Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 183 (2021) 486–492

Procedia Computer Science

www.elsevier.com/locate/procedia

The 10th International Conference of Information and Communication Technology (ICICT-2020)

Security and application of wireless sensor network

Zhang Huanan*, Xing Suping, Wang Jiannan

School of Data and Computer Science, Guangdong Peizheng College, Guangzhou,510830 , China

Abstract

At present, wireless sensor networks are developing rapidly with the support of the Internet of things. Wireless sensor networks can deliver the information people need at any time, free from the constraints of time and space. Wireless sensor network is widely used, which lays a solid foundation for the development of Internet of things. As the node deployment environment of wireless sensor networks is usually very complex, it is necessary to study the security of wireless sensor networks so as to reduce security threats and network attacks. In this paper, the security and application of the wireless sensor network are emphasized.

Keywords: Wireless sensor network, Security of WSN, Application of WSN, Communication.

1. Introduction

Wireless Sensor Network (WSN) is perception, and the main tool is sensor. The use of sensors can effectively sense the external environment, and then with the help of wireless network for information transmission, to meet user needs. The security of wireless sensor network must be paid attention to, because it is supported by high technical content and complex structure, once there is a problem, the consequences are unimaginable. The development of the Internet of things is inseparable from wireless sensor networks, and the ability of people to communicate quickly is also closely related to it [1].

WSN can be used to collect all kinds of data and information and deal with all kinds of complex environments, the application of WSN covers all aspects. In the military field, it can be used to detect the deployment of troops in enemy terrain and other situations, and it has the function of detecting biological and chemical pollution and nuclear radiation. In terms of environmental monitoring and protection, it can be used for data collection in the field

* Corresponding *E-mail address:* topwn2008@@163.com

10.1016/j.procs.2021.02.088

environment, tracking animal footprints, analyzing pollution situation, and predicting the explosion of forest fire and debris flow. In the field of industry and agriculture, the monitoring of crop growth and product flow intelligent production. In the field of medical care and health, it can realize the function of obtaining physiological data of patients, analyzing their conditions, and timely receiving medical treatment. In addition, wireless sensor network plays a crucial role in the field of smart home, smart transportation, smart city, cultural relic protection and business, etc. Wireless sensor network is changing people's life [2].

The information security of WSN is concerned in many contexts, such as military medical disaster prevention and other fields. Wireless sensor networks use open wireless communication channel technology to transmit data, but without security protection means, data is very vulnerable to internal and external attacks [3]. However, the amount of computation based on the cryptographic defence method is not suitable for WSN network. Therefore, it is also a big problem to choose an appropriate encryption method to ensure the security of WSN information [4].

2. The characteristics of WSN

The wireless sensor networks have the following characteristics:

2.1. Freedom of organization.

The construction of the wireless network sensor is not restricted by any external conditions. The organizer can quickly set up a wireless network sensor network with complete functions no matter when and where, and the maintenance and management work after the successful construction is completely carried out within the network [5].

2.2. Uncertainty of network topology.

From the perspective of network hierarchy, the network topology of wireless sensors is changeable. For example, sensor nodes that constitute the network topology can be increased or decreased at any time, and the network topology diagram can be separated or merged at any time.

2.3. The control mode is not centralized.

Though wireless sensor network (WSN) the centralized control of base station and sensor node, but between each sensor node control mode or distributed, routing, and the function of the host by the network of terminals for each host independent operation, non-interference in each other, so the strength of the wireless sensor network (WSN) is very high, it is difficult to be destroyed [6].

2.4. Low safety.

Wireless sensor network uses the wireless way to convey information, so the sensor nodes in the process of passing information is easy to be invaded by the outside world. Therefore, the leakage of information and the damage of wireless sensor network (WSN), most of the wireless sensor network nodes are exposed, which greatly reduces the security of the wireless sensor network [7].

3. 3. Security of WSN

Security of wireless sensor networks (WSN) has become a hotspot in the research of WSN technology. The characteristics of wireless sensor networks make them vulnerable to multiple attacks, which seriously affects the confidentiality, integrity and availability of data. Especially when the routing of the network is attacked, the data collected by the sensor node cannot be transmitted to the destination sink node timely and accurately. Just like the traditional computer communication network, the security threat of wireless sensor network mainly comes from various attacks. Radio characteristics of wireless channel and ad-hoc network features are making it easier for the

sensor network attacker's passive attacks and active attacks, sensor networks will be monitored, tampered with, forge and block attacks, at the same time, wireless sensor network as a kind of energy depletion, energy constrained sensor nodes, the network is vulnerable to denial of service attacks [8]. Wireless sensor networks may be attacked in the following ways:

(1)The physical layer network is vulnerable to congestion attack and physical damage. when the attacker knows the communication frequency of wireless sensor network, it will transmit radio interference near the frequency point of the network, making the network unable to work normally, it is congestion attack. Physical damage, sensor nodes are mostly deployed in unattended areas, and nodes are easy to be captured by attackers and hidden in the network for monitoring and damage.
(2)The link layer is vulnerable to collision attack, exhaustion attack and unfair competition attack. Collision attack means that the attacker sends malicious data grouping in the legitimate node, so that the output signals cannot be recognized due to overlapping.
(3)The network layer includes discard and selective forwarding, sink node attack, direction misdirection, sink hole attack, etc. Discard and selective forwarding refers to that when a malicious node is lurking in the network, some data packets may be dropped randomly when it receives the data packets sent by the upstream node. Or, malicious nodes group their data and send it with high priority, affecting normal network communication. Direction misdirection, namely false routing information attack, attackers forge, tamper or replay routing information to cause routing loop, attract or block network traffic, extend or shorten the source path, in order to achieve the purpose of splitting the network, increasing end-to-end delay and so on.
(4)The transport layer includes flood attack and synchronous damage attack. Flood attack means that the attacker constantly requests to establish a connection with the neighbor sensor node, thus depleting the resources of the neighbor node to establish a connection and causing other legitimate requests to be ignored.

Combined with the characteristics of wireless sensor network, the security purpose of wireless sensor network is summarized based on the analysis of security threats at all levels of the network: confidentiality, to prevent data eavesdropping and stealing by illegal users, key management to provide a secure key update and management mechanism; Integrity of data to prevent information from being tampered with illegally; Freshness of data to prevent malicious nodes from sending the same information to consume network resources; Auditability, can audit the whole access process of the system; Non-repudiation, the sensor nodes participating in the network communication process can’t deny its behavior; Access authentication, to verify the sensor nodes in the network, to verify the legitimacy of its identity; The physical device is safe to prevent sensor nodes from being stolen, destroyed, and safe to use [9].

Different from traditional wireless network wireless sensor network (WSN), the power of the sensor node energy, data processing, storage and communication ability are limited, and most of sensor nodes deployed in unmanned guard area, makes the safety of the wireless sensor network is faced with more challenges, so the traditional security protection mechanism can’t be completely applicable to wireless sensor network (WSN) [10].

4. 4. The key technology

4.1. Node security optimization technology

Node security optimization technology can also better serve the security protection of wireless sensor networks. This paper will introduce a node security optimization technology based on ternary key distribution algorithm, which can simplify the topology structure of nodes and improve the anti-attack performance of wireless sensor networks, so as to protect its security [14].In the process of optimizing wireless sensor network nodes, for security consideration, nodes should be distributed in the form of clusters, so as to complete the optimization by means of secure routing and key calculation. The network topology of wireless sensor network consists of variety forms of network nodes, network topology by using the way of cluster head election node self-organization form, each cluster key using three kinds of key distribution, in order to meet the needs of the key calculation, cooperate to adjust the adaptive security routing, wireless sensor network attack resistance can be improved [11].

A large number of network nodes are distributed in the wireless sensor network, and these nodes have unique ID identification. In the specific layout of the network, the ID of each node will be comprehensively counted in the form of a table. The network topology formed by the self-organizing nodes can be well understood by the base station, and the network nodes can propagate their ID by broadcasting after deployment. The interception of adjacent nodes can thus be implemented. Adjacent node ID can be added and counted in the routing table to form a separate cluster. The corresponding cluster heads can be selected by using the LEACHA protocol [11].

The cluster heads have the feature that the coverage scope will be broadened with the increase of signal strength. In the process of selecting cluster head, it is necessary to compare the range of preset threshold value with the value range of random number generated by wireless sensor node. If the preset threshold range is reduced, the corresponding node can be determined as cluster head [12].

There are three kinds of key calculation involved in the application of three key distribution algorithms. The keys are between base station and cluster head, between cluster head and sensor node, and between sensor node and base station. Kn key shall be used for data encryption of base station node. It can satisfy the need of key calculation between sensor node and base station. After receiving the broadcast message from the base station, ordinary sensor nodes need to decrypt the broadcast message data, and Ks can be used to decrypt this process. Ultimately, adaptive adjustment is needed. And send the fused data to the base station to carry out targeted adaptive adjustment. For example, wireless network has a single - stage clustering structure. It is necessary to adjust and optimize the secure routing algorithm, including base station routing algorithm and sensor node routing algorithm [13].

The optimization of base station routing algorithm should focus on whether the message broadcasting needs to be carried out through the base station. If the message needs to be broadcast through the base station, the message needs to be encrypted with the key Kn. If there is no need to broadcast, the cluster-head node can be automatically detected. Determine whether the sent data exists. If the sent data is found, it can be automatically decrypted with node ID and key KS. In order to verify the integrity and reliability of the data, MAC shall be used for verification, and incomplete or wrong data packets shall be discarded, otherwise, the data shall be processed to obtain the final information. In the process of adaptive adjustment of sensor node routing algorithm, Kn key is used for data encryption, and then the data can be sent to the cluster head. Packet decryption can be completed based on Kc, and the cluster head needs to add its own ID at the same time, and finally the Kn encrypted data is sent to the base station [14].

4.2. Data security fusion technology

Wireless sensor network nodes are generally located in security-sensitive areas and unsupervised environments, which makes data fusion of wireless sensor network easy to face various security threats. Under the influence of low energy cost, a complete security mechanism must be provided to ensure data security. Data integrity scheme and data rolling scheme are common data integration schemes in current wireless sensor networks. The former is based on data integrity, while the latter is based on data privacy. And in order to guarantee the data security, cooperate more symmetric cipher algorithm of data fusion method by encryption scheme, this scheme has high applicability to advantage, but also exists the shortage of the aggregation point too expensive, in order to reduce the energy consumption of the present scheme, can be targeted to adjust intermediate node in the process of data transmission, make its not decrypt the received data, and through the aggregation number, will receive the data packet and forward their own data encryption to the parent node, by omitting decrypted and encrypted link again, can greatly reduce energy consumption, and this change will not affect the network security, This new protection scheme with both security and low energy consumption is the data security fusion technology [15].

In order to ensure that the data fusion technology can better serve the security of wireless sensor networks, a data fusion security scheme based on trust mechanism should be specifically designed, in which the direct trust factor and mutual trust factor are composed of trust management factors of wireless sensor networks. Through to observe the motion of the monitoring node module, pretreatment and calculate the network monitoring results, can be based on the direct trust DT mentioned in the calculated value and build the trust value of the complete CT each node comprehensive letter stated value calculation, calculation result will be sent to the trust decision module described in the fusion processing, can carry out pertinent fusion processing. In the fusion process, in order to make the member nodes trust, the sampled fusion nodes should be watched by the cluster member nodes according to their behaviors.

In combination with data fusion byte points, the result set nodes should be calculated and evaluated, and the base station should be responsible for the final decision. In comprehensive trust value computation link, according to the integration of each node to store trust direct CT, indirect trust value T, direct trust value DT, can according to the trust value and the current trust DTNT history value synthesis method of weighted summation, the complete direct trust value computation, indirect trust value this process must be applied to include weighted factor is recommended [16].

In order to avoid the calculation error of indirect trust, it is necessary to pay more attention to whether the weighted factor is involved in the calculation, and the influence of the trust mechanism characteristics of periodic behaviors and the recommendation level of historical trust on the trust of fixed nodes should also be paid attention to. The specific formulation of data fusion security scheme should be combined with the need to protect privacy. In order to ensure the privacy of wireless sensor network, encryption processing method is generally adopted, and data fusion protection algorithm can also be adopted. This paper proposes to adopt an improved SMART scheme based on the traditional SMART scheme. Traditional SMART solutions by data detection, segmentation and convergence order of three phase, considering the cost of the scheme in recent years, and reduce the cost cannot adopt the way of lower safety threshold, so need to choose plan of improvement of SMART, with specific network initialization, data transmission, data fusion, to be able to better service in wireless sensor network security, network initialization should first establish the relief valve, and establish the data fusion tree. Data transmission needs to allocate different transmission time for each node group to avoid location and information exposure. Therefore, when passing through intermediate node I, the packet will not be forwarded directly, but will be forwarded after passing through random cache time T. Data fusion is based on data fusion tree expansion, and the key is used to add and decrypt data [17].

5. Range of application

It is important to note the role of the security layer that connects devices (sensor nodes) with applications (cloud computing, business intelligence layer); therefore, security is an important issue. However, security is not only applied at the highest-level layers but applied from the lower-level layer upwards (fig.1).

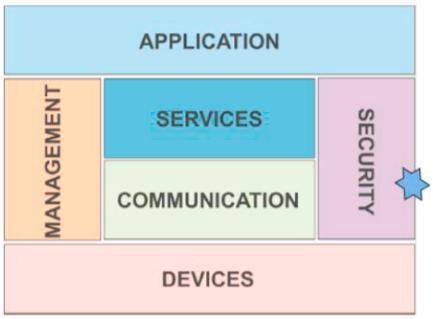

Fig.1. The application of security

5.1. The application of wireless sensor in electrical automation

With the rapidly development of automation technology, the automation of power system helps to reduce unnecessary energy waste, reduce the incidence of accidents, and improve the efficiency of repair and maintenance when accidents occur. Power system management requires low fault tolerance rate, which requires real-time monitoring of power system. Adjust the voltage according to the external environment, such as weather and temperature. If the external conditions change dramatically, the power properties in the power system will also change greatly. The collection of data is an important. There need to be devices that can count the values of electrical properties in the electrical system and then process them. Control it according to the transmitted data, improve its automation level. In addition, in electrical automation, most of the wireless sensor devices are used,

which can avoid some circuit problems and improve the efficiency of the sensor devices. In the power system, especially the high voltage transmission line, if the line is more complex, then its management and maintenance are very difficult, and have a high risk. Wireless sensors are less likely to be damaged and transmit more accurate and valuable data [18].

5.2. The application of wireless sensor technology in monitoring

In the process of monitoring using wireless sensor technology, different types of monitoring work used monitoring equipment is not only the same. In the process of industrial production, the most commonly used sensing technology is temperature sensing technology. In the process of industrial production monitoring using the sensing technology, it mainly monitors the boiler to ensure the safety of the boiler. In the boiler, and boiler temperature is closely related to the boiler's water cooling tube, today's common water cooling tube is mostly composed of steel tube, the heat in the process of discharge, need to discharge through the steel tube. During cooling process, with a large amount of heat discharge, so today's boiler management to use the computer remote control, and to avoid high temperature environment on the staff harm. However, the remote control technology requires the boiler monitoring in the high temperature environment, and need to invest more costs. In the process of data transmission, measurement data can be directly transmitted. In this way, during the process of monitoring and management, the number of damaged parts will be reduced, which can effectively reduce the production cost. And the use of wireless sensor network, can be more comprehensive monitoring of different parts, so that the work is more comprehensive [19].

5.3. The application of wireless sensing technology in positioning

Network location technology can achieve accurate location and meet user needs. Network location technology reflects the interactive characteristics of network information, the common technology is GPS. The technique can accurately locate the target position. Wireless sensor network can achieve accurate positioning, low application cost, and greatly meet user needs. Wireless sensor network (WSN) mainly range-based localization and non-distance location to lock the target position, but these two methods have their own advantages and disadvantages. The former cost high, positioning is very accurate; The latter has low cost and is far less accurate than the former.It is a great significance for the navigation of cars. In addition, the wireless sensor technology can also be used for some carry-on items, real-time location of some elderly or children, to avoid some vulnerable in the accidents [20].

6. Conclusion

With the rapid development of sensor technology and communication technology, the application of the wireless sensor network will be deeper and wider. As a basic security service, secret key management will attract more attention. The secret key management scheme and protocol must conform to satisfy the characteristics of WSN, such as scalability, low computational complexity, low storage space, low communication load, variable topology, etc., and must be closely related to the application. The security distribution, self-organization, fault tolerance and combination with geographic information of secret key management schemes and protocols will be the focus of the next research work.

References

1. Meena,O.P. and Somkuwar,A. Comparative Analysis of Information Fusion Techniques for Cooperative Spectrum Sensing in Cognitive Radio Networks.Proceedings of International Conference on Recent Trends in *Information,Telecommunication and Computing* ,ITC(2014)
2. Prema, G. and Narmatha, D.Performance of Energy a Ware Cooperative Spectruim Sensing Algorithm in Cognitive Wireless Sensor Network.Online *International Conference on Green Engineering and Technologies* (IC-GET), Coimbatore, 19 November (2016) .
3. Gharaei,N.,Abu Bakar,K.,Mohd Hashim,S.Z., Hosseingholi Pourasl,A.,Siraj,Mand Darwish,T. An Energy-Efficient Mobile Sink-Based Unequal Clustering Mechanism for WSNs.*Sensors(Basel)*,17,1858(2017).
4. Akyildiz, I.F.,Lo,B.F. and Balakrishnan,R. Cooperative Spectrum Sensing in Cognitive Radio Networks:A Survey.*Physical Communication* ,44,40-62(2011).

5. Alhumud, H.and Zohdy,M. Managing Energy Consumption of Wireless Sensors Networks in Multiple Greenhouses.*Wireless Engineering and Technology* ,99, 11-19(2018).
6. Wang,N.,Huang,Y. and Liu,W.A Fuzzy-Based Transport Protocol for Mobile Ad Hoc Networks. *IEEE International Conference on Sensor Networks,Ubiquitous,and Trustworthy Computing* , Taichung, 11-13 June 2008, 320-325 .
7. Zeng,B.and Yan,D.An Energy Efficient Harmony Search Based Routing Algorithm for Small-Scale Wireless Sensor Networks.IEEE 17 th International Conference on Computational Science and Engineering , Chengdu, 19-21 December 2014, 362-367.
8. Lee, H.M.,et al.Optimal Cost Design of Water Distribution Networks using a Decomposition Approach. *Engineering Optimization* , 48, 2141-2156 (2016).
9. Hoang, D.C., et al.Real-Time Implementation of a Harmony Search Algorithm Based Clustering Protocol for Energy-Efficient Wireless Sensor Networks.*IEEE Transactions on Industrial Informatics*,10,774-783 (2014).
10. Parenreng, J.M. and A. Kitagawa, A Model of Security Adaptation for Limited Resources in Wireless Sensor Network. *Journal of Computer and Communications*, 2017. 05(03): p. 10-23.
11. Vijayarajeswari, R., A. Rajivkannan and J. Santhosh, A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN. *Circuits and Systems*, 2016. 07(08): p. 1341-1351.
12. Saravanaselvan, A. and B. Paramasivan, Implementation of an Efficient Light Weight Security Algorithm for Energy-Constrained Wireless Sensor Nodes. *Circuits and Systems*, 2016. 07(09): p. 2234-2241.
13. Savoine, M.M., M.O.D. Menezes and D.A.D. Andrade, Proposal of a Methodology for the Assessment of Security Levels of IoT Wireless Sensor Networks in Nuclear Environments. *World Journal of Nuclear Science and Technology,* 2018. 08(02): p. 78-85.
14. Liu, Y. and Y. Morgan, Security Analysis of Subspace Network Coding. *Journal of Information Security*, 2018. 09(01): p. 85-94.
15. Parmar, K. and D.C. Jinwala, Symmetric-Key Based Homomorphic Primitives for End-to-End Secure Data Aggregation in Wireless Sensor Networks. Journal of Information Security, 2015. 06(01): p. 38-50.
16. Mawlood Hussein, S., J.A. López Ramos and J.A. Álvarez Bermejo, Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro. Sensors, 2020. 20(8): p. 2242.
17. Adil, M., et al., An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks. Sensors (Basel), 2020. 20(8).
18. Han, D., Du X and Y. Lu, Trustworthiness and a Zero Leakage OTMP-P2L Scheme Based on NP Problems for Edge Security Access. Sensors (Basel), 2020. 20(8).
19. Shang, X., et al., Secrecy Performance Analysis of Wireless Powered Sensor Networks Under Saturation Nonlinear Energy Harvesting and Activation Threshold. Sensors (Basel), 2020. 20(6).
20. Wang, R., Wang, B., Ding, X. et al. Planar array with bidirectional elements for tunnel environments. Sci Rep 7, 15421 (2017). https://doi.org/10.1038/s41598-017-15817-4