A Security Routing Protocol for Internet of Things Based on RPL

Guojun Ma[1,2]
1. School of Information Engineering,
Xi'an University,
2. State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an, China
guojunma@126.com

Xing Li, Qingqi Pei, Zi Li
State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an, China
261969550@qq.com, qqpei@mail.xidian.edu.cn,
lzchmily@163.com

***Abstract*—RPL is a lightweight IPv6 network routing protocol specifically designed by IETF, which can make full use of the energy of intelligent devices and compute the resource to build the flexible topological structure. This paper analyzes the security problems of RPL, sets up a test network to test RPL network security, proposes a RPL based security routing protocol M-RPL. The routing protocol establishes a hierarchical clustering network topology, the intelligent device of the network establishes the backup path in different clusters during the route discovery phase, enable backup paths to ensure data routing when a network is compromised. Setting up a test prototype network, simulating some attacks against the routing protocols in the network. The test results show that the M-RPL network can effectively resist the routing attacks. M-RPL provides a solution to ensure the Internet of Things (IoT) security.**

Keywords-IoT; routing security; routing attack; multipath routing

I. INTRODUCTION

In recent years, the communication technology has developed in a long run, and the communication method has also get richer, people are no longer limited to connecting people with people to communicate, they also expecting be able to connect people with things, things and things, so the idea of the Internet of Things was introduced. In the internet of things, everything around you can be added to the communication network and connect with the traditional internet, they can communicate freely, exchange information. The "things" of IoT refers to the intelligent devices that have communication and access to the internet, the equipment has the characteristics of large quantity, frequent switching and limited resource. Special routing protocol is need to manage and organize these smart devices for efficient and secure networks and to integrate it with the traditional internet. To meet the demand, the IETF designed a lightweight IPv6 network routing protocol for the internet of things, the RPL routing protocol [1].

RPL routing protocols enable efficient use of smart devices energy, compute resources, build flexible topology and data routing. However, the RPL routing protocol does not consider the network security in the network stage, and does not ensures network security through routing repair mechanisms when the network is built, and the network will be unable to respond in a timely manner after attack. Therefore, it is necessary to study and analyze the security issues of the RPL routing protocol.

The internet of things, due to resource constraints and complex deployment environments, threats come from a variety of stages, is more vulnerable than the traditional internet [2]. This paper discusses the contents of the RPL routing protocol network process, security policy and so on. An RPL based secure routing protocol M-RPL, is proposed. which expands the RPL protocol from the directed acyclic graphs topology to hierarchical clustering topology, and there are many clusters-cross path ensures data arrival rates against common routing attacks. In the end, a prototype test system platform is set up. The M-RPL multipath data communication and attack defense are tested.

Section 2 covers the contents of the RPL routing protocol, section 3 designs the principles and implementation of the M-RPL routing protocol, section 4 introduces the platform of the test network, and the M-RPL multipath communication and security defense of the network are tested. The results show that M-RPL routing protocol is effective against routing attacks. Finally, the paper summarizes and prospected the paper.

II. RELATED WORKS

RPL is a routing protocol based on distance vector, which is specially designed for low power, resource constrained network. The entire routing protocol is built through the interaction of ICMPv6 control messages across smart devices. The optimal path selection of RPL routing protocol is constrained by functions, different functions can be designed for different scenarios to make the structure more flexible, the network more efficient and the network communication more stable. The RPL routing protocol can meet the rapidly fields changing of the network topology in a fixed state at a certain point, the whole network construct is a destination oriented directed acyclic graph (DODAG). The network topology of the network will change at any time, and the RPL is able to respond quickly to network status changes and select the optimal path based on functions.

The RPL protocol has been widely studied due to large amount of threat to internet of things. The literature [3] studied the attack and defense against rank value of RPL routing protocol. The literature [4] analyzed the wormhole attack implementation and the detection of wormhole attack. The literature [5] is the standard document for RFC, analyzes

978-1-5386-0604-9/17 $31.00 © 2017 IEEE
DOI 10.1109/NaNA.2017.28

the possible security threats to the RPL routing protocol, and provides some theoretical solutions. In the literature [6], a method of topological authentication was proposed to address the rank value attack behavior of the RPL network. In the literature [7], the attack strategy and defense methods for selecting and forwarding of RPL network are given. In the literature [8], the attack implementation and defense method of black hole attack in RPL network are illustrated. In the literature [9], the paper gave the representation of the RPL network in the case of the sybil attack, and gave the theoretical solution.

III. M-RPL ROUTING PROTOCOL

Limited resources and unreliable communication link are two significant networks problem for smart devices in the internet of things [11], which bring the problem of rapid network topology changes.

The RPL is a single-link routing protocol. The RPL's security mechanism relies on the public key cryptography system, and secure routing control message is used to improve the RPL network security [10]. The network performance decreases when network size increasing. In the case of attacking or topology change, the routing mechanism is difficult to be repaired in time. Therefore the multi-path mechanism is necessary to study [12].

For the above question, a RPL based, layering, clustering, multipath secure routing protocol M-RPL (multiparty-rpl) is designed. The M-RPL adopts a hierarchical topology for managing large rules and multipath routing strategy is adopter to guarantee the data delivery rate and resist the routing attack.

A. The M-RPL routing protocol principle

M-RPL is a multi-path routing protocol for hierarchical clustering. The top layer of the topology is the gateway node of the entire network, realizing heterogeneous network communication. The second layer is the cluster head node, which can be used to network and forward the information. The bottom layer is the common node. In order to provide network security, each common node creates a backup path to another cluster. When a node sends data, it provides a multi-hop path for data forwarding. The topology of the entire network is shown at Figure 1. The light-colored line represents the backup path provided by the node.

The gateway node as the uppermost node, is responsible for self-organizing networks, inter-cluster communication, and other external form networks communication.

The cluster head node is responsible for initiating the self-organization of a cluster network, and providing the data forwarding capability to communicate nodes with the nodes in same cluster or in other cluster nodes. Cluster heads are specified directly, and directly communicate with gateway.

The common nodes in the cluster are self-organized to provide security and multiple paths for data forwarding.

When the node sending data, it sends two data packets through the destination address and the backup path, data delivery can be guaranteed by increasing the redundancy of the data to provide the reach-ability.

In this network topology, the entire self-organization composed of multiple clusters identified with instance, each cluster is identified with a special DODAG id. The basic topology of each cluster is a DAG. An Instance contains lots of clusters, which contain multiple DODAG, the same instance has the same instance id, which uses the same function to choose the parent node. Within the network, each cluster is identified with a DODAG ID, which based on a cluster head node IPv6 address. The common nodes' relative position to the cluster head node in the cluster are determined by the rank value.

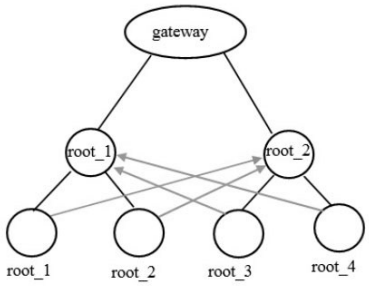

Figure 1. The network topology

B. The M-RPL routing protocol implementation

The entire network topology is built with the following procedures: cluster header elections, cluster head noticing and upward routing, the backup path establishing, the downstream routing creating, and the new nodes adding. The details of these processes will be explained separately.

1) The cluster head election

During the routing establishment phase, the cluster heads produced by comparing the value of a random number. Each node produces a random number and interact with their random values, by comparing the random values, the node whose has max random value is chosen as the cluster head.

2) Cluster head noticing

The nodes that were elected as cluster heads will send notification message (RN) to the gateway node. The gateway node maintains a cluster header table to hold the cluster header nodes relevant information. At the same time, the gateway node will always query the cluster headers' reach-ability. When the header receives a query message sent by the gateway node, it must reply to a cluster head notification message to help the gateway node maintain its own accessibility.

3) Upward routing and backup path setting up

a) The cluster header node sends the M-DIO message: After the configuration of network information, cluster nodes will broadcast the M-DIO messages. M-DIO message contains the M-RPL instance identifier, the version number of DAG, the identity values of DAG, the rank value of the cluster head, the pattern of routing protocol work, the messages of DAG, route control functions and the IP of the neighbor nodes, etc.

b) Common nodes select parent node: In the network, the upper node will broadcast the DIO messages, therefore

the nodes in the network topology will receive DIO messages from different nodes. At this point, relevent words are extracted from the DIO messages by the common node as parameters of optimal path selecting function, common node select a suitable node as its parent node through calculating and comparing.

c) Common nodes establish backup paths: After determining parent node, A node will process the received M-DIO message and judge whether the received M-DIO has same DODAG id as its parent has. If the DODAG id is different, that means the M-DIO was sent from a different cluster, the source address of the message is set as its own backup path.

4) Downstream routing building

After a common nodes handling the M-DIO messages from the neighbor's nodes and electing an appropriate neighbor as its parent. The node will mark the IP address in its default routing table as the parent IP address. And then, the common node will send the M-DAO message to its parent, because the upstream path to the parent node is already built, the node can broadcast the M-DAO message to the order nodes. The M-DAO message contains the address information for the child nodes, helping the parent node to establish the downstream route.

5) The new node's joining

For new nodes that want to join an existing networks, send M-DIS messages actively to the surrounding nodes to query the network status. According to M-RPL routing protocol rules, after receiving the request information, the surrounding nodes will response the new node an M-DIO message containing routing information to begin the process of network.

IV. THE ANALYSIS OF TEST AND RESULT

Each node in the test network is a combination of hardware and software node, using Contiki operating system and TI Company's CC2530 chip, and t-he M-RPL code is embedded in the test node. Each node is connected with the computer by the serial port to display communication data between nodes. After the cluster is completely built, the node can be triggered to submit the network topology to the gateway which will display the topology of each cluster through the topology display software of the computer side. The software displays the topology and data communication of the entire network protocol to verify routing protocols.

A. Multipath routing communication test

The whole network consists of gateway node, cluster head node and common node. The gateway node that can collect the entire network topology information, shows the network topology, at the same time, it can server as a heterogeneous router to realize the communication cross clusters.

The test procedure is as follows:

1) Organization: The network is displayed by the gateway after the topology notification. The entire network topology is shown in Figure 3. The post 16bit of the IPv6 of each node, temperature and humidity is shown in the topology to simulate data collected by sensors. The post 16bit of the IPv6 is used to identify the corresponding node in the subsequent paper. The node b6fc represents the gateway node, the node b5b4 and the node a1b7 represents the cluster head node, and other nodes represents common node.

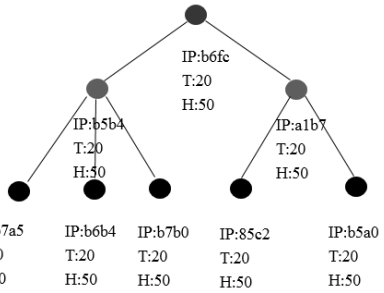

Figure 2. Network topology before multipath routing was turned on

2) Selection: node 85c2 is selected as the source node of data transmission, node b7b0 is selected as the destination node for data reception, where the destination node and the source node are in different cluster. The source node and the destination are connecting to the display to show the sending and receiving. The multipath is demonstrated at source node. When the multipath is not enabled, the display software does not show the backup path for the connection at the topology. This moment, the source node send data, the destination node can receive one data packet.

```
Node send message : 'hello#1', to aaaa::0212:4b00:02f5:b7b0
Node send message : 'hello#2', to aaaa::0212:4b00:02f5:b7b0
Node send message : 'hello#3', to aaaa::0212:4b00:02f5:b7b0

Node receive message : 'hello#1', from aaaa::0212:4b00:03d0:85c2
---------------------------
Node receive message : 'hello#2', from aaaa::0212:4b00:03d0:85c2
---------------------------
Node receive message : 'hello#3', from aaaa::0212:4b00:03d0:85c2
```

Figure 3. The backup path is not enabled

3) Multipath: when the multipath is turned on, the multipath opening information is uploaded to the gateway's topology display software by the source node. The source node displayed the connection to the backup path. In Figure 5, the dotted line represents the backup path.

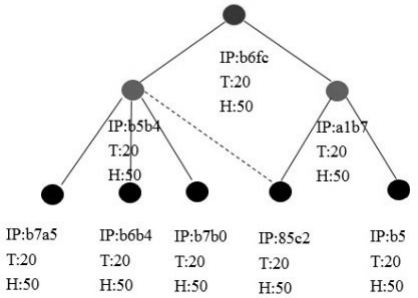

Figure 4. Network topology after multipath routing was turned on

4) Backup path: after the backup path is turned on, the source node sends the data to the destination node, through the serial display window, we can see that the destination node received two data packages. The specific process is shown in Figure 5.

Figure 5. The backup path is abled

B. The black hole attack test

One node is selected in the same cluster of the data source node, as a black hole node. A black hole attack is initiated at the selected node by means of a button hit and the black hole attack process is showed by the connecting monitor. The black hole node will take the other nodes in the cluster as its child nodes. The identity information of the black hole node and the topology of present stage of the cluster network will be reported to the gateway and showed in the gateway topology display software. Figure 6 show the topology in normal network state before black hole attack.

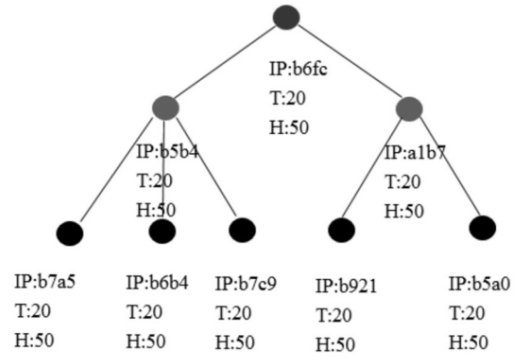

Figure 6. Network topology before black hole attack

Common nodes can receive data packets before the attack, the source node send the temperature information to the destination node periodically. Packet shows the IPv6 address of source node, specific data reception as shown in Figure 7.

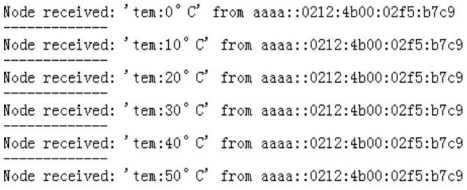

Figure 7. Common nodes receive normal packets

In Figure 8, the IPv6 address of the attack node is b6b4. The topology information is reported to the gateway after the attack beginning.

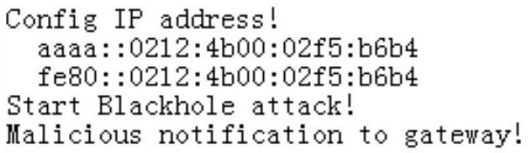

Figure 8. Malicious node attack

After attracting, the new topology shows that node b6b4 attracts the traffic of the neighboring nodes. It status is equivalent to a cluster head node, as shown in Figure 9.

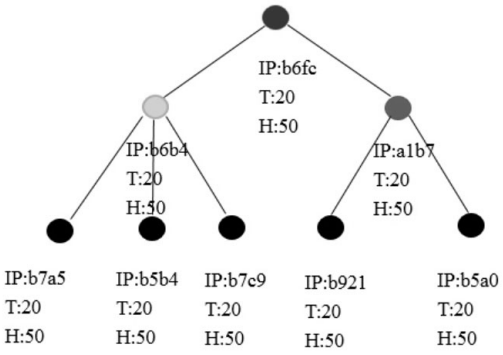

Figure 9. Gateway topology after attack

Common node receives the false control information from the attack node, as shown in Figure 10.

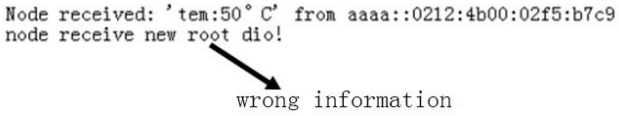

Figure 10. Common node receives wrong information

In this case, using RPL routing protocol, the common node can not receive any packets, because the malicious nodes intercepts all packets, as shown in Figure 11.

```
Malicious notification to gateway!
Something wants to forward through malicous node!Source
IP:aaaa::0212:4b00:02f5:b7c9 send message to Destination
IP:aaaa::0212:4b00:02f5:b7a5The message:
'tem:60° C' drop the message!
Something wants to forward through malicous node!Source
IP:aaaa::0212:4b00:02f5:b7c9 send message to Destination
IP:aaaa::0212:4b00:02f5:b7a5The message:'tem:70° C' drop the message!
Something wants to forward through malicous node!Source
IP:aaaa::0212:4b00:02f5:b7c9 send message to Destination
IP:aaaa::0212:4b00:02f5:b7a5The message:'tem:80° C' drop the message!
```

Figure 11. the malicious nodes received information

But, in this case, using M-RPL routing protocol, the common node can receive all packets, because of the multipath communication, as shown in Figure 12.

```
Node received: 'tem:0° C' from aaaa::0212:4b00:02f5:b7c9
-------------
Node received: 'tem:10° C' from aaaa::0212:4b00:02f5:b7c9
-------------
Node received: 'tem:20° C' from aaaa::0212:4b00:02f5:b7c9
-------------
Node received: 'tem:30° C' from aaaa::0212:4b00:02f5:b7c9
-------------
Node received: 'tem:40° C' from aaaa::0212:4b00:02f5:b7c9
-------------
Node received: 'tem:50° C' from aaaa::0212:4b00:02f5:b7c9
```

Figure 12. Common nodes receive packets after attack

C. *Wormhole attack test*

Node b5b4 is selected as the wormhole node in the same cluster of the data source node, and node a1b7 is selected as another wormhole node in the other cluster. The two node initiate the wormhole attack through the button click, and the wormhole attack process is showed in the monitor.

The wormhole node will attract other nodes within the cluster as their own child-node. A high-speed, direct connection between two wormhole nodes is established. The new network topology is drawn by the topology software. The two lines between node b5b4 and node a1b7 represent the virtual high-speed communication link, and the two malicious nodes can communicate directly and transmit network information to each other, shown in Figure 13.

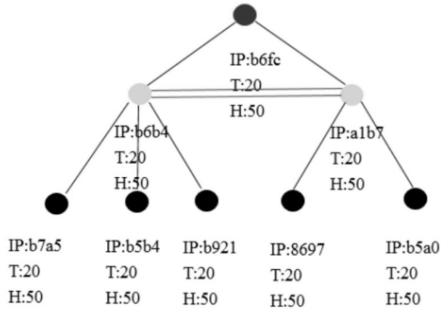

Figure 13. Wormhole attack topology

In this case, using RPL routing protocol, the node b7b0 can not receive any packets from node 85c2, because the malicious nodes intercepts and redirect all packets. But, using M-RPL routing protocol, the node 85c2 can receive all packets from node 85c2, because of the multipath routing.

V. CONCLUSION

This paper studies the security of RPL routing protocol. A hierarchical and clustered multipath secure routing, M-RPL, is proposed. A test network is built to test the performance of M-RPL routing protocol, by which the black hole attack and wormhole attack are simulated. The results show that M-RPL protocol can effectively resist the black hole attack and wormhole attack, offer security and robust data routing.

REFERENCES

[1] T. Winter, P. Thubert, A. Brandt, et al. RPL: IPv6 routing protocol for low-power and lossy networks,RFC6550, s.l.: IETF Mar. 2012. [Online]. Available: http://tools.ietf.org/html/rfc6.

[2] Z. Shelby and C. Bormann, 6LoWPAN: The Wireless Embedded Internet.Torquay, UK: Wiley, John & Sons, 2009.

[3] A. Le, J. Loo, A. Lasebae, A Vinel, et al., "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks," IEEE Sensors Journal,vol 13, no.10 ,pp.3685-3692, June, 2013.

[4] G. H. Lai, "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network," Eurasip Journal on Wireless Communications & Networking, pp. 274, Dec. 2016.

[5] L. Wallgren, S. Raza, T. Voigt,"Routing Attacks and Countermeasures in the RPL-Based Internet of Things,"International Journal of Distributed Sensor Networks,vol 2, pp. 167-174, Jan. 2013.

[6] A. Dvir, T. Holczer, L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, 2011,pp. 709-714.

[7] L. Wallgren, S. Raza, T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," International Journal of Distributed Sensor Networks, vol.2, pp. 167-174, Jan. 2013.

[8] S. Raza, W. Linus ,V. Thiemo, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad hoc networks vol. 11, no.8,pp. 2661-2674, Nov. 2013.

[9] K. Zhang, X. Liang ,R. Lu, et al., "Sybil Attacks and Their Defenses in the Internet of Things," Internet of Things Journal IEEE, vol. 1, no. 5, pp. 372-383, Oct. 2014.

[10] N. Accettura, L. A. Grieco, G. Boggia, et al., "Performance analysis of the RPL Routing Protocol," IEEE International Conference on Mechatronics, Istanbul, 2011, pp. 767-772.

[11] J. Granjal, E. Monteiro, J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol 17, no. 3, pp.1294-1312, Jan. 2015.

[12] P. L. R. Chze,K. S. Leong.A Secure Multi-Hop Routing for IoT Communication. IEEE World Forum Internet Things(WF-IoT), 2014, pp.428–4