A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network

Article *in* Journal of Electrical and Computer Engineering · June 2014

DOI: 10.1155/2014/240217

CITATIONS
46

READS
615

5 authors, including:

Ping yi
Shanghai Jiao Tong University
113 PUBLICATIONS **1,227** CITATIONS
SEE PROFILE

Yue Wu
Shanghai Jiao Tong University
53 PUBLICATIONS **292** CITATIONS
SEE PROFILE

Li Pan
Shanghai Jiao Tong University
35 PUBLICATIONS **210** CITATIONS
SEE PROFILE

Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2014, Article ID 240217, 8 pages
http://dx.doi.org/10.1155/2014/240217

Research Article

A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network

Wenchao Li, Ping Yi, Yue Wu, Li Pan, and Jianhua Li

School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Correspondence should be addressed to Ping Yi; yiping@sjtu.edu.cn

Received 18 March 2014; Accepted 17 June 2014; Published 30 June 2014

Academic Editor: Xia Zhang

The Internet of Things has broad application in military field, commerce, environmental monitoring, and many other fields. However, the open nature of the information media and the poor deployment environment have brought great risks to the security of wireless sensor networks, seriously restricting the application of wireless sensor network. Internet of Things composed of wireless sensor network faces security threats mainly from Dos attack, replay attack, integrity attack, false routing information attack, and flooding attack. In this paper, we proposed a new intrusion detection system based on K-nearest neighbor (K-nearest neighbor, referred to as KNN below) classification algorithm in wireless sensor network. This system can separate abnormal nodes from normal nodes by observing their abnormal behaviors, and we analyse parameter selection and error rate of the intrusion detection system. The paper elaborates on the design and implementation of the detection system. This system has achieved efficient, rapid intrusion detection by improving the wireless ad hoc on-demand distance vector routing protocol (Ad hoc On-Demand Distance the Vector Routing, AODV). Finally, the test results show that: the system has high detection accuracy and speed, in accordance with the requirement of wireless sensor network intrusion detection.

1. Introduction

Internet of Things refers to the network which combines various sensing devices, such as radio frequency identification (RFID) devices, infrared sensors, global positioning systems, laser scanners, and other various devices with the Internet. This paper focuses on the security of Internet of Things composed of wireless sensor networks (WSN). With the rapid development of microelectronic technology, computer technology, and wireless communication technology, the Internet of Things has broad application prospects in military field, commerce, environmental monitoring, and many other fields. However, the open nature of the information media and the poor deployment environment have brought great risks to the security of wireless sensor network, seriously restricting the application of wireless sensor network [1]. Internet of Things faces security threats mainly from DoS attack [2], replay attack, integrity attack, false routing information attack, and flooding attack.

In this paper, firstly we propose a new intrusion detection system based on KNN classification algorithm in wireless sensor network. This system separates abnormal nodes from normal nodes by observing their abnormal behaviors, and we analyse parameter selection and error rate of the intrusion detection system based on KNN classification algorithm [3]. The paper elaborates on the design and implementation of the detection system. This system makes use of the GAINZ Zigbee nodes designed by Integrated Circuit Co., Ltd., Ningbo Branch. The nodes use UC Berkeley TinyOS operating system. By improving the wireless ad hoc on-demand distance vector routing protocol (Ad hoc On-Demand Distance the Vector Routing, AODV), the intrusion detection system can achieve efficient, rapid intrusion detection. Finally, the test results show that the system has high detection accuracy and speed, in accordance with the requirement of wireless sensor network intrusion detection.

The contributions of this paper are as follows.

(1) We have identified and presented a new intrusion detection system based on KNN classification algorithm in wireless sensor network. It separates abnormal nodes from normal nodes by observing their abnormal behaviors.

(2) We present the design and implementation of the detection system. By improving the wireless ad hoc on-demand plane distance vector routing protocol (Ad hoc On-Demand Distance the Vector Routing, AODV), the intrusion detection system can achieve efficient, rapid intrusion detection.

(3) The test results show that the system has high detection accuracy and speed, in accordance with the requirement of wireless sensor network intrusion detection.

The remainder of this paper is structured as follows. Section 2 introduces a new intrusion detection system based on KNN in wireless sensor network. In Section 3, we describe the design and implementation of the detection system, presenting simulation experiments. Section 4 briefly discusses related work. Section 5 concludes the paper.

2. The Intrusion Detection Algorithm Based on KNN

Related studies have already raised many intrusion detection models. According to the method of analysis, these models can be divided into two categories: feature-based intrusion detection model and anomaly-based intrusion detection model. Related researches have proposed some feature-based intrusion detection systems, but there are some problems in extracting and analyzing the features. There are also some related researches having proposed anomaly-based intrusion detection systems. Through statistical analysis of the data, anomaly-based intrusion detection systems can identify the anomalistic data which deviate from the mean value seriously. Data mining technology can effectively mine the regular pattern of the data; thus, it can be applied to intrusion detection on the Internet of Things.

In this paper, we use data mining technology to design and implement the intrusion detection system. The system has three advantages: (1) the value of K for mining has little effect on the results; (2) the cutoff value used to determine the abnormal node is easy to determine; (3) the algorithm is fast and efficient.

2.1. Overview of K-Nearest Neighbor (KNN) Classification Algorithm. K-nearest neighbor (KNN) classification algorithm is a data mining algorithm which is theoretically mature with low complexity. The basic idea is that, in a sample space, if most of its K nearest neighbor samples belong to a category, then the sample belongs to the same category. The nearest neighbor refers to the single or multidimensional feature vector that is used to describe the sample on the closest, and the closest criteria can be the Euclidean distance of the feature vector.

In the intrusion detection algorithm, we use a n-dimensional vector to represent nodes, such as $a1, a2, \ldots, an$. These dimensions can be as follows: the routing message number can be sent in a period of time, the number of nodes with different destinations in the sending routing packets, the number of nodes with the same source node in the receiving routing packets, and so on. In general, the node of the same type has the same characteristics. Thus the abnormal nodes will be distinguished. As is shown in Figure 1.

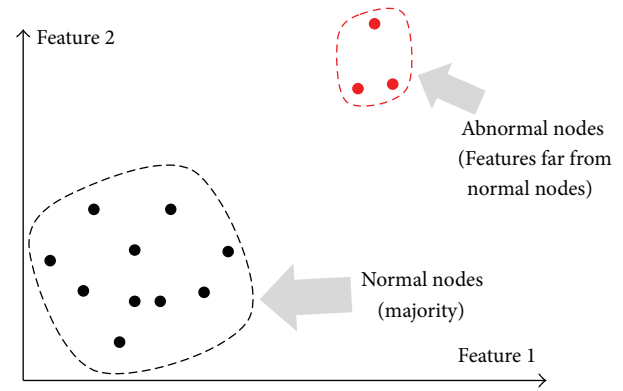

Figure 1: The schematic diagram of KNN intrusion detection algorithm.

Wireless sensor network intrusion detection algorithm based on KNN classification algorithm (hereinafter referred to as "KNN") requires two parameters: K value and the cutoff value. K value refers to the number of most adjacent nodes. Cutoff value refers to the threshold used for the judgment of the abnormal nodes. In order to describe the process of this algorithm, we have the following definitions: (1) the feature vector describing the node i is $ai, bi, \ldots$, a total of n; (2) the assemblage of all nodes in the network (including abnormal nodes and normal nodes) is NS; (3) the Euclidean distance of two different nodes i and j is eudis(i, j); (4) the K-distance function of node i is the value got by the summation of all the K most adjacent nodes' Euclidean distance, divided by K.

2.2. The Application of KNN Algorithm in terms of Flooding Attack. In this section, we describe the application of KNN algorithm in terms of flooding attack. We first describe the process of flooding attack. Flooding attack [2] can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV [4] and DSR [5]. The intruder broadcasts mass useless route request packets or sends a lot of useless DATA packets to exhaust the communication bandwidth and node resource so that the valid communication cannot be kept.

In KNN, the appropriate K value is a major factor that affects the detection effectiveness and cost, while cutoff value directly affects the detection error rate. The KNN detection algorithm uses the feature where abnormal nodes send RREQ messages more frequently than normal nodes in the flooding attack. By comparing the frequency to send RREQ messages of each node in the network, we can find the abnormal nodes. The feature vector describing the node is the frequency of RREQ messages.

Here we will discuss how to choose an appropriate K value and the cutoff value. We have the following assumptions and definitions of the KNN mining model: (1) the number of normal nodes in the network is $m1$ and the number of abnormal nodes $m2$, and $m1 > m2$. The number of all nodes in the network (including abnormal nodes and normal

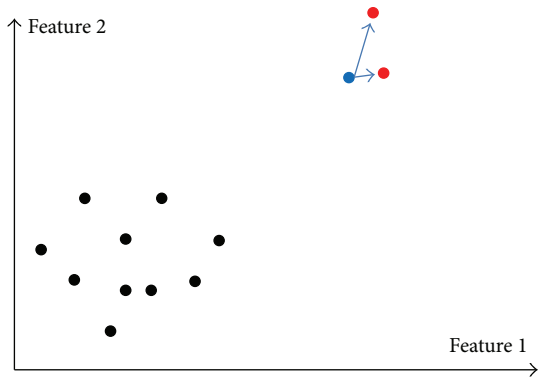

Figure 2: The effect of K value on abnormal node's K-distance function ($K = 2 < m2$).

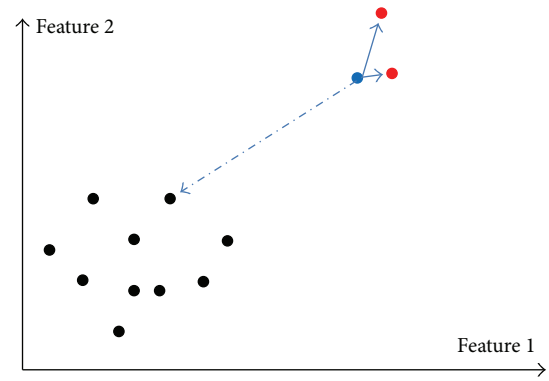

Figure 3: The effect of K value on abnormal node's K-distance function ($K = m2 = 3$).

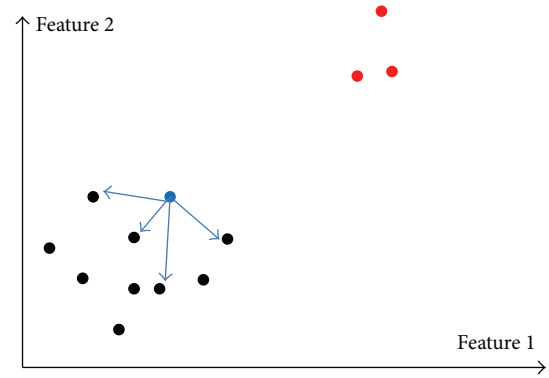

Figure 4: The effect of K value on normal node's K-distance function ($K = 4 < m1$).

nodes) is card (NS) $= m1 + m2$. Detection nodes in the network know the value of $m1$ and the general scope or the upper limit of $m2$. We set the upper limit of $m2$ to M. (2) An appropriate K value is the value that makes the K-distance function of abnormal nodes as large as possible, while making the K-distance function of normal nodes as small as possible.

KNN detection algorithm identifies abnormal nodes by comparing the K-distance function and cutoff value of each node. And K value can affect the result of K-distance function. We will discuss how K value affects the result of K-distance function of abnormal nodes and normal nodes and then get the reasonable range of K value.

(1) Analysis on How K Value Affects the K-Distance Function of Abnormal Nodes. When $K < m2$, as is shown in Figure 2, the abnormal node number $m2$ is 3 (including one blue node and two red nodes), and the K value is set to 2. We need to calculate K-distance function of the blue node. The nearest K neighbor nodes of the blue node are two red nodes pointed by the arrowhead. As the distance between the blue node and two red nodes is small, the K-distance function of the blue node is small. An appropriate K value is the value that makes the K-distance function of abnormal nodes as large as possible; thus, the K value is not appropriate.

When $K \geqslant m2$, as is shown in Figure 3, the abnormal node number $m2$ is 3 (including one blue node and two red nodes), and the K value is set to 3. We need to calculate K-distance function of the blue node. The nearest K neighbor nodes of the blue node include two red nodes and one normal red node. As the distance between the blue node and the normal red node is far larger than that of the blue node and the two red nodes, the K-distance function of the blue node is larger. Thus, the K value is appropriate.

Therefore, when we compute and analyse the K-distance function of abnormal nodes, the K value should be greater than or equal to $m2$.

(2) Analysis on How K Value Affects the K-Distance Function of Normal Nodes. When $K < m1$, as is shown in Figure 4, the K value is set to 4, the normal node number $m1$ is larger than the K value, and the blue node is a normal node. We need to calculate K-distance function of the blue node. The nearest K neighbor nodes of the blue node are all normal nodes. As the distance between the blue node and normal nodes is small, the K-distance function of the blue node is small. An appropriate K value is the value that makes the K-distance function of normal nodes as small as possible; thus, the K value is appropriate.

When $K \geqslant m1$, as is shown in Figure 5, the K value is larger than normal node number $m1$, and the blue node is a normal node. We need to calculate K-distance function of the blue node. The nearest K neighbor nodes of the blue node include all the red normal nodes and a red abnormal node. As the distance between the blue node and the abnormal red node is far larger than that of the blue node and the red normal nodes, the K-distance function of the blue node is large. Thus, the K value is not appropriate.

Therefore, when we compute and analyse the K-distance function of normal nodes, the K value should be less than $m1$.

In summary, since the detection nodes usually do not know the specific number of abnormal nodes, we can use M (the upper limit of $m2$) to determine the range of K value, and the appropriate range of K value should be $[M, m1)$.

Cutoff value directly affects the detection effect. The appropriate cutoff value should make the error rate of detection algorithm as low as possible. Due to the characteristics of wireless sensor network, we are unable to give a single, accurate communication model of it at present. For the

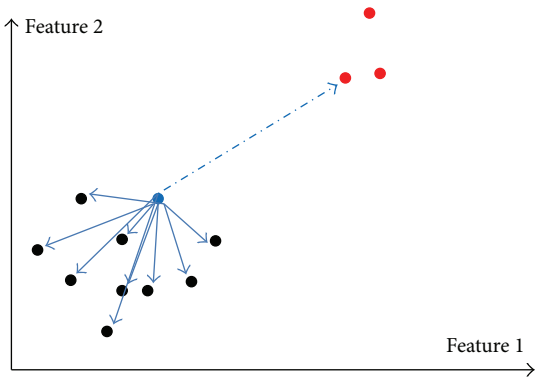

Figure 5: The effect of K value on normal node's K-distance function ($K = m1$).

unknown distribution model of the network, we cannot get the best cutoff value through the Bayes Decision of Minimum Error Ratio. Nevertheless, it is certain that we can determine the range of an appropriate cutoff value through observation and statistics of the network.

3. Evaluation

In this section, we introduce the simulation setup, describe the simulation results, and discuss the reason behind the simulation results.

3.1. System Implement. To study the performance of the intrusion detection system, we have implemented the intrusion detection system. The hardware platform includes GAINZ wireless sensor nodes and terminal equipment equipped with wired network card. GAINZ wireless sensor nodes are produced by Ningbo Zhongke integrated circuit Co., Ltd., and they are used to acquire network traffic and broadcast redlist. Terminal equipment is used to detect control system, analyze network traffic, judge the abnormal nodes, and respond to attacks. The software platform includes a serial communication assistant, the TinyOS operating system, and the AVRStudio integrated development environment. The serial communication assistant is used to exchange the control information message with users.

The intrusion detection system includes the following modules: wireless network interface module, data storage module, analysis and judgment module, and intrusion response module. The wireless network interface module is implemented by GAINZ wireless sensor nodes. The data storage module receives data from the wireless network interface module, obtaining statistical information, storing the information into the data domain to be read by the analysis and judgment module. The analysis and judgment module reads the test parameters and the data from the data storage module to analyze and make a judgment, keeping the intrusion response module informed of abnormal nodes. The intrusion response module adds abnormal nodes to the redlist and submits the redlist to the wireless network interface module. A redlist recording the abnormal nodes will be

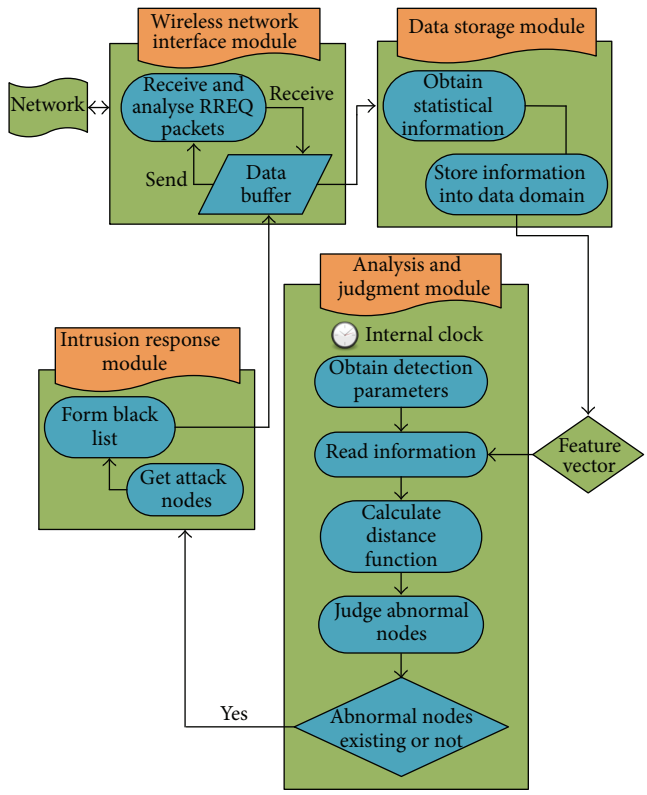

Figure 6: The schematic diagram of KNN intrusion detection algorithm.

broadcasted in the network; then, all the normal nodes will no longer receive or forward RREQ messages from the abnormal nodes. At the same time, the redlist will be forwarded to other nodes to realize flooding attack response. The system structure and module function are shown in Figure 6.

3.2. System Test Solution. Considering the feasibility and effectiveness, the test solution of this system is realized with wireless sensor network. Wireless sensor nodes used in this system test solution are GAINZ nodes designed by Ningbo Zhongke integrated circuit Co., Ltd., using Zigbee technology, compatible with 2.4 GHz wireless sensor nodes. The nodes use TinyOs operating system, and the routing layer uses ad hoc on-demand distance vector routing protocol (AODV).

The network test model is composed of a detection node, several common sensor nodes, and several attacking sensor nodes. The network test model is shown in Figure 7. The detecting node is composed of a control computer and a sensor node, receiving messages from all the other sensor nodes. It works as the core module of the system, responsible for collecting and detecting network data, providing alarm information and making a response. Common sensor nodes are responsible for the establishment of the test network, using the AODV protocol to transmit data. Attacking sensor nodes start flooding attack, broadcasting a large number of RREQ packets to the network, increasing the network load, and consuming resources of other nodes. The dotted line

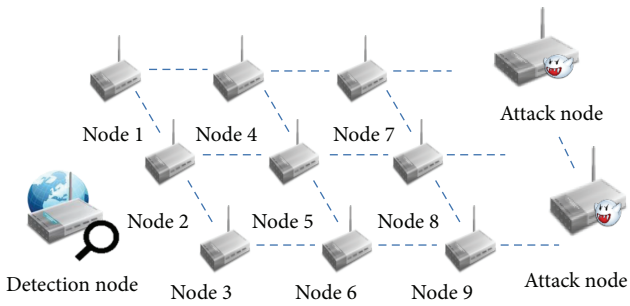

Figure 7: The schematic diagram of the test network.

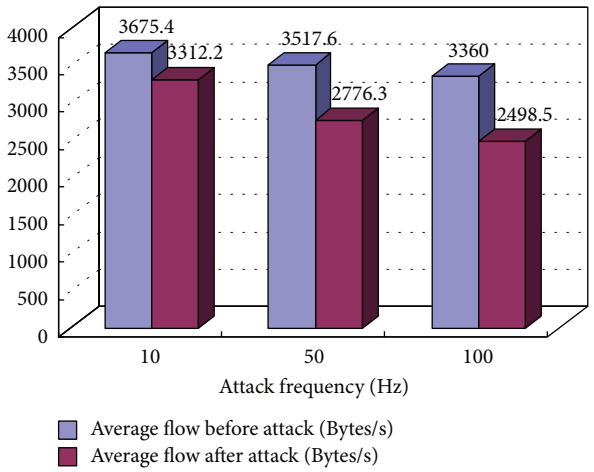

Figure 8: The average flow with different attack frequencies with 3 normal nodes and 1 attack node.

represents a hop transmission distance between two sensor nodes.

3.3. Simulation Results of Flooding Attack. In the experiment, we choose flooding attack frequency, the number of flooding attack nodes, and normal nodes as the attack parameters. By adjusting these parameters, we observe the flow of one node in a certain link. First, we study the relationship between flooding attack frequencies and the flow. The first scenario is performed under different flooding attack frequencies with the same number of flooding attack nodes and normal nodes. The number of normal nodes is 3, while the number of flooding attack nodes is 1.

Figure 8 shows the average flow as the flooding attack frequency varies. When the attacker broadcasts 10 RREQ packets every second in a flooding attack, the average flow changes from 3675.4 Byte/s before the attack to 3312.2 Byte/s after the attack. When the attacker broadcasts 50 RREQ packets every second, the average flow changes from 3517.6 Byte/s before the attack to 2776.3 Byte/s after the attack. When the attacker broadcasts 100 RREQ packets every second, the average flow changes from 3360.0 Byte/s before the attack to 2498.5 Byte/s after the attack.

The flow obviously decreases with the increase of the flooding attack frequency. This is explained by the fact that the more RREQ packets the attacking node broadcasts, the heavier the network load is, thus leading to decrease of other nodes' flow in the network.

Similar experiments show that the flow obviously decreases as the number of flooding attack nodes increases.

Also the flow decreases as the number of normal nodes increases. This is because there are more nodes participating in forwarding RREQ packets the attacker sends. Thus flooding attack has a serious effect in the self-organization network with a large number of nodes.

3.4. Simulation Results of Attack Prevention. In this section, we analyze the simulations of the method to prevent the flooding attack, which is presented in Section 2.

In our experiment, the K value is set to 4. We choose flooding attack frequency, the number of flooding attack nodes, the number of normal nodes, and the cutoff value as the attack parameters. The experimental data of average value is shown in Table 1.

Experiment 1 shows that when the K value is not between the number of attacking nodes and the number of normal nodes, detection system will bring a considerable rate of false alarm, which is consistent with our previous analysis. Experiments 2 and 3 show that the detection effect is obvious and the detection delay is tolerable when we set the appropriate K and cutoff values. In Experiment 4, the detection system cannot detect the attacking node as the cutoff value is not appropriate. Experiments 4, 5, and 6 have the same cutoff value and different attack frequencies; we can see that the more noticeable the attack feature is, the better the detection effect is, the less the detection delay is. This is explained by the fact that the more information the detection system obtains, the easier it detects. So the detection system can work better in larger networks.

Furthermore, we carry on experiments in a large network. The scenario is performed under different cutoff values with the same flooding attack frequency, the same number of flooding attack nodes and normal nodes. The number of normal nodes is 20, while the number of flooding attack nodes is 5. The K value is set to 10. In order to ensure the accuracy of experimental data, the test is repeated 50 times and the data is the average value of the 50 tests. Figure 9 shows the detection effect as the cutoff value varies.

We can see that the detection rate of this detection system is basically above 98.5%, and the false alarm rate 4.63% is relatively high when the cutoff value is 10. This is consistent with our previous analysis. When the cutoff value is above 20, the average detection rate is 99.0%, and the average false alarm rate is 1.5%. Thus the system to detect and prevent the flooding attack is efficient with high correct detection rate and low false alarm rate.

4. Related Work

Due to ubiquitous architecture and wireless transmission channel, the Internet of Things is vulnerable to many security attacks. The Internet of Things is composed of application layer, transport layer, and perceptual layer; thus, security threats the corresponding are also divided into application layer security threats, transport layer security threats, and

Table 1: The experiment data of average value under detection.

Experiment number	Attack frequency (Hz)	Attack nodes	Normal nodes	Cutoff value	K-distance (attack nodes)	K-distance (normal nodes)	Detection delay (s)	Detection rate	False alarm rate
1	10	3	3	15	39	37	1.231	1	0.5
2	10	1	6	15	52	3.2	1.826	1	0
3	10	1	6	35	50.5	2.8	1.821	1	0
4	10	1	6	55	51.7	3	~	0	0
5	50	1	6	55	64	4.1	1.229	1	0
6	100	1	6	55	79	4.5	0.617	1	0

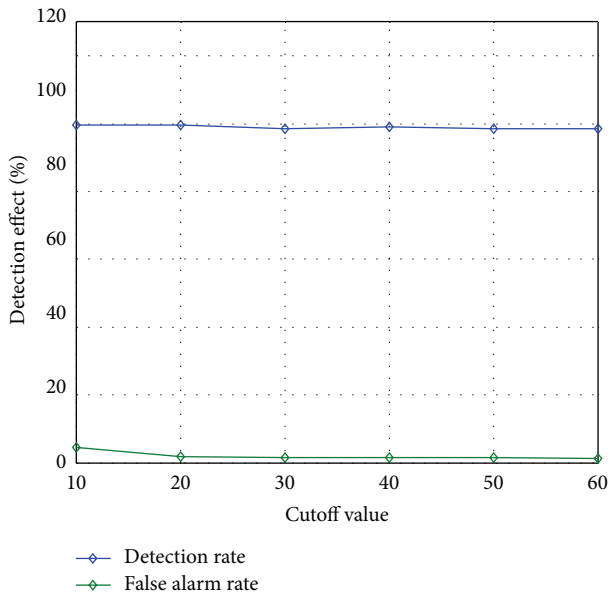

Figure 9: The detection effect with different cutoff values.

perceptual layer security threats. Since the transmission medium broadcast nature, wireless networks have susceptibility to protection attacks such as denial of service (DoS), wormhole attack, Hello flood attack, sinkhole attacks, and Sybil attack [6]. The structure of the Internet of Things is complex and the environment it faces is also complex. Wireless sensor network is an important part of perceptual layer, so we should carry on comprehensive study on its password and security technology [7, 8], secure routing technology [9, 10], secure data fusion technology [11–13], secure localization technology [14, 15], and privacy protection technology [16, 17].

In fact, data mining technique has been widely applied to intrusion detection of wired network [18]. Meanwhile, previous studies [19, 20] have proposed intrusion detection system based on K-means clustering analysis, but the system has two major problems: (1) the K value has serious influence on the mining results and (2) the abnormal node group is difficult to determine.

Yi et al. discussed flooding attack [2, 21]. The intruder broadcasts mass Route Request packets or sends a lot of attacking data packets to exhaust the communication bandwidth and node resource. He presented neighbor suppression, which is a generic defense against the flooding attack in MANETs [22]. He analyzed effect of DoS attack in wireless network [23–25]. Yi et al. presented a cross-layer detection [26], which is an adaptive approach to detecting red and gray hole attacks in ad hoc network based on a cross layer design. He presented the other intrusion detection methods including based finite state machine detection [27], based artificial immune systems detection [28], and distributed intrusion detection [29]. He also presented intrusion prevention mechanism [30] in wireless network, including mobile firewall [31], multiagent cooperative intrusion response [32], and green firewall [33].

Choi et al. proposed a flooding algorithm with retransmission node selection (FARNS) [34] for wireless sensor networks. It is an efficient cross-layer based flooding technique to solve a broadcast storm problem that is produced by simple flooding of nodes in wireless sensor networks. FARNS can decrease waste of unnecessary energy by controlling retransmission action of whole network nodes by deciding retransmission candidate nodes that are selected by identifier information of neighbor nodes in MAC and distance with neighborhood nodes through received signal strength information in PHY. Nigam et al. proposed a profile based protection scheme (PPS) [35] security scheme against DDoS (distributed denial of service) attack. The profile based security scheme checks the profile of each node in network and only the attacker is one of the nodes that flooded the unnecessary packets in network then PPS blocks the performance of attacker. Rughiniş and Gheorghe presented the Storm Control Mechanism [36] that aims at mitigating flooding and denial-of-sleep attacks. The system tracks the frequency of the received packets, triggering an alert when it goes beyond a configured limit. The node tries to send the alert to the base station and then it shuts its wireless transceiver for a predefined period of time. Magotra and Kumar proposed a noncryptographic solution for HELLO flood attack detection [37] in wireless sensor network (WSN). Du et al. presented an effective scheme to defend DoS attack on broadcast authentication in sensor networks [38]. They proposed using sender-specific one-way key chain for broadcast authentication.

Wazid et al. proposed an algorithm named Topology Based Efficient Service Prediction (TBESP) [39] algorithm

depending upon the analysis done which will help in choosing the best suited topology as per the network service requirement under red hole attack. They also proposed a novel technique [40] for the detection and prevention of red hole attack in WSN.

5. Conclusion

As a new technology, the Internet of Things has been more and more widely used. Many related applications have appeared. As one of the applications, the wireless sensor network is becoming more and more popular. As one of the most important technologies in the 21st century, wireless sensor network plays an important role in connecting the logic information world and the existing physical world. However, the open nature of the information media and the poor deployment environment have brought great risks to the security of wireless sensor networks, and it is seriously restricting the application of wireless sensor networks. In this paper, we proposed a new intrusion detection system based on KNN classification algorithm in wireless sensor network. The system can detect flooding attack in wireless sensor network. We also conduct experiments to investigate the effect of flooding attack. The simulation results show that flooding attack can seriously affect the flow especially in larger networks. After analyzing the flooding attack, we present the detection and prevention method to detect the attack. The simulations show that the system can prevent the flooding attack efficiently.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported in part by National Key Basic Research Program of China (2013CB329603), the National Natural Science Foundation of China (no. 61271220 and no. 61170164), and NSF Grant CNS-1217791.

References

[1] P. Yi, Y. Wu, F. Zou, and N. Liu, "A survey on security in wireless mesh networks," *IETE Technical Review*, vol. 27, no. 1, pp. 6–14, 2010.

[2] P. Yi, Y. Hou, Y. P. Zhong, and Z. L. Dai, "Flooding attack and defence in ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 17, no. 2, pp. 410–416, 2006.

[3] Y. Liao and V. R. Vemuri, "Use of k-nearest neighbor classifier for intrusion detection," *Computers & Security*, vol. 21, no. 5, pp. 439–448, 2002.

[4] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, New Orleans, La, USA, February 1999.

[5] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, draft-ietf-manet-dsr-10.txt, 2004.

[6] S. Ahmad Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Security in wireless sensor networks: issues and challenges," in *Proceedings of the IEEE International Conference on Space Science and Communication (IconSpace '13)*, pp. 356–360, Melaka, Malaysia, 2013.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*, pp. 41–47, Washington, DC, USA, November 2002.

[8] W. Zhang and M. Tran, "A random perturbation-based scheme for pairwise key establishment in sensor networks," in *Proceedings of the 8th ACM International Symposium on Mobile ad Hoc Networking and Computing*, New York, NY, USA, 2007.

[9] N. Nasser and Y. Chen, "Secure multipath routing protocol for wireless sensor networks," in *Proceedings of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW '07)*, Toronto, Canada, June 2007.

[10] K. Zhang and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in *Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08)*, Dalian, China, October 2008.

[11] B. Sun, X. Jin, K. Wu, and Y. Xiao, "Integration of secure in-network aggregation and system monitoring for wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 1466–1471, Politecnico di Milano, Glasgow, Scotland, June 2007.

[12] W. Zhang, Y. Liu, S. K. Das, and P. De, "Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach," *Pervasive and Mobile Computing*, vol. 4, no. 5, pp. 658–680, 2008.

[13] D. J. Ferrer, "A provably secure additive and multiplicative privacy homomorphism," in *Proceedings of the 5th International Conference on Information Security*, London, UK, 2002.

[14] C. G. Chang, W. E. Snyder, and C. Wang, "A new relaxation labeling architecture for secure localization in sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, pp. 3076–3081, Glasgow, Scotland, June 2007.

[15] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a theory of robust localization against malicious beacon nodes," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 2065–2073, Phoenix, Ariz, USA, April 2008.

[16] H. E. Wenbo, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: privacy-preserving data aggregation in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 2045–2053, Anchorage, Alaska, USA, May 2007.

[17] W. Zhang, C. Wang, and T. Feng, "GP2S: generic privacy-preservation solutions for approximate aggregation of sensor data," in *Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom '08)*, pp. 179–184, Hong Kong, March 2008.

[18] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection," in *Proceedings of the 7th USENIX Security Symposium*, January 1998.

[19] M. Asaka, T. Onabuta, T. Inoue, S. Okazawa, and S. Goto, "A new intrusion detection method based on discriminant analysis," *IEICE Transactions on Information and Systems*, no. 5, pp. 570–577, 2001.

[20] N. Ye, X. Li, Q. Chen, S. M. Emran, and M. Xu, "Probabilistic techniques for intrusion detection based on computer audit data," *IEEE Transactions on Systems, Man and Cybernetics A: Systems and Humans*, vol. 31, no. 4, pp. 266–274, 2001.

[21] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. H. Li, "A denial of service attack in advanced metering infrastructure network," in *Proceedings of the IEEE International Conference on Communications (ICC '14)*, Sydney , Australia, June 2014.

[22] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "A new routing attack in mobile ad hoc," *International Journal of Information Technology*, vol. 11, no. 2, pp. 83–94, 2005.

[23] P. Yi, F. Zou, Y. Zou, and Z. Wang, "Performance analysis of mobile ad hoc networks under flooding attacks," *Journal of Systems Engineering and Electronics*, vol. 22, no. 2, pp. 334–339, 2011.

[24] P. Yi, Y. Zhou, Y. Wu, and N. Liu, "Effects of denial of service attack in mobile ad hoc networks," *Journal of Shanghai Jiaotong University (Science)*, vol. 14, no. 5, pp. 580–583, 2009.

[25] P. Yi, J. Cai, Y. Wu, and Y. Li, "Impact of two kinds of DoS attacks on mobile ad hoc networks," *Journal of Computational Information Systems*, vol. 5, no. 5, pp. 1433–1443, 2009.

[26] P. Yi, T. Zhu, N. Liu, Y. Wu, and J. Li, "Cross-layer detection for black hole attack in wireless network," *Journal of Computational Information Systems*, vol. 8, no. 10, pp. 4101–4109, 2012.

[27] P. Yi, Y. Wu, N. Liu, and Z. Wang, "Intrusion detection for wireless mesh networks using finite state Machine," *China Communications*, vol. 7, no. 5, pp. 40–48, 2010.

[28] P. Yi, Y. Wu, and J. Chen, "Towards an artificial immune system for detecting anomalies in wireless mesh networks," *China Communications*, vol. 8, no. 3, pp. 107–117, 2011.

[29] P. Yi, X. Jiang, and Y. Wu, "Distributed intrusion detection for mobile ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 19, no. 3, pp. 851–859, 2008.

[30] P. Yi, T. Zhu, J. Ma, and Y. Wu, "An intrusion prevention mechanism in mobile ad hoc networks," *Ad-Hoc & Sensor Wireless Networks*, vol. 17, no. 3-4, pp. 269–292, 2013.

[31] P. Yi, X. Jiang, and J. Li, "Mobile firewall: a framework to isolate intruders in wireless mesh networks," *Journal of Computational Information Systems*, vol. 3, no. 6, pp. 2207–2218, 2007.

[32] P. Yi, F. Zou, X. Jiang, and J. Li, "Multi-agent cooperative intrusion response in mobile adhoc networks," *Journal of Systems Engineering and Electronics*, vol. 18, no. 4, pp. 785–794, 2007.

[33] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, "Green firewall: an energy-efficient intrusion prevention mechanism in wireless sensor network," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 3037–3042, Anaheim, Calif, USA, December 2012.

[34] S. Choi, K. Kwon, and S. Yoo, "An efficient cross-layer based flooding algorithm with retransmission node selection for wireless sensor networks," in *Proceedings of the 22nd International Conference on Advanced Information Networking and Applications Workshops/Symposia (AINA '08)*, pp. 941–948, Okinawa, Japan, March 2008.

[35] V. Nigam, S. Jain, and K. Burse, "Profile based scheme against DDoS attack in WSN," in *Proceedings of the 4th International Conference on Communication Systems and Network Technologies (CSNT '14)*, pp. 112–116, Bhopal, India, 2014.

[36] R. Rughiniş and L. Gheorghe, "Storm control mechanism in wireless sensor networks," in *Proceedings of the 9th Roedunet International Conference (RoEduNet '10)*, pp. 430–435, Sibiu, Romania, June 2010.

[37] S. Magotra and K. Kumar, "Detection of HELLO flood attack on LEACH protocol," in *Proceedings of the IEEE International Advance Computing Conference (IACC '14)*, pp. 193–198, Gurgaon, India, 2014.

[38] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending DoS attacks on broadcast authentication in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 1653–1657, IEEE, Beijing, China, May 2008.

[39] M. Wazid, A. Katal, and R. H. Goudar, "TBESP algorithm for wireless sensor network under blackhole attack," in *Procreedings of the 2nd International Conference on Communication and Signal Processing (ICCSP '13)*, pp. 1086–1091, Melmaruvathur, India, April 2013.

[40] M. Wazid, A. Katal, R. Singh Sachan, R. H. Goudar, and D. P. Singh, "Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network," in *Proceedings of the 2nd International Conference on Communication and Signal Processing (ICCSP '13)*, pp. 576–581, Melmaruvathur, India, April 2013.