2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming

A Secure Routing Mechanism Against Wormhole Attack in IPv6-based Wireless Sensor Networks

Tao Chen[1], Haiping Huang[1, 2*], Zhengyu Chen[1, 2], Yiming Wu[1], Hao Jiang[2, 3]
1 College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2 Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3 School of Computing, Clemson University, Clemson, SC 29634, U.S.A;
Corresponding e-mail: peach_ct@163.com

***Abstract*—The increasing popularity of wireless sensor networks and IPv6 technology is creating varieties of applications for wireless sensor networks based on IPv6. However, IPv6-based Wireless sensor networks are vulnerable to a harmful attack known as the wormhole attack, where a malicious node overhears data packet at one location and tunnels it to a colluding node, which replays it locally. This can have a negative influence on the routing mechanism by preventing nodes from discovering the normal routes. In this paper, we present a secure routing mechanism against wormhole attack in IPv6-based wireless sensor networks. The design of this routing mechanism can be divided into two phases--wormhole detection and defense, which is based on the average distance per hop in the network and the TTL of IP header. Besides, our proposal does not require special hardware or high computation and storage capacity of the node, which is quite suitable for the resource-constrained IPv6-based wireless sensor networks. The simulation results show that our proposal is effective under the conditions of different network topology and wormhole parameters.**

Keywords—Wireless sensor networks(WSNs), Wormhole attack, IPv6, Wormhole detection and defense, Security

I. INTRODUCTION

In recent years, wireless sensor networks (WSNs) has been applied to many fields such as traffic, medication, and military affairs [1]. With the development of next generation Internet technology, IP protocol is transferring from IPv4 to IPv6. Compared with IPv4, IPv6 has many merits--larger address space, extended address structure, flexible header format, etc. Thus, WSNs based on IPv6 communication will have widespread application in the future [2].

However, security problems in WSNs have received comprehensive attention, especially in routing protocol supporting IPv6 communication. ROLL (Routing Over Low power and Lossy networks) panel once proposed an IPv6 routing protocol--RPL for low power and lossy networks [3], but they didn’t take into account the security of data transmission in WSNs [4]. Besides, due to the constraint in energy, computing and storage, it is difficult for the traditional security measures to be directly applied to WSNs. For instance, owed to limited resources in WSNs, the implementations of encryption algorithm or IDS module would probably shorten the life of node and thus decrease its availability [5].

Wormhole attack is one of the most threatening and harmful attacks against IPv6-based WSNs [6]. In the wormhole attack, two malicious nodes conspire to build a low-latency, high-quality and out-of-band tunnel between them. The tunnel is also referred to as ‘wormhole link’ and is available only to these two nodes. One node (attacker) overhears the packets sent by the surrounding nodes and then delivers them via the tunnel to the other malicious node (colluding node) to replay. Since the colluding node is able to transmit packets to the sink with less hops, nodes around attacker would mistakenly believe that packets delivered via the wormhole link would cost less hops and distance. As a result, the wormhole link would become the favored route via which packets are transmitted.

In this paper, we propose a secure routing protocol against wormhole attack in IPv6-based WSNs. The protocol is divided into two phases--wormhole detection and wormhole defense. The wormhole detection mechanism depends on whether the average distance per hop in the network exceeds the threshold (i.e. the communication range of node). In the wormhole defense mechanism, the defending node will send a large number of packets to cause the wormhole link congestion.

The rest of this paper is organized as follows. Section II reviews the related work against wormhole attack. In Section III, we describe the network model, wormhole attack model and essential assumptions. Section IV describes our proposed secure routing protocol in detail. Finally, in Section V, we concludes this paper and outlines our future work.

II. RELATED WORK

The wormhole attack in wireless sensor networks was independently introduced by Dahill [7], Papadimitratos [8] and Hu [9]. In order to guarantee the security of data transmission, many routing protocols have employed light-weight encryption mechanisms. For instance, in IPv6 network, users can encrypt data and check IP packets in the network layer. Besides, the encryption and authentication options in IPv6 provides the service for the packet’s confidentiality and integrity, which dramatically strengthens network security [10]. However, wormhole attack is immune to the encryption mechanism because malicious nodes can replay authenticated packets [11]. Although wormhole attack is difficult to prevent, researchers still obtained some solutions. In this section, we will summarize some existing approaches against wormhole attack.

2168-3042/15 $31.00 © 2015 IEEE
DOI 10.1109/PAAP.2015.30

Some detection mechanisms involve equipping nodes with special hardware and enable these nodes to detect the wormhole attack. Capkun et al. [12] proposed a detection approach called SECTOR based on one special hardware. The hardware calculates the distance between two sides of communication in terms of the packets it received, so the node would know whether the packets are transmitted via the legal route or via the wormhole link. This approach is based on distance limitation, one-way hash chain and hash tree and does not need clock synchronization and location information. But cost of extra hardware restricts the application of this approach in WSNs.

Apart from employing special hardware, some approaches based on location information were used to detect the wormhole attack. In [9], Hu et al. proposed two kinds of packet mechanisms, geographical leashes and temporal leashes to detect the wormhole attack. In the geographical leashes mechanism, each node must know its own location, while in the temporal leashes mechanism, the whole network needs to be tightly synchronized. However, the approach increases the consumption of communication and storage.

Besides, some approaches detect the wormhole attack by setting trust value of the node. The source node gives trust value of each neighbor node by monitoring their behaviors. Node having the highest trust value would be chosen to be the next hop. Hence, the source node can choose the most credible route to the destination node by the trust value mechanism, which is possible for the node to avoid the wormhole attack [13]. Ozdemir et al. [13] proposed a wormhole detection approach based on time and trust value. Node is composed of two modules--trust value based module and time-based module. Since the malicious node would cause fake transmission time, trust value can help get rid of wrong time and thus ensure the correctness of route.

Moreover, a wormhole detection approach based on statistics analysis is proposed by many researchers. The basic assumption of this approach is that the number of neighbor nodes surrounding malicious nodes would increase due to the wormhole attack. Kong F et al. [14] devised a distributed algorithm WAPN to detect the wormhole attack. First, the threshold of each node is given according to the distribution of nodes in the network. Then, each node counts the number of neighbor nodes and compares it with the threshold. If the number exceeds the threshold, then the node is infected, indicating that there exits wormhole attack in the network.

In [15], a label-based secure localization scheme is proposed to defend against the wormhole attack. The main idea of this scheme is to generate a pseudo neighbor list for each beacon node, use all pseudo neighbor lists received from neighboring beacon nodes to classify all attacked nodes into different groups, and then label all neighboring nodes (including beacons and unknown nodes). According to the labels of neighboring nodes, each node prohibits the communications with its pseudo neighbors, which are attacked by the wormhole attack. Dezun Dong et al. [16] proposed a distributed approach dependent on network connectivity information. They analyzed the wormhole issue by topology methodology and by observing the inevitable topology deviations introduced by wormholes. By detecting non-separating loops(pairs), their approach can detect and locate various wormholes.

III. Assumptions, Notations and Models

A. Network Model

In wireless sensor networks, sensor nodes are classified into beacon nodes and unknown nodes depending on whether the location information of node is known. The ratio of beacon nodes in the network plays an important role in localization and routing mechanism in WSNs. The network model used in this paper is depicted in Fig.1. It employs the following assumptions:

(1) All the nodes are disposed in a relatively stable environment. Nodes are static and none of them are physically damaged.

(2) All the nodes are randomly and uniformly disposed in a square sensing area whose side is *D*.

(3) Normal nodes including beacon nodes and unknown nodes have the same communication range. Nodes with specific IPv6 address are designated as beacon nodes.

(4) The sensing area is relatively broad compared with the communication range of a single sensor node, which means *D*>>*R*.

(5) Each node has a neighbor list and can adjust it based on the change of network topology. For example, node can remove the IPv6 address of some nodes from the neighbor list so that the packets it forwards would not arrive at these nodes.

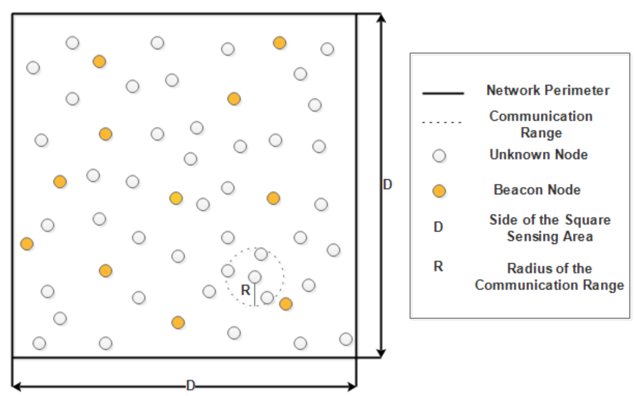

Fig. 1. The network model

B. Wormhole Attack Model

In this paper, we only discuss the wormhole attack between beacon nodes and the wormhole attack is a visible attack via an out-of-band tunnel. Visible attack means the malicious node in the network topology is visible, but only pretends to be a normal node. Besides, we suppose that there is, if any, only one pair of malicious nodes in the network. Malicious nodes only selectively forward packets. In other words, they don't drop or alter packets being transmitted.

The wormhole attack model is depicted in Fig.2. A malicious node M_1 can overhear all the nodes $\{B_1, U_1, U_2, U_3, U_4, U_5\}$ that are in its communication range. Then, M_1 deliver all the packets being overheard to the other malicious node M_2 via the low-latency and high-quality tunnel. When M_2 receives the packets from M_1, it forwards them to part of nodes $\{B_2, U_6, U_7, U_8, U_9, U_{10}\}$ that are in M_2's communication range. Because the tunnel allows bidirectional transmission, messages overheard by M_2 can also be delivered to M_1 via the tunnel.

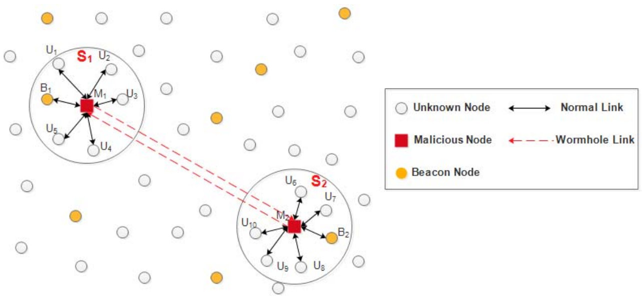

Fig. 2. The wormhole attack model

We refer to the influencing area of malicious nodes M_1 and M_2 as infected area S_1 and S_2, as shown in Fig.2. Nodes in the infected area are affected by the same pair of malicious nodes. Therefore, if we can find a pair of nodes in the infected area, e.g. U_1 and U_6 in Fig.2 and enable them to detect wormhole and take defensive measures with specific algorithm, the wormhole link M_1-M_2 can be eliminated and the corresponding infected area would disappear. Since each node has its IPv6 address, when the malicious nodes are removed, the IPv6 address of them should be recycled and other nodes should be informed.

Considering that the beacon node has its location information and hops away from other beacon nodes, we choose a pair of beacon nodes B_1 and B_2 to detect and defend against the wormhole attack. Admittedly, the most obvious drawback of this scheme is that if there is no beacon node in one infected area, the scheme would become invalid. However, if the nodes are randomly and uniformly disposed in a stable area and we keep the ratio of beacon nodes within certain range, e.g. by disposing some specific beacon nodes in the IPv6 net section, we can always find at least one beacon node in any infected area with high probability.

Thus, the simplified wormhole attack model is shown in Fig.3. In this figure, A and B are referred to as beacon nodes; U_1, U_2 ... U_{13} symbolize unknown nodes and M_1 and M_2 are referred to as malicious nodes. When A sends packets to B, because the hops of wormhole link M_1-M_2 are much less than that of other two links U_1-U_2-U_3-U_4-U_5-U_6-U_7 and U_8-U_9-U_{10}-U_{11}-U_{12}-U_{13}, packets would be delivered to B via the wormhole link M_1-M_2.

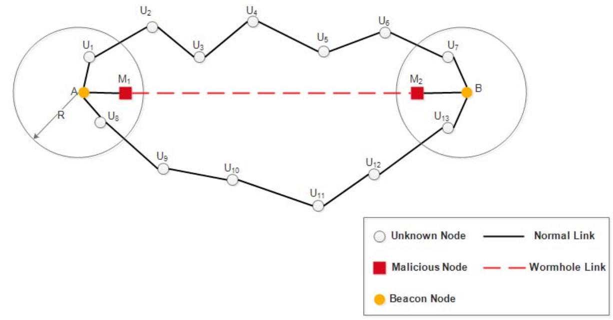

Fig. 3. The simplified wormhole attack model

In this paper, our work is to enable the pair of beacon nodes A and B to detect and defend against the wormhole attack. Section IV describes the detection and defense algorithm in detail.

IV. SECURE ROUTING ALGORITHM DESCRIPTION

The routing algorithm is divided into two phases--wormhole detection and wormhole defense. The purpose of detection algorithm is to judge whether or not there is a wormhole attack in the network topology. If the attack exists, we further determine the wormhole link, defending node and corresponding defensive measures.

A. Wormhole Attack Detection

In order to guarantee that two neighboring nodes can keep normal communication, the distance between these two nodes is supposed be no greater than the communication range of node R. So, for a pair of beacon nodes A and B, the average distance per hop between them should also be no greater than the communication range of node R. However, if the node suffers from the wormhole attack, the hops of the wormhole link are much less than that of normal route, which makes average distance per hop between A and B greater than the communication range of node R. Therefore, we can detect the wormhole attack in the network by the following inequality:

$$\frac{\sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}}{h_{AB}} > R$$

where (x_A, y_A) and (x_B, y_B) are the coordinates of A and B; h_{AB} is the minimum hops between A and B; R is the communication range of the node. If the above inequality is satisfied, it means that there is a wormhole link between A and B.

As illustrated in Fig.3, suppose that the communication range of normal node R is 20m, and the distance between A and B is 120m. Under the influence of wormhole attack, the hops between them is shorten to 4. So, based on the above inequality, the average distance per hop between A and B is 30m, greater than the communication range of node R. Thus, we can make a conclusion that wormhole attack happens between A and B.

Furthermore, in Fig.3, as the hops of link A-M_1-M_2-B is the least compared with other links between A and B, we decide that the link A-M_1-M_2-B is abnormal and take it as the suspicious target. Thus, we can further determine the wormhole link M_1-M_2 and the malicious nodes M_1 and M_2.

The wormhole detection algorithm is specified as follows:

Algorithm 1 Wormhole Attack Detection

Step1: Initialize i=0.

Step2: Beacon node B_i broadcasts its message to the network with the format $\{id_i, x_i, y_i, hop_i\}$, where id_i is referred to as IPv6 address of beacon node, representing the identity of node; (x_i, y_i) is the coordinates of the beacon node and hop_i is the hop-count with the initial value 0.

Step3: Node which has received the message from B_i would increase hop_i by 1, store the minimum hops away from beacon node B_i, and then broadcast its message to the network with the same format.

Step4: Initialize $j=i+1$.

Step5: After receiving the message from B_i, another beacon node B_j would update the hops and add its own ID number (IPv6 address) and location information to the packet, sending back to the node B_i.

Step6: After receiving the message from B_j, B_i calculates $\frac{\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{h_{ij}}$ and compares it with the communication range of node R, where (x_i, y_i) and (x_j, y_j) are the coordinates of B_i and B_j, h_{ij} is the minimum hops between two nodes. If $\frac{\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}}{h_{ij}} > R$, which indicates that there is a wormhole between B_i and B_j, then go to Step9 else increment j by 1;

Step7: If $j<N$, then go back to Step5 else go to Step8, where N is the number of beacon nodes.

Step8: Increment i by 1. If $i=N$-1, which indicates that no wormhole exits, then go to Step9 else go back to Step2.

Step9: End.

B. Wormhole Attack Defense

As shown in Fig.4, after determining the malicious nodes, we cannot simply screen them, otherwise other nodes are still likely to take M_1 or M_2 as the next hop when conducting neighbor discovery, which would cause an unnecessary and repetitive judgment. Therefore, we take the following algorithm to defend against wormhole attack.

Algorithm2 Wormhole Attack Defense

Step1: Choose node A and B adjacent to M_1 and M_2 as the defending node.

Step2: A sends a large number of packets to B in a short time and the value of TTL in the IP header is set to 255. Since there is a wormhole link between A and B, all the packets would go to B via the M_1-M_2 link.

Step3: Then, A refuses to receive packets from M_1 and B refuses to receive packets from M_2. As TTL is set to the maximum value, these packets would transmit between M_1 and M_2 back and forth, leading to the congestion and high-latency in link M_1-M_2.

Step4: Surrounding nodes would remove M_1 and M_2 from their neighbor lists when conducting neighbor discovery. So, nodes would not choose M_1 and M_2 to transmit their packets and thus wormhole attack gets eliminated.

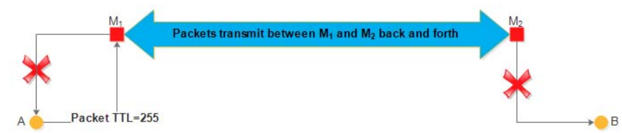

Fig. 4. Packets transmit between M_1 and M_2 back and forth leading to congestion

V. SIMULATION AND PERFORMANCE EVALUATION

In order to make an objective evaluation of the performance of our algorithm, we design a set of experiments to simulate the algorithm and compare with Wu J's proposal [15].

We dispose some nodes in a $50 \times 50m^2$ sensing area and generate the corresponding network topology. In these nodes, we randomly choose two nodes to become a pair of malicious nodes and enable them to launch wormhole attack. Parameters involved in experiments are shown in Table 1.

TABLE I. THE SIMULATION PARAMETER SETTING

Parameter(unit)	*Definition*
R(m)	Communication range of normal node(beacon node and unknown node)
$R_M(m)$	Communication range of malicious node
L(m)	Length of wormhole link
n	The number of nodes
ω	The ratio of beacon nodes

We dispose 100 nodes randomly in the sensing area, setting the communication range of R to 10m and the ratio of beacon nodes to 30%. Then, we evaluate the algorithm's performance on detecting wormhole by varying the length of wormhole link. Fig.5 reveals the relationship between wormhole detection rate and the ratio L to R. In Fig.5, we can find that two algorithms both have a high detection rate. In Wu J's algorithm, when L/R varies from 1 to 1.5, the detection rate has a slight downward trend. When L/R continues to increase, the detection rate levels off, maintaining at about 0.955. By contrast, in our proposal, the detection rate shows an upward trend with the increase of L. Moreover, when L/R is greater than 2, the detection rate of our algorithm is higher than that of Wu J's. The reason is that the longer the wormhole link is, the more hops the packets have to pass from source to destination if packets are transmitted through the normal link. But if there exists a wormhole link, the hops between source and destination would dramatically decrease and thus make the wormhole attack effect much more significant. So, according to our algorithm, we can easily detect the wormhole attack and thus get a high detection rate.

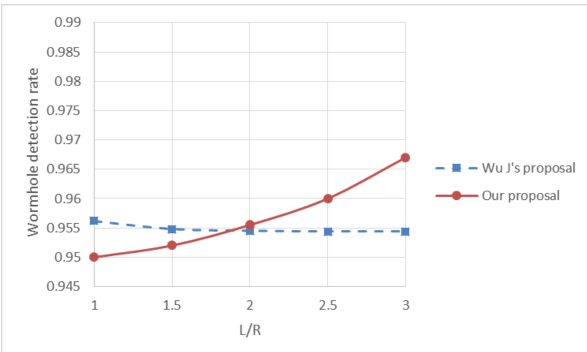

Fig. 5. Wormhole detection rate against L/R

Then, under the condition of n=100, R=10m, R_M=10m, and L/R=2, we evaluate the algorithm's performance on wormhole detection rate by varying the beacon node ratio for different communication range of malicious node. Fig.6 shows the relationship between wormhole detection rate and beacon node ratio. In this figure, we can find that when R_M in our proposal is set to 10m, the detection rate is lower than that of Wu J's algorithm. Since our detection algorithm depends on the number of beacon nodes, this can be explained by the fact that when the R_M is small, probably there will be no beacon nodes in the infected area, which makes the false negatives become high. So, when we raise R_M, the detection rate as shown in Fig.6 dramatically increases. Meanwhile, with the increase of ω , the probability of nodes appearing in the infected area increases, which increases the detection rate of our algorithm.

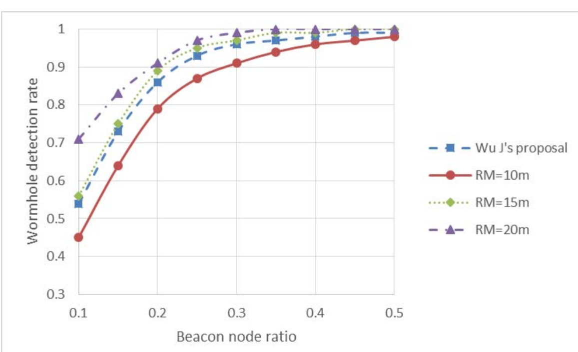

Fig. 6. Wormhole detection rate against beacon node ratio at different communication ranges, R_M, of the malicious node

Finally, we evaluate the defending effectiveness after detecting the wormhole attack. The parameters involved in this experiment are set as follows: n=100, R=10m, R_M=15m, and L/R=3. When the wormhole attack is initiated, the surrounding packets would transfer from the original route to this high-quality wormhole link. As shown in the Fig.7, the dot curve indicates that the number of packets on the wormhole link dramatically increases after the wormhole attack; when the defending nodes begin to take defensive measures, the square curve reveals that the number of packets on the wormhole link grows exponentially. Gradually, the wormhole link becomes congested and the metric of link decreases, which indicates that our algorithm's defense against wormhole is effective. Therefore, when the nodes conduct the neighbor discovery, they will remove the malicious nodes from their respective neighbor lists and the wormhole link gets eliminated.

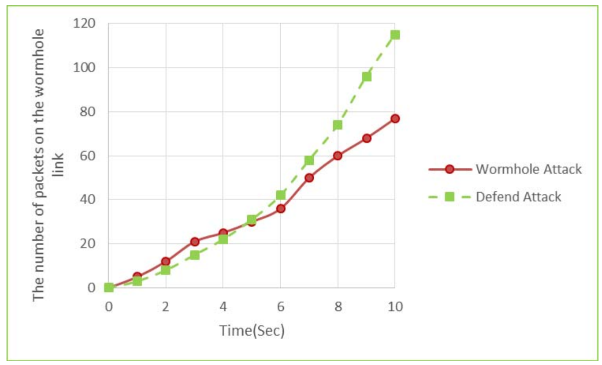

Fig. 7. The number of packets on the wormhole link against time

Fig.8 shows the packet loss rate from the beginning of attack to the end of attack. At the beginning, wormhole attack causes about 25% packets loss whereas the packet loss rate drops from 25% to 5% at the end of defense.

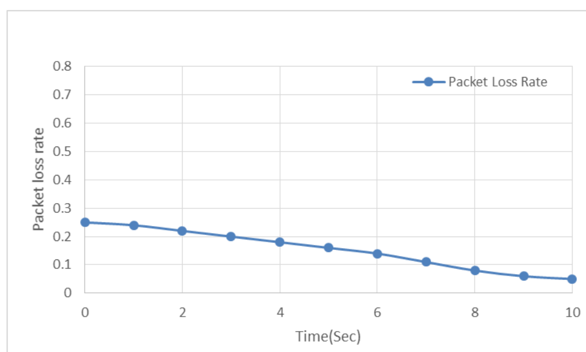

Fig. 8. Packet loss rate against time

VI. Conclusion and Future Work

Aimed at wormhole attack, this paper presents a secure routing protocol based on average distance per hop and TTL of IPv6 header. It differs from previous approaches that require extra hardware or high computation and storage capacity of node. Meanwhile, we prove the effectiveness of our algorithm by the simulations and comparisons with Wu J's proposal. The results of simulations shows that our wormhole detection rate is desirable and the defensive measure is effective.

In this paper, we only discuss a pair of malicious nodes that launch wormhole attack. In the following work, we will study how to detect wormhole attack when there are more than one wormhole link in the network topology. Moreover, we will study how to detect invisible wormhole attack in the network.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers of this paper for his/her objective comments and helpful suggestions while at the same time helping us to improve the English spelling and grammar throughout the manuscript.

And meanwhile, the subject was sponsored by the National Natural Science Foundation of P. R. China (No. 61170065, 61202355, 61373138), Natural Science Key Fund for Colleges and Universities in Jiangsu Province (No.12KJA520002), the Key Research and Development Program of Jiangsu Province(Social Development Program, No.BE2015702), Postdoctoral Foundation (No. 2015M570468), Science and Technology Innovation Fund for Postgraduate Education of Jiangsu Province (No. KYLX15_0853).

REFERENCES

[1] Bokare M M, Ralegaonkar M A. Wireless Sensor Network[J]. International Journal of Computer Engineering Science (IJCES), 2012, 2(3).

[2] Wu P, Cui Y, Wu J, et al. Transition from IPv4 to IPv6: A state-of-the-art survey[J]. Communications Surveys & Tutorials, IEEE, 2013, 15(3): 1407-1424.

[3] Winter T, Thubert P, Clausen T, et al. RPL: IPv6 routing protocol for low power and lossy networks, RFC 6550[J]. IETF ROLL WG, Tech. Rep, 2012.

[4] Grgic K, Zagar D, Krizanovic V. Security in IPv6-based wireless sensor network — Precision agriculture example[C]//Telecommunications (ConTEL), 2013 12th International Conference on. IEEE, 2013: 79-86.

[5] Alrajeh N A, Khan S, Shams B. Intrusion detection systems in wireless sensor networks: a review[J]. International Journal of Distributed Sensor Networks, 2013, 2013.

[6] Krentz K F, Wunder G. 6LoWPAN Security: Avoiding Hidden Wormholes using Channel Reciprocity[C]//Proceedings of the 4th International Workshop on Trustworthy Embedded Devices. ACM, 2014: 13-22.

[7] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad-hoc networks," Electrical Engineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001.

[8] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[9] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

[10] Deering S E. Internet protocol, version 6 (IPv6) specification[J]. 1998.

[11] Sastry A S, Sulthana S, Vagdevi S. Security Threats in Wireless Sensor Networks in Each Layer[J]. Int. J. Advanced Networking and Applications, 2013, 4(04): 1657-1661.

[12] Capkun S, Butty an L,Hubaux J P. SECTOR: Secure tracking of node encounters in multi-hop wireless networks [A]. Proc the 1st ACM workshop on Security of ad-hoc and sensor networks [C]. 2003. 21-32.

[13] Ozdemir S,Meghdadi M,Giiler I. A time and trust based wormhole detection algorithm for wireless sensor networks [A]. Proc the 3rd Information Security and Cryptology Conference [C], 2008. 139-144

[14] Kong F,Li C, Ding Q,et al. WAPN: a distributed wormhole attack detection approach for wireless sensor networks [J]. JOURNAL OF ZHEJIANG UNIVERSITY - SCIENCE A, 2009,10(2): 279-289

[15] Wu J, Chen H, Lou W, et al. Label-based DV-HOP localization against wormhole attacks in wireless sensor networks[C]//Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on. IEEE, 2010: 79-88.

[16] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks, " IEEE/ACM Transactions on Networking, vol. 19, no. 6, 2011, pp. 1787-1796.