International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.219-228
http://dx.doi.org/10.14257/ijsia.2016.10.12.17

An Intrusion Prevention Technology Based on Dynamic Random Password Authentication in Wireless Sensor Networks

Xiaolong Xu[1], Zhonghe Gao[2] and Lijuan Han[1]

[1]*Experiment Teaching Center, Qufu Normal University, Rizhao Shandong 276826, China*
[2]*Institute of Software, Qufu Normal University, Qufu Shandong 273165, China*
xiaolongxu@foxmail.com

Abstract

Security is an important problem in wireless sensor networks. Intrusion detection system is one of the most common methods of network security, for which more and more people have shown solicitude. In this paper, a dynamic random password authentication (DRPA) method is proposed for the identity authentication of communication nodes, which can detect and prevent malicious behavior at each stage of the network operation. This paper introduces the method of automatic generation of random passwords. When a user wants to communicate, the password will be verified to confirm whether it is a normal user or a malicious user. The password's generation and verification process is very suitable for wireless sensor networks. By using NS2, the simulation experiments are carried out and the results show that this method is superior to the other methods.

Keywords*: Wireless sensor network; Dynamic random password; Intrusion prevention*

1. Introduction

Intrusion detection system is a kind of active network security technology, which will alert us or take active response when suspicious transmissions are found. But there is also the problem of false negatives and false positives [1]. In recent years, mobile communication technology has got rapid development. Smartphones, tablet computers are becoming more and more popular, and they are able to access the Internet at high speed and bring us many conveniences. People's lifestyles have changed a lot. Communication, entertainment, travel, shopping, finance and so on can be achieved by means of mobile communication devices. There is a lot of personal sensitive information in mobile devices and there are many attackers in the network, so it is necessary to protect mobile devices and their communication. Host-based detection, network-based detection, misuse detection and anomaly detection are popularly used intrusion detection technologies nowadays [2].

Wireless sensor network consists of a large number of sensor nodes deployed in the monitoring area, which is a multi-hop network using wireless communication. Its purpose is to cooperatively sense, collect and process the information of the objects in the network coverage area, and send it to the observer. Wireless sensor networks have many types of sensors, which can detect various phenomena in the surrounding environment such as earthquake, electromagnetism, temperature, humidity, noise, light intensity, pressure, velocity and direction [3]. In order to obtain accurate information, tens of thousands of sensor nodes, or even more are usually deployed in the monitoring area. The sensor node consists of interface circuit, micro controller, signal transceiver and battery. The performance of the sensor node depends on the parameters such as bandwidth, energy consumption, memory and calculation speed. Network security includes authentication, privacy, robustness, integrity, survivability, and etc. [4] Considering those different aspects, a variety of different network security methods are proposed.

ISSN: 1738-9976 IJSIA

Wireless sensor network security includes many aspects, in which the authentication and confidentiality mechanisms are of great importance. Therefore, many people committed to the development of confidentiality and authentication protocol [5]. In order to improve the security of wireless sensor networks further, the DRPA algorithm is introduced. The security level of the system is improved by the randomly generated password, which plays a defensive role in attack behaviors. The password is a combination of letters, numbers and special symbols, which is difficult to crack and has high security.

2. Literature Review

In this section the previous literatures will be reviewed, in which various kinds of attacks and coping strategies were discussed. Literature [6] proposes a score-based multi-cycle intrusion detection algorithm, and detects the change of nodes rapidly according to the attributes of nodes. This method is also called the Shiryaev-Roberts method, which is more effective than other detection methods. Method in literature [7] classifies detection probability by sensing scene and analyzing intrusion detection problems in wireless sensor networks. It verifies the consistency of user behaviors by examining and comparing various network parameters. Based on extreme learning machine, a hybrid intrusion detection framework is proposed in literature [8], which divides the wireless sensor network into different layers and then uses appropriate intrusion detection methods in each layer.

From the perspective of network survivability, literature [9] discusses the security of the wireless sensor network, which enhances the network security from the aspects of route control, network reconfiguration, topology evolution and so on. In literature [10], a post-processing solution with multiple IDS sensor indication systems is introduced, and each set of instructions is aggregated into a single instruction to improve the quality of the system. Whenever a critical event occurs, the instruction system creates a related alert for all the other nodes in the network. In order to prevent the data from being tapped at the time of transmission, literature [11] provides a distributed decision fusion method FRSM, which can ensure the data to be turned over by the random function in order to prevent the eavesdropping, once the sensor node transmits data to the fusion center.

2.1 Existing System

To detect and prevent malicious behaviors in wireless sensor networks, an intrusion detection system based on leader was proposed in [12], and the name of this system is Leader Based Intrusion Detection System (LBIDS). A leader is selected from a group of nodes in the network and monitors these nodes. When a node is activated, then it will notify the leader of its own status, so the leader knows all the nodes' information. Leader information should also be notified to the new nodes, but it will be time consuming. In order to solve this kind of problem, this paper puts forward the DRPA (Dynamic Random Password Authentication) method.

3. Problem Description

With the development of mobile communication, people's requirements on mobile devices is no longer confined to making and receiving calls, sending and receiving messages, etc., but requiring them to have more perfect business and entertainment functions, such as inquiries, booking, payment, transfer and etc. Once a security problem occurs, there will be a significant loss, so it is necessary to provide a security mechanism for the communication units [13]. The main purpose of this paper is to design a mechanism to detect malicious behavior based on the identity information.

3.1. Structure of the System

The proposed DRPA system consists of three modules, namely, node identification module, mutual authentication module and key updating module. The comprehensive function and working process of the system is illustrated clearly in Figure 1. The network G is a wireless network, and the node can be any type of wireless communication devices, such as mobile phones, tablet PCs, laptops, etc. The base station is responsible for managing the entire network, which can assign ID, key, and carry out the key verification.

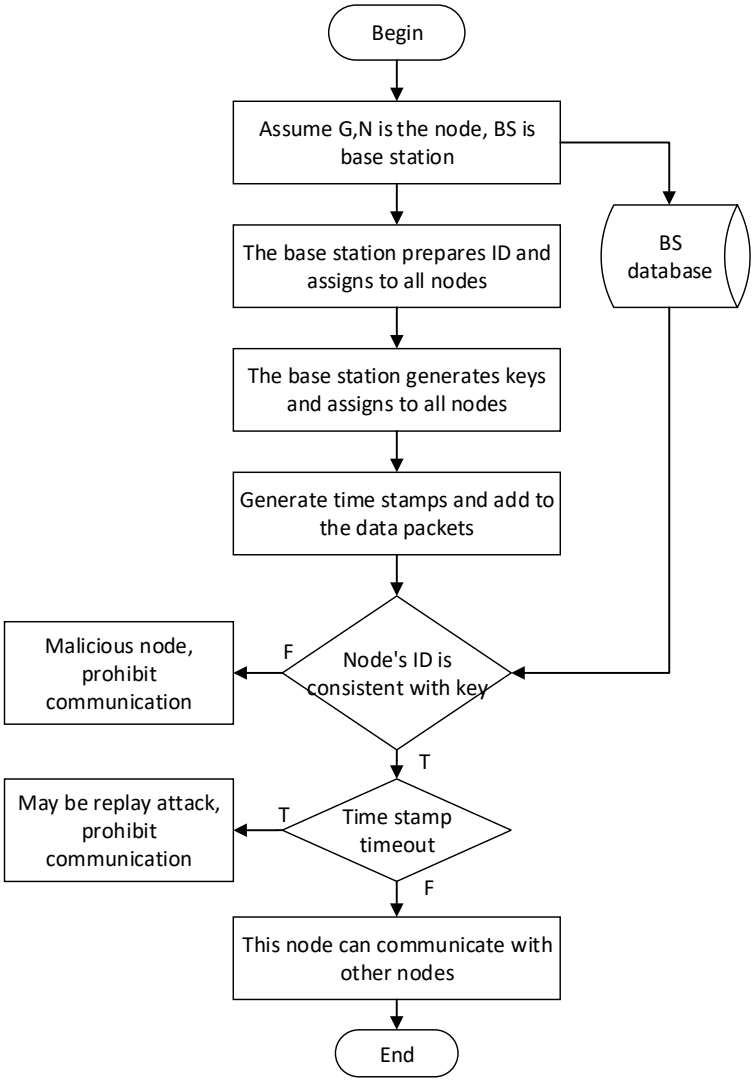

Figure 1. The Integrated System Model

3.2. Node ID Preparation

The base station generates the node's ID according to the node's equipment type, communication type, production company and so on. For example, if the first node is a laptop, then the ID created for it is "TALTA0001", as shown in Table 1. In "TALTA0001", the "TA" means that the company is "ToshibA"; "LT" means that the device is "LapTop"; "A" is the serial number added to the device according to the product

characteristics; "0001" is an automatically generated unique number. It carries out mod operations with 2 bit by bit and stores the results in the BS database. Similarly, if the second node is a mobile phone, then according to the relevant information, the ID created by this method is "SAMEA0002".

Table 1. The ID of a Laptop Node

Company name	Device type	Series	Auto generated number	Generated ID
ToshibA	LapTop	A	0001	TALTA0001

3.3. Dynamic Key Generation Algorithm

A dynamic number is generated by the KeyGEN method to generate the IMEI number, then the generated IMEI number and the node ID are combined together to generate the key.

```
KeyGEN()
{
        for (i = 1; i <= N; i++)
        {
                Vi = substr(Node-ID, 4);
                keyi = append(Vi, Node-ID + Vi);
                for (j=1; j<=length(Keyi); j++)
                        IMEIj = IMEIj ⊕2
        }
}
```

For example, the method of finding the key of Node1 is given:

IMEI = 278373612 ⊕2 = 010111010

Key(Node1) = 010111010TALTA010111010

The key is stored in the BS database for the verification of the node. The length of the key is 32 bits. If the length increases, it means series of the device is upgraded. Because the key is unique and the length is small, the submission and verification of the key requires less time, thereby reducing the workload of the base station and saving the resources.

3.4. Security Analysis of the Algorithm

When the node ID is generated, the hardware characteristics of the node itself are fully considered. The production company, equipment type and series are properly encoded, which combines an automatically generated number to generate an ID that contains a large number of character information. This increases the difficulty of forging ID, and enhances the security of the system.

The key is the combination of dynamically generated random number IMEI and node ID, and can be continuously updated, so it can effectively detect and prevent malicious behavior. Considering the limited energy of nodes in wireless sensor networks, our key length is limited to only 32, in order to reduce the computational amount of data and save energy. The key generation algorithm and the authentication algorithm are relatively simple, realizing the purpose of high efficiency and energy saving.

Replay attack is a kind of attack method which can deceive the system by sending duplicate data packets received by the host in a malicious or fraudulent way, and its main purpose is to destroy the correctness of identity authentication. Since encryption technology can not prevent this kind of attack, our system uses a time stamp technology in order to resist replay attacks. Upon sending the data, the time stamp information is added to the data packet, and the time stamp is authenticated when the packet reaches the

receiving end: If the time stamp timeout is detected, the system would consider it a replay attack packet and discard it. If there is a high possibility of replay attack in the environment, the time window of the receiving end will be reduced to enhance the detecting ability of replay attacks.

3.5 Secure Communication

The network G consists of N nodes, in which any node can communicate with other nodes in the network. As shown in Figure 2, S is the source node; D is the target node; node-1 to node-3 are the intermediate nodes between the source and destination. If the intermediate node's information exists in the BS database, the node can transmit data, otherwise the node is considered malicious and forbidden to transmit data.

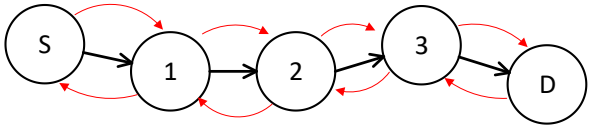

Figure 2. Paired Node Authentication

The overall functions of DRPA have been discussed above, and the algorithm can be written as follows:

```
DRPA()
{
        for (i = 1; i <= N; i++)
        {
                Node-ID = concat(CompanyName, DeviceType, Series, AutoNumber);
        }
        for (i=1; i<=N; i++)
        {
                Vi = substr(Node-ID, 4);
                keyi = append(Vi, Node-ID + Vi);
                for (j=1; j <= length(keyi); j++)
                {
                        IMEIj = IMEIj ⊕2;
                }
        }
        for (i = S; i <= D; i++)
        {
                if (Nodei == D)
                        stop;
                elseif (Nodei.ID, Nodei.Key.exists(BS-DB.record))
                        nodei+1.data = nodei.data;
        }
}
```

3.6. Simulation Settings

In order to study the efficiency of DRPA method, NS2 simulation method is used to verify the system based on the parameters of Table 2. The size of the network is 1500×1500, the numbers of nodes deployed in the simulation are 10, 20, 30, 40, 50, totally five rounds. The front end of the simulation is developed by using TCL language, and the protocol configuration uses C++.

Table 2. Simulation Parameters

Parameters	Value
Size	1000m×1000m
Speed	5—20m/s
Propagation model	Two ray ground reflection
Range	300m
Number of nodes	20—150
MAC protocol	802.11
Application	CBR, 100—500
Packet size	50
Simulation time	120s
Layout method	Random
Number of malicious nodes	6%

4. The Results and Discussion

The simulation results include the number of malicious activities before and after the deployment of DRPA scheme. At first, the visual interface of network topology is demonstrated, and in this interface, the DRPA algorithm identifies and detects malicious nodes by their behaviors.

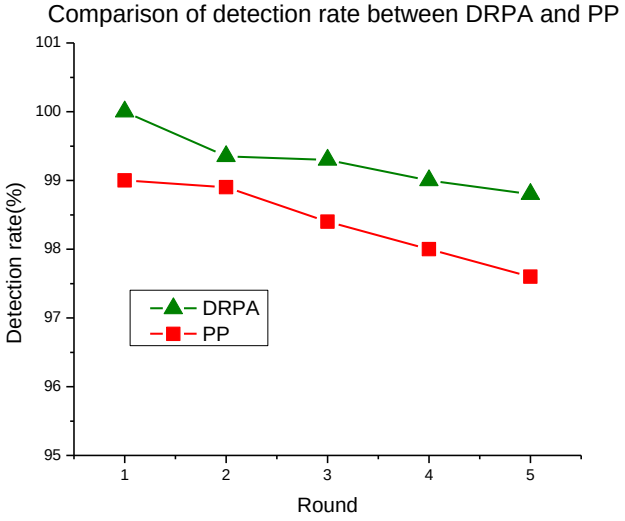

Figure 3. The Comparison of Detection Rate Between DRPA Algorithm and PP Algorithm

In order to detect malicious nodes, the DRPA algorithm verifies the ID and key of each node when data packets are sent or received. When a node is detected as a malicious

one, it will be blocked. Literature [14] presents an intrusion detection scheme of wireless sensor network based on projection pursuit algorithm, which is called PP algorithm. Figure 3 shows the comparison between DRPA algorithm and PP algorithm in terms of detection rate. By comparison, we can see that the DRPA algorithm has a higher detection rate than the PP algorithm.

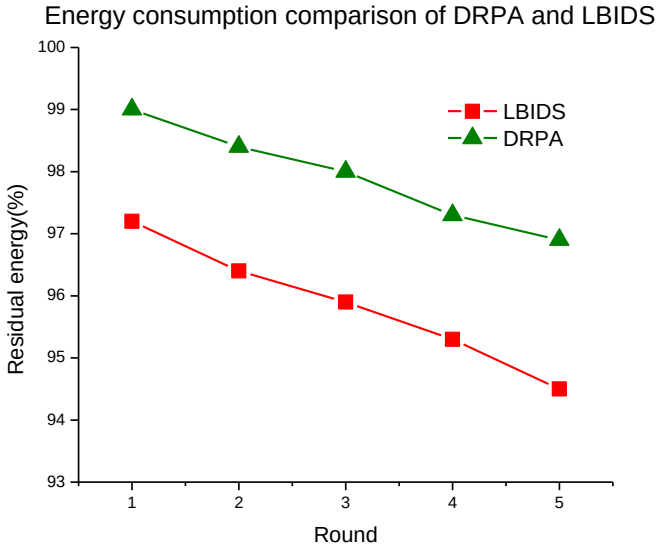

Figure 4. Comparison of Energy Consumption Between DRPA and LBIDS System

Figure 4 shows the remaining energy per round, and the numbers of nodes deployed per round are 10, 20, 30, 40, and 50 respectively. Compared with the LBIDS system, the DRPA system has a longer survival time. The reason is that the redundant node communications and data transmissions are avoided by the key comparison. If the node cannot submit a valid ID and key, it cannot send data, thus saves the limited energy. After 5 rounds, the remaining energy of the LBIDS system is 94.52%, while the remaining energy of the DRPA system is 96.93%, which indicates that the DRPA system is more energy saving.

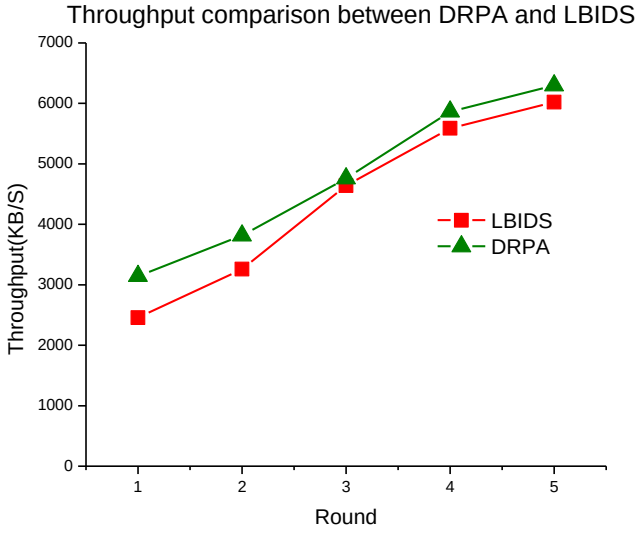

Figure 5. Comparison of Throughput Between DRPA and LBIDS System

The throughput of DRPA system is better than that of LBIDS system. A lot of malicious activities in the existing system destroy the successful transmission of the data. Figure 5 shows the throughput of each round. In the fifth round, the throughput of the LBIDS system is 6022KB/S and that of the DRPA system is 6297KB/S, reaching the conclusion that the DRPA system can achieve a higher throughput.

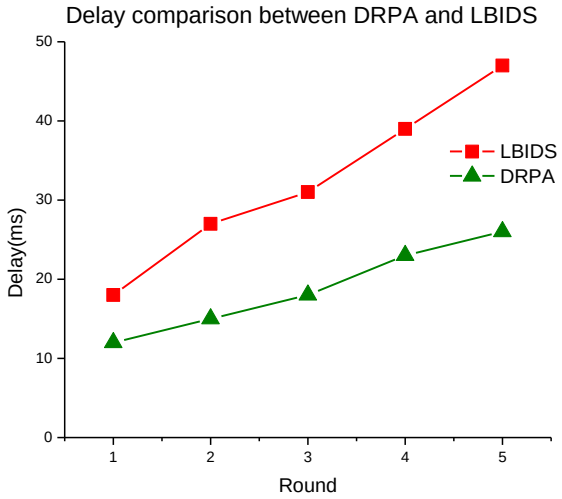

Figure 6. Comparison of Time Delay between DRPA and LBIDS System

The time to transfer a packet from the source node to the destination node is shown in Figure 6. By comparing the time delay before and after using the DRPA method, it is found that the system has lower time delay after DRPA. Figure 6 shows the delay of each round. In LBIDS system, the transmission time of each round is 17,27,31,39,48 ms. After the use of DRPA, the transmission time of each round is 12,15,17,23,26 ms. The numbers of nodes deployed in teach round are 10, 20, 30, 40, 50 respectively.

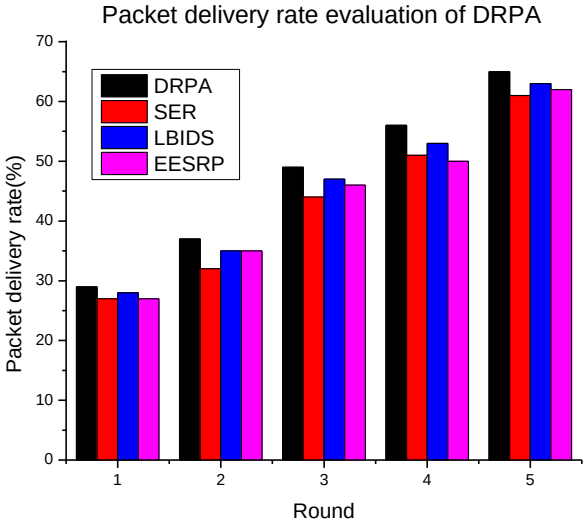

Figure 7. Packet Delivery Rate Evaluation of DRPA

In terms of packet delivery ratio (PDR), Figure 7 shows the comparison of DRPA and other popular routing protocols. The numbers of nodes in the five rounds are 10, 20, 30, 40, and 50 respectively. The PDRs of DRPA in five rounds are respectively 29%, 38%, 49%, 56% and 66%. The PDRs of SER protocol in five rounds are respectively 27%, 32%, 43%, 51% and 61%. The PDRs of LBIDS protocol in five rounds are

respectively 28%, 35%, 47%, 52% and 63%. The PDRs of EESRP protocol in five rounds are respectively 27%, 35%, 46%, 49% and 62%. By comparing with the several protocols, it is found that DRPA can get higher PDR.

5. Conclusions

Deriving from an existing LBIDS scheme, DRPA can realize mutual authentication between nodes. DRPA uses the unique ID generated by the special method of combining node type with node sequence number, so it can authenticate the nodes correctly and cannot be copied by malicious nodes. In order to improve the ability of resisting replay attacks, time stamp technology is applied to the system, therefore the security of the system will be greatly improved.

DRPA technology is particularly useful for WSN-based applications, and this method improves the quality of the network. The comparison of ID and key is the pretreatment method in the network, which can protect the network and make the network more reliable. Simulation results show that it is a common solution to prevent data from being taken by attackers. This method is also effective in large scale networks. DRPA technology can help the network achieve higher security without affecting network performance.

At present, there are some limitations in this technology, such as the limited extendibility of device types, and data level security, which are the future research focus.

References

[1] J. Xu, J. Wang, S. Xie, W. Chen and J. U. Kim, "Study on intrusion detection policy for wireless sensor networks", International Journal of Security & Its Applications, vol. 7, no. 1, (2013), pp. 1-6.
[2] Y. T. Li, Z. P. Xia and J. Xiong, "Study on Evaluation Method of Multi-layer Hybrid Intrusion Detection System", Computer Science, vol. 42, no. 6A, (2015), pp. 425-428.
[3] B. Wang, H. Qian, X. Sun, J. Shen and X. Xie, "A Secure Data Transmission Scheme Based on Information Hiding in Wireless Sensor Networks", International Journal of Security & Its Applications, vol. 9, no. 1, (2015), pp. 125-138.
[4] A. Ahmed，K. A. Bakar，M. I. Channa and A. W. Khan, "A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network", Mobile Networks & Applications, vol. 21, no. 2, (2016), pp. 272-285.
[5] M. C. Veettil, V. Sandhya and N. Niyas, "Authentication and Hybrid Security in Heterogeneous Wireless Sensor Network", International Journal of Advanced Research in Computer Science, vol. 6, no. 5, (2015), pp. 156-161.
[6] A. G. Tartakovsky, A. S. Polunchenko and G. Sokolov, "Efficient Computer Network Anomaly Detection by Changepoint Detection Methods", IEEE Journal of Selected Topics in Signal Processing, vol. 7, no. 1, (2013), pp. 4-11.
[7] Y. Wang, W. Fu and D. P. Agrawal, "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks", IEEE Transactions on Parallel & Distributed Systems, vol. 24, no. 2, (2013), pp.342-355.
[8] Y. W. Guan, T. Liu and G. Huang, "ELM-based Hybrid Intrusion Detection Scheme in Wireless Sensor Networks", Computer Engineering, vol. 41, no. 3, (2015), pp. 136-141.
[9] W. F. Li and X. W. Fu, "Survey on Invulnerability of Wireless Sensor Networks", Chinese Journal of Computers, vol. 38, no. 3, (2015), pp.625-647.
[10] G. P. Spathoulas and S. K. Katsikas, "Enhancing IDS performance through comprehensive alert post-processing", Computers & Security, vol. 37, no. 9, (2013), pp. 176-196.
[11] Y. Luo and W. Chen, "A Security Distributed Decision Fusion Method for the Wireless Sensor Network", Journal of Sichuan University(Natural Science Edition), vol. 52, no. 3, (2015), pp. 499-504.
[12] D. U. S. Rajkumar and R. Vayanaperumal, "A Leader Based Monitoring Approach for Sinkhole Attack in Wireless Sensor Network", Journal of Computer Science, vol. 9, no. 9, (2013), pp. 1106-1116.
[13] H. Imai, S. H. Shin and K. Kobara, "How to Establish Secure Channels for Wireless Communications", Iete Journal of Research, vol. 52, no. 2, (2015), pp. 229-238.
[14] X. Y. Ge, L. J. Wang and X. R. Guo, "Intrusion Detection Model for WSNs Based on Projection Pursuit", Transducer and Microsystem Technologies, vol. 34, no. 9, (2015), pp. 24-27.

Authors

Xiaolong Xu, born in 1977, he is now an experimenter of Experiment Teaching Center, Qufu Normal University. He obtained his bachelor's degree of computer science from Qufu Normal University in 1999, and master's degree of computer application technology from Qufu Normal University in 2006. He has published more than 15 papers. His major research interests include network security and wireless sensor network.

Author: Xiaolong Xu, male, Experiment Center of Qufu Normal University.
Tel: 13562396141
E-mail: xiaolongxu@foxmail.com
Address: Experiment Center of Qufu Normal University. No.80 of Yantai Road, Donggang District, Rizhao, Shandong province, China.
Zip code: 276826

