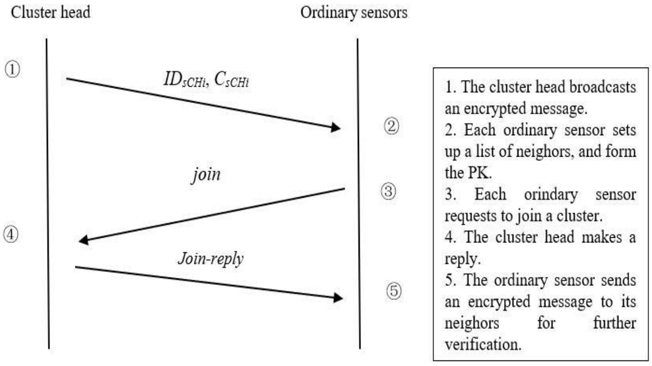

Cluster head
Ordinary sensors
①
ID_{sCHi}, C_{sCHi}
②
join
③
④
Join-reply
⑤
1. The cluster head broadcasts an encrypted message.
2. Each ordinary sensor sets up a list of neighbors, and form the PK.
3. Each orindary sensor requests to join a cluster.
4. The cluster head makes a reply.
5. The ordinary sensor sends an encrypted message to its neighbors for further verification.

Figure 4. Workflow of LEACH generation

4.3 ISM

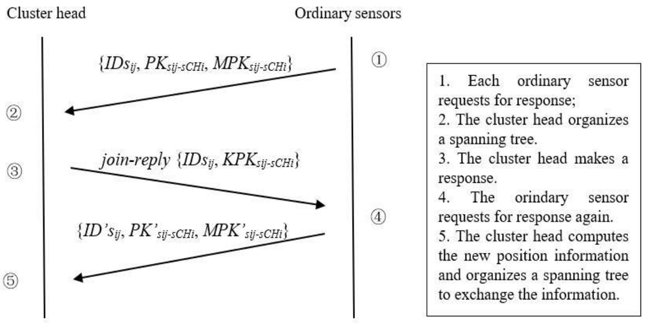
Firstly, each ordinary sensor s_{ij} sends a message containing $\{IDs_{ij}, PK_{sij-sCHi}, MPK_{sij-sCHi}\}$ to each cluster head s_{CHi}, serving as the initial information for the latter to construct the key system. Here, $PK_{sij-sCHi}$ and $MPK_{sij-sCHi}$ are the initial key and the new key to be exchanged. The initial value of $MPK_{sij-sCHi}$ is $PK_{sij-sCHi}$.

Upon receiving the message, s_{CHi} immediately decrypts the message, and organize the *ID*s and keys of all ordinary sensors in its cluster into a balanced LEACH, according to the initial algorithm of LEACH generation.

Once the LEACH is generated, the cluster head s_{CHi} will send the *join-reply* message $\{IDs_{ij}, KPK_{sij-sCHi}\}$ to the ordinary sensors s_{ij} in its cluster, where $KPK_{sij-sCHi}$ is a new key integrated from the old key $PK_{sij-sCHi}$ and the position information $LIDs_{ij}$. The cluster head will learn from $KPK_{sij-sCHi}$ and $LIDs_{ij}$ the keys of all ordinary sensors s_{ij} in its cluster, and assign them the corresponding position information.

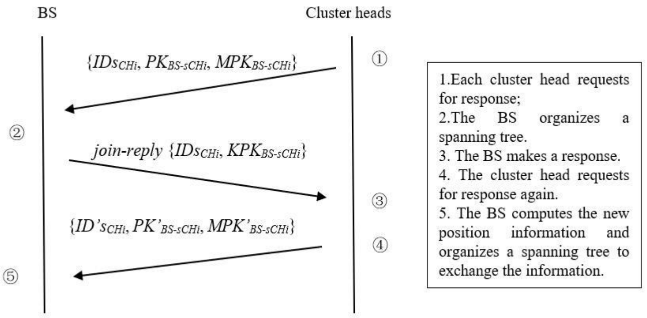
In the next cycle of information exchange, each cluster head, upon receiving the message from ordinary sensor s_{ij}, will exchange positions and compute new position information, as per the operation rules of LEACH. The workflow of the ISM between cluster head and ordinary sensors is shown in Figure 5.

Similarly, a LEACH can be established between the cluster heads and the BS: Firstly, the message of each cluster head is embedded with $\{IDs_{CHi}, PK_{BS-sCHi}, MPK_{BS-sCHi}\}$, where $MPK_{BS-sCHi}$ is the temporary intermediate key. Once receiving the message, the BS will organize the *ID*s and keys of all cluster heads into a LEACH.


Cluster head
Ordinary sensors
①
{IDs_{ij}, $PK_{sij\text{-}sCHi}$, $MPK_{sij\text{-}sCHi}$}
②
③
join-reply {IDs_{ij}, $KPK_{sij\text{-}sCHi}$}
④
{$ID's_{ij}$, $PK'_{sij\text{-}sCHi}$, $MPK'_{sij\text{-}sCHi}$}
⑤

1. Each ordinary sensor requests for response;
2. The cluster head organizes a spanning tree.
3. The cluster head makes a response.
4. The orindary sensor requests for response again.
5. The cluster head computes the new position information and organizes a spanning tree to exchange the information.

Figure 5. Workflow of the ISM between cluster head and ordinary sensors


BS
Cluster heads
①
{IDs_{CHi}, $PK_{BS\text{-}sCHi}$, $MPK_{BS\text{-}sCHi}$}
②
join-reply {IDs_{CHi}, $KPK_{BS\text{-}sCHi}$}
③
{$ID's_{CHi}$, $PK'_{BS\text{-}sCHi}$, $MPK'_{BS\text{-}sCHi}$}
④
⑤

1.Each cluster head requests for response;
2.The BS organizes a spanning tree.
3. The BS makes a response.
4. The cluster head requests for response again.
5. The BS computes the new position information and organizes a spanning tree to exchange the information.

Figure 6. Workflow of the ISM between BS and cluster heads

Once the LEACH is generated, the BS will send a response {IDs_{CHi}, $KPK_{BS\text{-}sCHi}$} to the cluster heads s_{CHi}, where $KPK_{BS\text{-}sCHi}$ is a new key integrated from the old key $PK_{BS\text{-}sCHi}$ and the position information $LIDs_{CHi}$. The BS will learn from $KPK_{BS\text{-}sCHi}$ and $LIDs_{CHi}$ the keys of all cluster heads s_{CHi}, and assign them the corresponding position information.

In the next cycle of information exchange, the BS, upon receiving the message from cluster head s_{CHi}, will exchange positions and compute new position information, as per the operation rules of LEACH. The workflow of the ISM between BS and cluster heads is shown in Figure 6.

4.4 Information fusion

In the ISM of a DC with a huge data flow, the amount of data transmission can be reduced by fitting the most amount of data with the most cost-effective model, thereby reducing the energy consumption of sensors. To save energy, the information under LEACH can be fused by the following multiple linear regression model:

$$Y = \alpha_0 + \alpha_1 X_1 + \alpha_2 X_2 \cdots + \alpha_K X_K + \varepsilon$$

where, Y is the estimated position; $X_i(i=1, 2, ..., n)$ are the factors that affect Y; $\alpha_i(i=1, 2, ..., n)$ are n+1 unknown regression parameters; ε is the random error term. Suppose the regression is carried out based on observations (X_{1j}, X_{2j}, …, X_{nj}, Y_j). Then, error between observation and estimation can be expressed as:

$$e_j = Y_j - \hat{Y}_j = Y_j - (\hat{\alpha}_0 + \hat{\alpha}_1 X_{1j} \cdots + \hat{\alpha}_n X_{kj})$$

Then, the regression parameter that minimize the sum of squares of e_j can be found by the least squares (LS) method. According to the extremum principle of the multivariate function, the derivative of e_j^2 relative to α_i can be found, and the LS estimation vector of α can be simplified as:

$$\hat{\alpha} = (X^T X)^{-1} X^T Y$$

To calculate α, the given position information (IDs_{ij}, $PK_{sij\text{-}sCHi}$), (IDs_{CHi}, $PK_{BS\text{-}sCHi}$) or replied position information (IDs_{ij}, $PK_{sij\text{-}sCHi}$), (IDs_{CHi}, $KPK_{BS\text{-}sCHi}$) can be substituted as variables into the following formula:

$$f(ID, PK) = \hat{\alpha} + \hat{\alpha}_1 y + \hat{\alpha}_2 y^2 + \hat{\alpha}_3 x + \hat{\alpha}_4 xy$$
$$+\hat{\alpha}_5 xy^2 + \hat{\alpha}_6 x^2 + \hat{\alpha}_7 x^2 y + \hat{\alpha}_8 x^2 y^2$$

By the above formula, it is possible to estimate the position of each sensor. Firstly, each ordinary sensor generates a series of regression parameters, and sends them to its cluster head as coefficients. Then, the cluster head will update the estimated positions based on the received coefficients. After that, new regression parameters will be computed based on the estimated positions and observed positions, and transmitted to the BS. Through information fusion, the cluster heads within the LEACH can obtain the coordinate boundaries of the sensing area.

If the BS needs to know the data at a given position, it will send a query message to each cluster head. Upon receiving the message, each cluster head from the BS to the given position will report the observed data to each other, and then execute the information fusion process. Throughout information fusion, the attributes of the information sensed in area A directly affect the accuracy of the fused value. The upper and lower bounds of the area can be defined as the minimum and maximum coordinates of all sensors within it.

5. SECURITY PERFORMANCE ANALYSIS

Compared with other ISM solutions, the proposed network has the following advantages:

(1) Early after network deployment, neighbor verification is performed to safeguard the communication between neighbors.

(2) During LEACH generation, cluster heads and ordinary sensors verify each other, ensuring the communication safety between upper and lower layers.

(3) During LEACH generation and ISM, the keys of cluster heads and BS can be updated in real time, enhancing the durability of network security.

(4) The information fusion effectively reduces the volume of data transmission and improves the transmission efficiency in the DC.

The proposed plan was simulated on Visual C++ and MATLAB, using the zero collision MAC protocol. A total of 250 sensors were deployed on the 800×800 sensing area. The temperature attribute was selected to evaluate the effectiveness of our plan. The temperature range of 30-35°C was regarded as normal, and that of 39-49°C as abnormal.

As shown in Figure 7, the probability that abnormal temperature is judged as normal and normal temperature is judged as abnormal did not increase with the transmission range of single sensor. The reason is that, during information fusion, ordinary sensors generate different multiple linear regression models for different observations. The e_j between the observed value and the regression value is independent of the transmission range of each sensor.

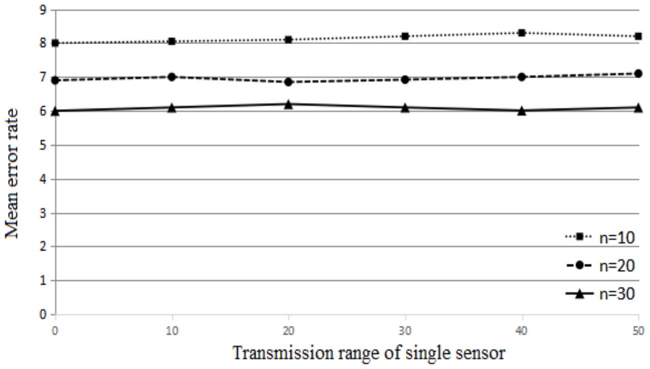


Figure 7. Relationship between error rate and transmission range of single sensor

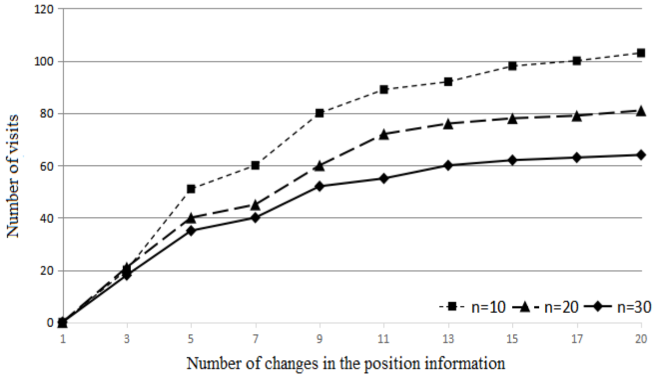


Figure 8. Relationship between the number of visits and the number of changes in the position information

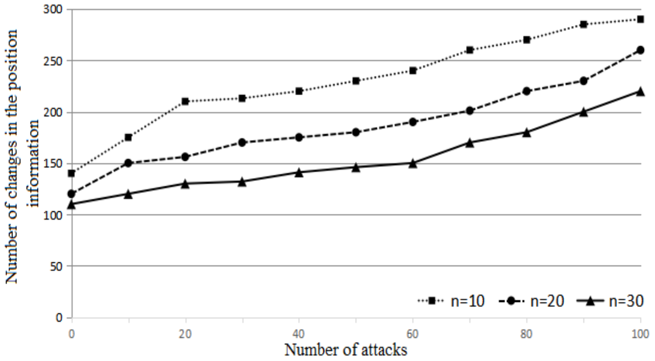


Figure 9. Relationship between the number of changes in the position information and the number of attacks

Figure 8 displays the number of changes in the position information of single sensor for temperature monitoring events. When an event is detected, only a few sensors are required to make the report. Hence, the keys are not frequently updated in the absence of network attacks. Therefore, each operation consumes a relatively short time, using the operation algorithm of the optimized LEACH and the ISM strategy centering on information fusion. In addition, the proposed plan meets the real-time requirements of the DC WSN on ISM and reduces the amount of energy consumed in ISM.

Finally, the security defense of our plan was tested under different number of attacks on single sensor. Figure 9 shows the simulation results on LEACH WSNs containing 10, 20 and 30 sensors. It can be seen that the number of changes in the position information increased with the number of attacks on single sensor. This is because, under our ISM strategy, the key update is triggered whenever a single sensor and even a cluster head is undermined. The frequency update protects the safety of network communication.

6. CONCLUSIONS

This paper aims to realize real-time, dynamic ISM of the DC WSN, reduce the amount of data transmission through data fusion, and save the energy consumed by sensors. For these purposes, the authors clarified the structure of the DC WSN for the EIoT, modelled the LEACH WSN, predicted the possible types of attacks, and optimized the LEACH structure. Simulation experiment proves that the proposed plan safeguards the communication between neighboring sensors and between upper and lower layers, enhances the durability and effectiveness of network security through real-time key update, and improves the efficiency of data transmission through information fusion.

ACKNOWLEDGMENT

This paper was supported by the Fundamental Research Funds for the Central Universities of Southwest Minzu University (Grant No.: 2017NZYQN33).

REFERENCES

[1] Wang, A.P., Fan, J.G., Guo, Y.L. (2016). Application of blockchain in energy interconnection. Electric Power Information and Communication Technology, 14(9): 1-6.

[2] Zhang, Y. (2019). Energy efficiency management and route optimization for wireless sensor network under the ubiquitous power internet of things. European Journal of Electrical Engineering, 21(2): 217-222. https://doi.org/10.18280/ejee.210213

[3] Li, B., Cao, W.Z., Qi, B., Sun, Y., Guo, N., Su, Y., Cui, G.Z. (2017). Overview of application of block chain technology in ancillary service market. Power System Technology, 41(3): 736-744. https://doi.org/10.13335/j.1000-3673.pst.2016.1179

[4] Fedele R., Merenda M., Praticò F.G., Carotenuto R., Corte F.G.D. (2018). Energy harvesting for IoT road monitoring systems, Instrumentation Mesure Métrologie, 17(4): 605-623. https://doi.org/10.3166/I2M.17.605-623

[5] Nellore, K., Hancke, G.P. (2016). A survey on urban traffic management system using wireless sensor networks. Sensors, 16(2): 1-25. https://doi.org/10.3390/s16020157

[6] Wu, C.M., Yang, T., Ma, D.M., Guo, J., Zhao, Y.X. (2016). An improved DV-HOP wireless sensor network positioning algorithm. Journal of Henan University of Science and Technology (Natural Science Edition), 37(6): 55-60. https://doi.org/10.15926/j.cnki.issn1672-6871.2016.06.012

[7] Manikandan, G., Sakthi, U. (2018). Dynamic key management system using channel hopping in IEEE 802.15.4 wireless sensor networks. International Journal of Mobile Network Design and Innovation, 8(2): 73-79. https://doi.org/10.1504/IJMNDI.2018.092343

[8] Thevar, G.K.C., Rohini, G. (2017). Energy efficient geographical key management scheme for authentication

in mobile wireless sensor networks. Wireless Networks, 23(5): 1479-1489. https://doi.org/10.1007/s11276-016-1228-9

[9] Kang, S.Y. (2017). Development status and research progress of quantum communication technology. Security Science and Technology, (3): 7-10.

[10] Yang, M. (2017). Discussion on the development status and development trend of quantum communication technology in the new era. China High Technology, 1(3): 35-37.

[11] Chen, Z.Y., Hao, H.Y., Wang, D., Gao, D.Q., Li, G.C., Cao, Y.F. (2018). Research progress and prospect of practical technologies for quantum secure communication. Electric Power Information and Communication Technology, 16(4): 15-23.

[12] Talmale, R., Bhat, M.N., Thakare, N. (2019). Energy attentive pre-fault detection mechanism with multilevel transmission for distributed wireless sensor network. Revue d'Intelligence Artificielle, 33(2): 97-103. https://doi.org/10.18280/ria.330203

[13] Chen, H., He, Y.H., Li, K., Huang, W., Xu, B.J. (2018). Quantum key service and mobile application technology. Journal of China Academy of Electronics and Information Technology, 13(4): 406-409, 414.

[14] Luo, B. (2018). Quantum communication and its application in power communication. Electronic Test, (20): 76-77.

[15] Wang, L., Zhao, G.H., Fan, X.N., Ni, P.C., Lin, C., Chen, H., Zhang, D.W., Wen, L.F. (2018). Research and design of quantum private communication in power grid service application. Electric Power Information and Communication Technology, 16(3): 34-38. https://doi.org/10.16543/j.2095-641x.electric.power.ict.2018.03.005

[16] Cao, Y., Zhao, Y.L., Yu, X.S., Zhang, J. (2017). Secure power communication network architecture driven by quantum key distribution. China Electric Power, 50(10): 8-11, 34. https://doi.org/10.11930/j.issn.1004-9649.201708037

[17] Miao, C.H., Wang, J.F., Wei, S.H., Liu, Y. (2018). Design of mobile terminal encryption scheme based on quantum key. Network Security Technology and Application, (6): 38, 44.

[18] Irshad, T., Ishak, D., Baloch, M.H. (2019). Comparative analysis of rectangular and circular four-resonator coil system for wireless power transfer using magnetic resonance coupling technique. European Journal of Electrical Engineering, 21(1): 67-73. https://doi.org/10.18280/ejee.210111

[19] Zeng, M., Wang, Y.Q., Li, M.Z., Dong, H.Q., Zhang, X.C., Wang, H.L., Huo, X.X., Zhang, Z.G. (2019). A preliminary study on the architecture and implementation scheme of the ubiquitous power internet of things. Smart Power, 47(4): 1-7. https://doi.org/10.3969/j.issn.1673-7598.2019.04.001

[20] Jiang, X.C., Liu, Y.D., Fu, X.F., Xu, P., Wang, S.J., Sheng, G.H. (2019). Ideas and development trends of ubiquitous power IoT network construction of transmission and distribution equipment. High Voltage Technology, 45(5): 1345-1351. https://doi.org/10.13336/j.1003-6520.hve.20190505001

[21] Liu, J.M., Zhao, Z.Y., Ji, X. (2018). Research and application of internet of things technology in power transmission and distribution System. Journal of Internet of Things, 2(1): 88-102.

[22] Ai, J.W., Dang, X.J., Lv, Q.S., Mei, C.H., Zhang, Y.Y. (2019). Research on full dimension equipment status monitoring system with panoramic function. Power System Protection and Control, 47(16): 122-128. https://doi.org/10.19783/j.cnki.pspc.181158

[23] Yang, C.K., Su, Y.F., Ren, S.Z., Ding, B. (2019). Secure access technology of electric power LTE private network based on improved authentication protocol. Electric Measurement and Instrumentation, 56(3): 91-96.

[24] Zou, X.F., Xiao, Y.X. (2018). SM2-based distribution network Modbus message security research. Power System Protection and Control, 46(12): 151157.

[25] Kumar, R.V.K., Naik, G.M., Murali, G. (2019). Wireless nano senor network (WNSN) for trace detection of explosives: The case of RDX and TNT. Instrumentation Mesure Metrologie, 18(2): 153-158. https://doi.org/10.18280/i2m.180209