International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.181-190
http://dx.doi.org/10.14257/ijsia.2016.10.8.16

Multi-level detection and Warning Model for Bandwidth Consumption Attacks

Jincui Yang[1*], Fangjiao Zhang[2] and Wenbo Hu[3]

[1]*School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing, China;*
[2]*Institute of Computing Technology, Chinese Academy of Science Beijing, China;*
[3]*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China.*
jincuiyang@bupt.edu.cn

Abstract

Along with the development of IoT(Internet of Things) in industrial control field, more and more security issues are emerged, which cause great damage in the physical world. Under the background of IoT for industrial control, we propose a multi-level detection and warning model, the model can find the attacked node quickly and further effectively forecast data transmission situation of IoT. In addition to detecting the attacks accurately and effectively, the algorithm could give different levels of alarm according to network running situations. And then corresponding measures would be taken to guarantee network availability. An OMNeT++(Objective Modular Network Tested in C++) simulation is performed to validate correctness and practicability of the model at last. And the results verify that this model is feasible to a certain degree.

Keywords: *industrial control, bandwidth consumption attacks, multi-level, detection*

1. Introduction

IoT, as an important part in a new generation of information technology, acquires various needy information of objects or process required to be monitored or connected by information sensing devices in real time, combining with Internet to develop a huge network. It is also known as the third wave after computer and the Internet.

In response to the tide of integration of industrialization and information, IoT is applied to industrial control system and achieve intelligent identification, positioning, tracing, monitoring and managing objects and equipment, finally completing the incorporation of physical system into human society. However, IoT is a mixed network, and due to its openness and complexity, data may be hijacked, altered or blocked in transit.

In June, 2010, Stuxnet-the world's first network superweapon was detected, the virus specifically for industrial control systems [11-13]. Brought into the intranet by the infected U disk, it altered the commands sent to the PLC (Programmable Logic Controller) finally to change the rotational speed of the centrifuge. The centrifuge was disastrously damaged. Stuxnet virus had led to serious damage to Iran's industrial facilities, from which we could see along with intelligent system, efficient management and convenient control comes severe security challenge.

Low power consumption, low cost, distribution and self-organization would not lead to system crash even if some nodes are badly vandalized in wireless sensor networks. As an application of IoT, wireless sensor networks have vast development prospect in military, defense, environmental monitoring, health care, building monitoring, *etc*. For instance, they could replace workers and monitor the environment to remove dangerous situations

* Corresponding Author

ISSN: 1738-9976 IJSIA

and ensure staff security in such hazardous environment as coal, oil drilling and nuclear power plants.

However, because of the limit in computing, power and storage, wireless sensor networks are confronted with more security threats, such as DDoS (Distributed Denial of Service), Sinkhole, Sybil and Hello flood attacks. In the practice, it's significant to maintain the availability of the network. DDoS attacks, the events or behaviors to weaken or even destroy wireless sensor networks, are to make the network unavailable, not merely to obtain confidential data or privacy. Hardware failures, software bugs, resource depletion, environmental interference could cause a DDoS attack. The bandwidth consumption attack of DDoS attack is simple, and for an attacker, it does not require much safety knowledge to launch a new attack, which indicates that probability of attacks is bigger.

A multi-level detection and warning model for bandwidth consumption attacks in wireless sensor networks is researched in the article. Its aim is to detect the nodes attacked, and warnings are launched according to the degree of the attacks. Besides, some defensive measures are provided for repairing.

The article is organized as follows. In Section 2, we give background and related work on bandwidth consumption attacks in wireless sensor networks. Section 3 presents a scenario about the application of wireless sensor networks in industrial control field whereby requirement analysis on the model is made. In Section 4, we discuss the detection algorithm based on response time. Multi-level warning mechanism is described in Section 5. In Section 6, through the simulation experiments, it checks the validity of the model. We summarize our work in Section 7.

2. Related Works

Wireless sensor network is peer network composed of sensor nodes without any network infrastructure, where each sensor node is required to be independent and flexible to be self-organizing. Each node could join or leave the network at any time, so the topology changes frequently. Node's coverage is small and nodes have to communicate with each other through other nodes' multi-hop forwarding. All the above determine that wireless sensor networks suffer the DDoS easily apart from data leakage, data tampering, replay attacks and other threats [1].

In a simple and natural way from quite a lot of agents with enough resources, packets, including TCP (Transmission Control Protocol), UDP(User Datagram Protocol) and ICMP (Internet Control Message Protocol), flow into the target at the same time, aiming to deplete its bandwidth severely. Yu lin *et. al.,* in literature [2] presented a method for detecting DoS and also response measures. With ARMA (2,1) model for real-time traffic prediction, attacked nodes were identified immediately. Intelligent agents were used to respond to attacks to prolong the life of the entire network. Han *et. al.,* [3] designed a DDos detection scheme-MPDD, based on traffic prediction using Markov linear prediction model for wireless sensor networks, in which each node detected the attack in accordance with traffic predicted. In literature [7], Jian Yin, *etc*. proposed a secure routing protocol-SecRout to detect attacked nodes in the network. Besides, Issa Khalilel put forward a local monitoring model for detecting and controlling attacks using one node listening to its neighboring nodes in [8].

Most of the existing detection algorithms are considered from the view of network traffic, not nodes' limited power. And current warning against bandwidth consumption attacks is only two states: yes or no, without different levels of warning being taken into account. Measures corresponding to its level are vital for saving manpower and money and avoiding associated economic loss.

Combined with the characteristics of wireless sensor networks, we propose a new detection algorithm based on packet's response time for the bandwidth consumption

attacks. And the warning is divided into different levels on the response time.

3. Requirement Analysis and Model Framework

The application of wireless sensor networks in industrial control system is depicted in Figure 1. Wireless sensor networks are connected to industrial core network by industrial access network. Nodes in the network reliably acquire surrounding information (devices, environment *et. al.,*) in real-time. Multi-service application platforms for various applications are built in application layer, which provide a fine-grained management and control based on the data sensed [4].

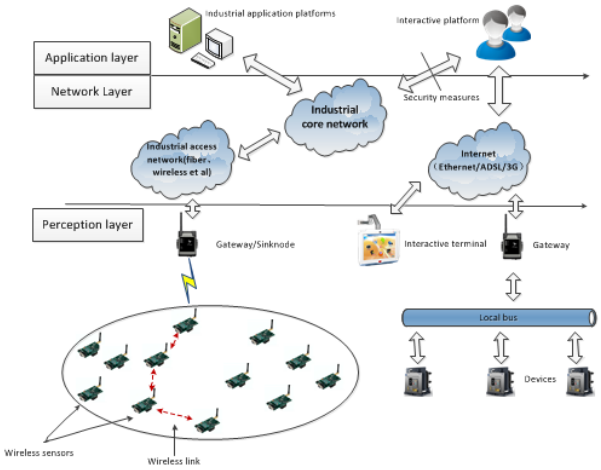


Figure 1. Wireless Sensor Networks in Industrial Control System

Wireless sensor networks make it possible to measure critical industrial parameters that were difficult in the traditional. They also optimize the control process and improve quality of products, ultimately decreasing energy consumption and reducing maintenance and operation costs [5]. There is a great chance of Bandwidth consumption attacks in wireless sensor networks. Thus it is quite necessary to research detection algorithm and warning mechanism for it.

To complete the detection and multi-level warning once attacks occur, the multi-level detection and warning model must have the following functions: be able to compute the response time of nodes in networks; determine whether the node is attacked or not based on the response time; launch different levels of warning; adopt corresponding measures following the warning level to prevent the influence of attacks. In order to achieve these aspects, we introduce a monitoring device M in wireless sensor networks, as shown in Figure 2. And the logic diagram of M is described in Figure 3.

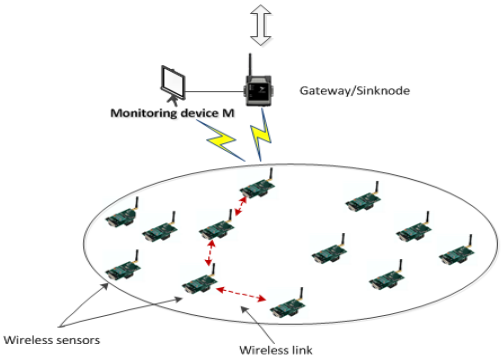


Figure 2. Monitoring Device M in Wireless Sensor Networks

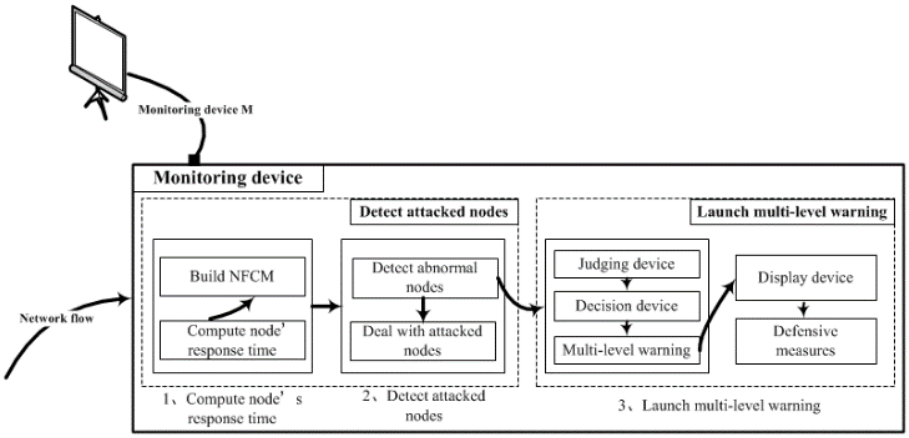


Figure 3. Logic Program of Monitoring Device M

4. Bandwidth Consumption Attacks Detection Algorithm Based on RT

Several concepts are introduced as follows before the detection algorithm.

Definition 4.1.:

Response Time (RT): The time counting from the sending node putting message in the physical channel until receiving the response again.

Definition 4.2.:

Response Time per Hop (RTH): Similar to RT, time starting from one node receiving the packet till the next neighboring node receiving it again.

Definition 4.3.:

Node Forward Cycle (NFC): The number of nodes that a packet passes from the sender to the receiver, including the receiver, which is the hops. And the sender is the monitoring device M. For example, the node's NFC is 2, which means the receiver is two jumps from M and one intermediate node exists.

Definition 4.4.:

Node Forward Cycle Matrix(NFCM)- Drawn from Definition, each node in the network has its NFC and many nodes may have the same NFCs, thus forming the NFCM as in Table 1.

Table 1. Node Forward Cycle Matrix (NFCM)

Node / NFC	1	2	3	……	N-1	N
1	√	√				
2						
……					……	
S-1			√			√
S					√	

(Notice: √ where is the nodes' RT; N is the number of nodes; S is the maximum of NFC.)

The algorithm is: The monitoring device M sends request packets to nodes in the wireless sensor networks at a time interval-Tm, which not only returns the response time from M to the receiver, but also calculates the receiver's NFC, to form NFCM. Obviously, NFCM is changing over time. Then, the M would check RTs in NFCM to verify whether

the node is attacked by comparing. And depending on the damage suffered, different levels of alarms would be launched and certain measures would be taken.

4.1. RTH Statistics

In the fields of production and scientific experiments, most random variables abide by normal distribution. Central limit theorem explains the conditions that normal distribution is produced, that is: if a random variable is decided by a lot of tiny and independent random factors , each factor works little and even and none of them plays a leading role, we could say it follows a normal distribution[6]. Therefore, the repeated measurements of RTH satisfy it and follow the normal distribution, depicted in Figure 4.

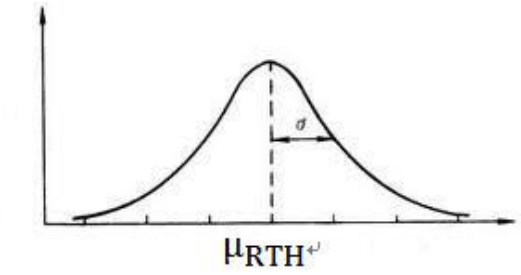


Figure 4. Normal Distribution of RTH

Within the certain communication range, RTH may vary due to the load, environment and other independent factors, absolutely around certain value. We use the normal distribution to describe RTH, denoted by RTH~N(), that is :

$$f(RTH) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(RTH-\mu_{RTH})^2}{2\sigma^2}} \quad (4\text{-}1)$$

$$RTH \in [\mu_{RTH} - A\sigma,\ \mu_{RTH} + A\sigma] \quad (4\text{-}2)$$

RT of node n(n ∈[1, N])in layer s(s∈[1, S]) should be :

$$RT \in 2^* s^* RTH = 2^* s^* [\mu\_RTH - A\sigma, \mu\_RTH + A\sigma] \quad (4\text{-}3)$$

A relies on the specific applications. If strict, A is small, and on the contrary, it's big.

4.2. NFCM Forming

Each node in wireless sensor networks has its own NFC. At the early stage, monitoring device M broadcast packets to the working nodes for nodes' information, including number, location and others. And similarly, the node that receives the broadcast would respond to the request packet, together with the hops. Ultimately, M would calculate the maximum S and develop initial NFCM. Then the M repeats it at regular interval-Tm and thus, the NFCM would automatically updated based on the newer RT and NFC.

4.3. Abnormal Nodes Detection

Comparison and statistical approach is used to detect the attacked nodes. RT of node n is noted as RT (n) described in (4-4), while RT computed by the algorithm is RT(n)'. If the formula (4-5) is satisfied, the node would be judged as abnormal.

$$RT(n) \in (0,\ 2^*s^*RTH+\Delta t] \quad (4\text{-}4)$$

$$RT(n)' \in RT(n) \quad (4\text{-}5)$$

The direct use of formula (4-5) would produce a higher rate of false rate, so formula 4-6 is introduced as follows:

$$count(n) \geq k \quad (4\text{-}6)$$

Count(n) means the number of the node suspected to be malicious. Only the node was suspicious for k times continuously would it be justified to be attacked[7].

4.4. Attacked Nodes Processing

The attacked nodes would be isolated for some time T_{iso} that is set to init early. When isolated, nodes are dormant. After the time, the nodes would be under heavy surveillance. If detected malicious once again, the nodes are re-isolated and the isolation time change as in (4-7).

$$T_{iso}=\min(T_{iso\_max}, init*\mu^{i}) \quad (4\text{-}7)$$

T_{iso_max} is the maximum isolated time. μ, a regulator, is used to denote how fast the time increases and obviously, μ>1. Besides, i represents the number of times nodes attacked.

5. Multi-level Warning for Bandwidth Consumption Attacks

Warning or early-warning refers to that an alarm would be launched earlier when something bad happens, which is estimated based on a priori or the past. The extent and scope of the harm also is predicted following some proposed feasible precautions.

Multi-level warning for bandwidth consumption attacks in the article uses it in information security field, that is network behaviors or others could be monitored, evaluated for final alarming.

Modeled after warning mechanism in TBT (Technical Barriers to Trade)[8], warning for bandwidth consumption attacks according to their influence of the network is divided into four levels:

- **Blue(0) level** (no warning): The network could operate normally.
- **Yellow(1) level** (mild warning): There is a little influence on the operation of the network, which is smaller and shorter.
- **Orange(2) level** (moderate warning): Between Yellow and Red level, the network is affected to some extent.
- **Red(3) level** (serious warning): The attacks are bigger and longer and the network is damaged severely.

For convenience, we only consider the unique indicator-threatening and see the alarm in terms of attack intensityy- δ , which is the ratio of attacked nodes to all here.

$$\delta = \frac{N_{attacked}}{N} \quad (4\text{-}8)$$

Table 2. Risk Level of Warning

Risk	0	1	2	3
δ	≤ α	≤ β	≤ γ	> γ

α, β, γ are the specific value of δ. For different levels of warning, corresponding measures would be taken, such as isolating the nodes and adopting the redundant one.

6. Simulations and Analysis

The simulations are performed to prove the feasibility and performance of detection algorithm mentioned. We use OMNeT++ as the simulation tool. By simulating bandwidth consumption attacks, the numerical analysis tool, Matlab, is used to analyze response time of nodes gathered in wireless sensor networks, to finally verify the mathematical model we raise effectively.

6.1. Simulation Description

Figure 5 is the topology we used in our experiments. The network consisting of 50 nodes (Node [0]~Node[49]), scattered randomly in 500m500m space. And Node [2] is the monitoring device.

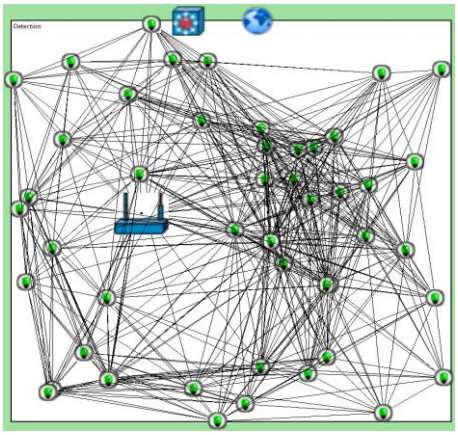


Figure 5. Network Topology

6.2. Analysis on Simulation Results

After initializing the network, data gathered without any attacks would be used to verify that RTH of nodes in the network follows normal distribution we mentioned above. By extending the time packet processed to simulate bandwidth consumption attacks, the performance of the algorithm could be checked.

1) The distribution of RTH

In Figure 6, the red curve shows the RTH change of all nodes in the wireless sensor networks, which apparently obeys the normal distribution. And μ_{RTH}=0.496926s, σ= 0.201525 following RTH~N(0.496926, 0.040612325625). So it is feasible for the use of normal distribution to represent the RTH in the network.

$$f(RTH) = \frac{1}{0.201525\sqrt{2\pi}} e^{-\frac{(RTH-0.496926)^2}{0.08122465125}} \quad (4\text{-}9)$$

Besides, the blue curve in Figure 4 describes the RTH of node [0]. And we also notice that the blue curve (RTH[0]~N(0.498013, 0.041932800625)) almost overlaps the red one, which means the RTH for every node is also in normal distribution.

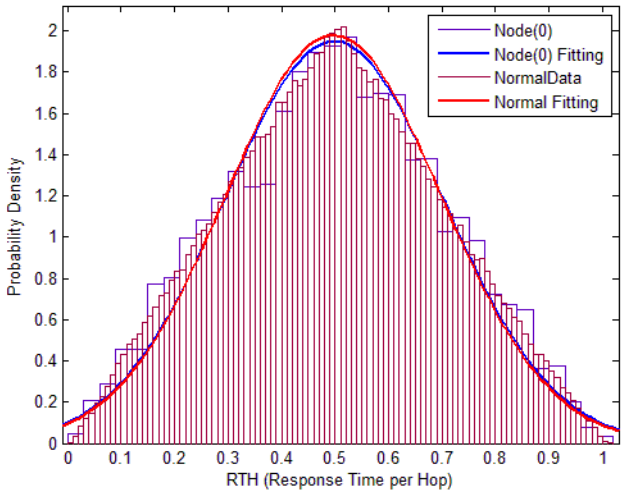


Figure 6. The Normal Distribution of RTH

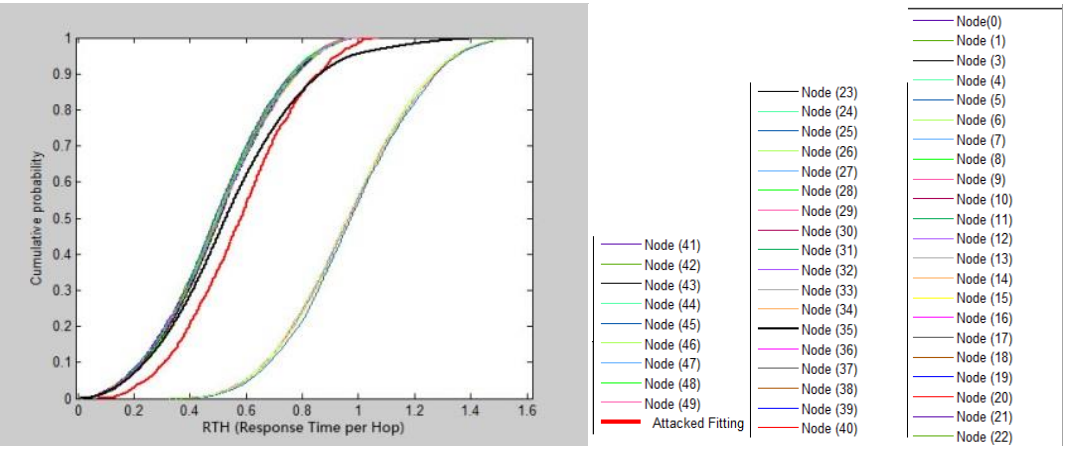


Figure 7. Cumulative Probability Plots of All Nodes in the Network

2) Performance Analysis

In experiments, we assume that nodes, including Node [7], Node[9], Node[15], Node[25], Node[35], Node[46], are attacked, and A=0.5, Δt=0.1. As described previously, the RTH of nodes should be:

$$RTH \in [\mu_{RTH} - A\sigma,\ \mu_{RTH} + A\sigma] = [\,0.3961635\ ,0.5976885]$$

Figure 7 shows the cumulative probability plots (CDF) of all nodes in the wireless sensor network. From where, we are able to see that the right part deviates from the main. And RTH of the right part is obviously longer, which caused by the attack. The result is that Node [35] is not detected. Comparing the parameters of Node [9] and Node[35] before and after attack, the change of Node[35] is not so evident. At the same time, we should also realize the significance of threshold, the key to the detection algorithm.

Table 3. Parameters change of Node [35] and Node [9]

Nodes	Node[35]		Node[9]	
	μ_{RTH}	σ	μ_{RTH}	σ
Before attack	0.502816	0.200847	0.493269	0.201853
After attack	0.579138	0.203243	0.967031	0.228459

7. Conclusion and Future Works

In the paper, the main contribution is to propose a multi-level detection and warning model for bandwidth consumption attacks. In the model, a new concept-RTH is raised and normal distribution is adopted to describe it. Then, multi-level mechanism is also applied in the warning according to the extent of damage. And the simulation also proves the certain feasibility of the model.

In our future work, we would perfect the model raised above continuously and extensively, where there are still many problems existing, such as the best position of the monitoring device, specification of warning mechanism and practical application in industrial control system.

Acknowledgments

This paper is supported by the Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education

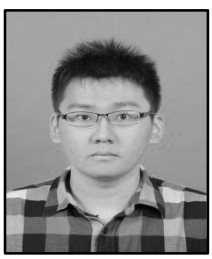
References

[1] M. Zi-heng and D. Xin-wen, "Dos Detection Scheme Based on Voting Mechanism In Wireless Sensor Networks", Modern Computer, **(2010)** July.
[2] Y. Lin and Y. Shaohua, "A Method to Detect Dos Attack in Wireless Sensor Networks", Computer Era, **(2009)** March.
[3] H. Zhi-jie, Z. Wei-wei and C. Zhi-guo, "A Markov-Based Intrution Detection Scheme for Wireless Sensor Networks", Computer engineering & science, vol. 32, no. 9, **(2010)**.
[4] Y. Jin-cui, F. Bin-xing, Z. Li-dong and Z. Fang-jiao, "Research towards IoT-oriented Universal Control System Security Model", Journal on Communications, vol. 33, no. 11, **(2012)**.
[5] H. Qi, "Development and Application of Wireless Sensor Networks in Industrial Control Area", Automation in Petro-Chemical Industry, **(2010)** March.
[6] W. Zhaohong, X. Mengqiang, L. Yan and L. Xin, "The Forcasting Algorithm for Cloud Model of Similar Normal Distribution Data", Computer Applications and Software, **(2009)** September.
[7] C. Bo, "Detection and Mitigation of Abuse Attack for Large Scale Network. Harbin Institute of Technology", Dissertation for the Doctoral Degree in Engineering, **(2007)**.
[8] H. Xin-rong, "Accelerating the establishment of Warning in Technical Barriers to Trade(TBT)", Sci/tech Information Development & Economy, **(2005)** August.
[9] J. Yin and S. Madria, "SecRout: A Secure Routing Protocol for Sensor Networks[C]", Proceedings of the 20th International Conference on Advanced Information Networking and Applications. Vienna, Austria, **(2006)** Apr. 18-20, pp. 393-398.
[10] I. Khalil, S. Bagchi and C. Nina-Rotaru, "DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks[C]", Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks. Athens Greece, **(2005)** Sept. 5-9, pp. 89-100.
[11] Falliere N., Murchu O. L. and Chien E., "W32. Stuxnet Dossier[R]", Symantec Security Response, **(2011)**.
[12] Matrosov A., Rodionov E. and Harley D., "Stuxnet Under the Microscope[R]", ESET.
[13] Larimer J., "An inside look at Stuxnet[R]", IBM.

Authors

Jincui Yang, She received her PhD (2013) in computer science and technology from Beijing University of Posts and Telecommunications. Now she is a lecturer of software engineering at Software Engineering Department, Beijing University of Posts and Telecommunications. Her current research interests include different aspects of Software Engineering, Trustworthiness & The Internet of Things.

Fangjiao Zhang, She received his Bachelor degree (2014) from Beijing University of Posts and Telecommunications. Now she is an engineer of Institute of Computing Technology, Chinese Academy of Science, research in security of Internet of Things and Industrial Control.



Wenbo Hu, He is a Ph.D. student of Information and Communication Engineering at School of Information and Communication Engineering, BUPT. His current research focuses on Software-Defined Network and Future Network Architecture.