Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# ANALYSIS AND COUNTERMEASURES FOR THE SECURITY OF ROUTING PROTOCOL IN PERCEPTION LAYER OF IOTS

[1, 2]WEIDONG FANG, [1]YUN YAN, [1]ZHIDONG SHI

[1] School of Communication and Information Engineering, Shanghai University, Shanghai, 200072, China
[2] Shanghai Institutes of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, 200050, China

## ABSTRACT

The security has always been the eternal topic in the field of Information technology. As a major part of Internet of Things (IoT), the perception layer acts critical roles from cognizing and sensing the ambient world to implement control instructions. So, the security of perception layer is very important. In this paper, a simplified attack detection method is proposed through study of typical routing protocol in the perception layer of IoT. This method, based on attack model, could analyze the security leak of routing protocol in perception layer to a certain extent. We firstly give the background of research of routing protocol, and then propose simplified attack detection method, analyze the security of LEACH protocol, verify Sybil and Hello Flooding attack are major security threats of LEACH protocol. On this basis, we put forward to security countermeasures of routing protocol.

**Keywords:** *Internet of Things (IoT), Perception Layer, Routing Protocol, Security, LEACH*

## 1. INTRODUCTION

In 2005, the Internet of Things' definition: that "The connectivity for anything by embedding short-range mobile transceivers into a wide array of additional gadgets and everybody items, enabling new forms of communication between people and things, and between things themselves." was given by ITU [1]. Actually, through various micro-sensor and MEMS (Micro Electro Mechanical Systems), IoT could sense and collect different information from the ambient world, use embedded technology process and converge it. Through transmission network, this information could be transferred to the user's terminal to complete various applications.

Generally speaking, the universal architecture of IoT is divided into three layers, which includes perception layer, network layer and the application layer (Seeing in figure 1). In short, perception layer mainly collects information and implements instructions, network layer provides a channel for transmitting information, and application layer represents all kinds of terminal user's application. As the source of the information chain, the perception layer acts important roles from cognizing and sensing the ambient world to implement control instructions. In this important role, the transport network of perception layer is the "Core of the Core". Moreover, the routing protocol performance directly influences the accuracy, integrity and real-time of the collected information.

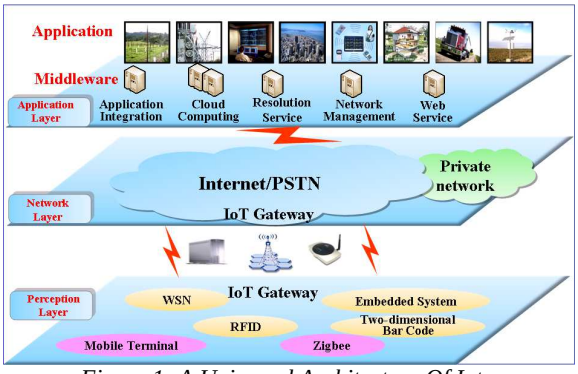


*Figure 1: A Universal Architecture Of Iot*

In contrast to guided media, the wireless medium is openly accessible, less reliable and has no obvious physical boundary for the perception layer. An attacker does not need to break any physical barriers to gain access to the wireless medium and can enter the network from anywhere and from all directions. On the other hand, the limited resources of node determine routing protocol security is not possible using traditional algorithms.

Although many valuable security proposals are put forward in routing protocol of perception layer, these methods just solve one aspect of single protocol, and we believe that the security issues of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

routing protocol are inseparable for scenes and application form. In this paper, we take two typical network (Ad hoc and WSN (wireless sensor network)) of perception layer of layer as examples, analyze the current routing protocols and secure routing protocol, propose simplified attack detection method, give an example about security analysis of LEACH protocol, verify Sybil and Hello Flooding attack are major security threats of LEACH protocol. On this basis, we put forward to security countermeasures of routing protocol.

## 2. BACKGROUND

In contrast to conventional wired networks and cellular wireless network, the networks of the perception layer, especially the Ad hoc and WSN, are built without a fixed infrastructure and centralized management. In this non-centric environment, the routing can be viewed as the processes, which obtain to the network topology information distributed, calculate and maintenance the path through a certain mechanism. So, the functionality of routing protocol mainly includes two aspects:

- To find the optimal path of the source node and the destination node
- Correct forwarding data packets along the optimal path

For the design of routing protocol in perception layer, in addition to the above mentions, energy efficiency and scalability are also considered for first and foremost. This is due to some practical factors, such as energy constraints, limited computing capability and so on. In this section, we will depict the current situation of research on the routing protocol in perception layer.

### 2.1 Routing Protocol in Ad hoc

Any node of Ad hoc network can not cover the entire network area. The node's communication needs to be forwarded through the intermediate node to complete. Node is not only the both sides endpoint of communication, but also the router for forwarding data. When Ad hoc deployment has completed, no centralized management institutions manage the network and its behavior, including addressing and routing. The routing protocol of Ad hoc focuses on the mobility, the variability of network topology and the multi-hop of transmission. According to routing policy, routing protocol is categorized into two classes:

1) Proactive routing protocol,

The existing proactive routing protocols of ad hoc are DSDV (Destination-Sequenced Distance vector), WRP (Wireless Route Protocol), CGSR (Cluster Gateway Switch Routing) and FSR (Fisheye State Routing Protocol) [2-5]. The differences between them are the maintenance number of the routing table and updated ways.

2) Reactive routing protocol,

The reactive routing protocol includes DSR (Dynamic Source Routing), AODV (Ad hoc on Demand Distance vector), TORA (Temporally Ordered Routing Algorithm) [6-8], and so on. The main difference between them lies in the implementation and optimization mechanism of route discovery.

### 2.2 Routing Protocol in WSN

Compared to Ad hoc, the energy supplements and the computing capability are strictly limited. The data is focused on rather than nodes in WSN, so the WSN node address can not be the only. Meanwhile, in order to maximize the WSN coverage and life cycle, WSN generally take intensive deployment. Therefore, the numbers of nodes in the WSN are generally far greater than the number of nodes in the ad Hoc. Ad Hoc network node has an independent address, but WSN has none. WSN routing protocol is based on local topology information, and data-centric

Routing protocols are classified into three categories according to the topology of WSN:

1) Geographic routing protocol,

The typical geographic routing protocol includes: GEAR (Geographic and Energy Aware Routing), GPSR (Greedy Perimeter Stateless Routing), and GPER (Geographic Power Efficient Routing) [9-11].

2) Hierarchical routing protocols

The representations of the hierarchical routing protocol are LEACH (Low-Energy Adaptive Clustering Hierarchy), TEEN (Threshold sensitive Energy Efficient sensor Network protocol) and TTDD (Two-Tier Data Dissemination) [12-14].

3) Data center routing protocols

The SPIN (Sensor Protocol for Information via Negotiation) [15], DD (Directed Diffusion) [16] and Flooding [17] are three mainly types of data center routing protocols

There is a comprehensive evaluation of the routing protocols in table I.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Table 1: Comprehensive Evaluation Of Routing Protocols*

| *Protocol* | *Multi-path* | *Locality-aware* | *Energy-aware* | *Scalability* | *Complexity* | *QoS* | *Data Aggregation* | *Security* |
|---|---|---|---|---|---|---|---|---|
| Flooding | N/A | N/A | N/A | Poor | Simple | No. | N/A | No |
| Gossip | N/A | N/A | N/A | Poor | Simple | No | N/A | No |
| Rumor | N/A | N/A | N/A | Normal | Simple | No | N/A | No |
| SPIN | N/A | N/A | N/A | Normal | Simple | No | N/A | No |
| Directed Diffusion | N/A | N/A | N/A | Good | Simple | No | Support | No |
| LEACH | N/A | N/A | N/A | Good | Complex | No | Support | No |
| TEEN | N/A | N/A | N/A | Poor | Complex | No | N/A | No |
| EAR | N/A | Support | Support | Normal | Simple | No | Support | No |
| GEAR | Support | Support | Support | Good | Simple | No | N/A | No |
| PEGAGIS | N/A | N/A | N/A | Poor | Simple | No | N/A | No |

### 2.3 Secure Routing Protocol

Currently, the secure routing protocol is mainly proposed in Ad hoc network. These protocols are put forward by increasing the security mechanisms in the original protocols, which include SRP (Secure Router Protocol) [18], ARIADNE (A secure On-Demand Routing Protocol for Ad Hoc Networks) [19], ARAN (Authenticated Routing for Ad hoc Networks) [20], SEAD (Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks) [21], SAODV (Secure Ad Hoc On-Demand Distance Vector) [22] and SLSP (Secure Link State Routing for Mobile Ad Hoc Networks) [23]. The comparisons of these secure routing protocols are given in the table II.

Although these secure routing protocols could solve some security issues, they emphasize safety in the design, while ignore availability of algorithm. These secure routing protocols do not adequately taken into account the computing capability constrained battery and limited communication bandwidth of Ad Hoc network, such as ARAN and SAODV. In order to ensure the security, these protocols shield some features of the routing protocols, reducing the effectiveness of the routing protocols such as SRP, ARAN.

*Table 2: Comparisons Of Typical Secure Routing Protocols*

| *Secure Protocol* | *Derivation* | *Protocol Premise* | *Security Technology* | *Authentication* | *Superiority* | *Disadvantage* |
|---|---|---|---|---|---|---|
| SRP | DSR | Established a shared key between he source node and destination node | Message Authenticati on Code (MAC) | Message identification of source and destination address | Algorithm is simple and applicable to a wide range | Lack of protection of route maintenance information, intermediate node can not respond the route request |
| ARAN | AODV/ DSR | Certificate server, publish and maintain public key certificate for each node | Digital Signature | Entire message | Authentication, integrity and non-repudiation | Large computation, need a trusted CA, the intermediate node cannot respond route request |
| SAOD V | AODV | Distributing node's public key | Digital Signature, One-way HASH Chain | Entire message | Intermediate node can respond the route request | Using public key algorithm, large amount of calculation |
| SLSP | ZRP | Distributing node's public key | Digital Signature, One-way HASH Chain | Entire message | Neighbor monitoring mechanism to prevent DoS attacks. | Using public key algorithm, large amount of calculation |
| ARIAD NE | DSR | Released TESLA authentication key, established a shared key between source node and destination node, node clock synchronization | One-way HASH Chain, Message Authenticati on Code (MAC) | Entire message, routing sequence | Symmetric key and TESLA, less computation, simple management | Requirements node clock synchronization, the send authentication key occupied bandwidth, certification delay |
| SEAD | DSDV | Publish certification initial value | One-way HASH Chain | Sequence number, hops | Computationa l load is small | Need a trusted entity to distribute and maintain the each node certification |

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

## 3. SECURITY ANALYSIS

Currently, the method of protocol security analysis is categorized as two broad classes:

• Attack detection method: collect and carry out these effective attack methods for a protocol, individually detect the protocol whether has the ability to defense these attacks. In the process of analysis, natural language and a schematic diagram are used, and the exchanged messages of protocol are analyzed.

• Formal analysis methods [24]: use a variety of formal language or model to build security protocol model, and prove the security of the protocol in accordance with the specified assumptions, verification and analysis. This method is mainly used for the verification of cryptographic protocols and security of electronic transaction protocol.

### 3.1 Definitions

#### 3.3.1 Basic definitions

The Perception layer network is constituted by many independent subjects, which are routers. The subject communication is carried out by transmitted packet, and the relationship between subjects is built by packet. Therefore, the model takes <subject, object relations> as the main element. The subject represents the nodes, and object represents packets. The model is defined as $\{B \times H \times A\}$. The description of symbol is shown in table 3.

*Table 3: Symbles' Description*

| Abbr. | Representation | Abbr. | Representation |
|---|---|---|---|
| $B$ | A subset of $\{S \times T \times R \times O\}$ | $O$ | Object.: packet between nodes, a subset of $\{S_r \times D_e \times T_y \times T_m \times M_s \times TTL\}$ |
| $H$ | Object's Structure, packets' dependency | $Sr$ | Source node address |
| $A$ | Inter-subject's topology | $Sr$ | Destination node address |
| $S$ | Subject:: Attack node (C) , Normal node (N) | $De$ | Broadcast type |
| $T$ | A set of relationship. Time characteristic between the subject and object | $Ty$ | Timestamp or sequence number |
| $R$ | Relationship: operation of the subject to the object, | $Tm$ | Routing information : node address sequence |
| | | $TTL$ | Maximum number of hops |

#### 3.1.2 Symbol definitions

1) $Send(S_i, O_j)$: Node $S_i$ transmits packet $O_j$

2) $\mathrm{Re}cv(S_i, O_j)$: Node $S_i$ receives packet $O_j$

3) $Null(S_i, O_j)$: Node $S_i$ maintains packet $O_j$, expressed as $[X \cdots X1X \cdots X] \xrightarrow{Null} [X \cdots X1X \cdots X]$

*Where 'X' represents the uncertain element value, the same below.*

4) $Modify(S_i, O_j(\ldots))$: Node $S_i$ modifies data packet $O_j$. It is expressed as

$$[X \cdots X1X \cdots X] \xrightarrow{Modify1} \begin{bmatrix} X & \cdots & X & 1 & X & \cdots & X \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}$$

The Modified contents may be any one or a combination among Sr, De, Ty, Tm, Ms and TTL.

5) $Delete(S_i, O_j)$: Node $S_i$ deletes packet $O_j$, expressed as $[X \cdots X1X \cdots X] \xrightarrow{delete} [X \cdots X0X \cdots X]$

6) $Make(S_i, O_j)$: Node $S_i$ makes packet $O_j$, it is expressed as $\xrightarrow{makee} [0 \cdots 010 \cdots 0]$

7) $\mathrm{Re}member(S_i, O_j)$: Node $S_i$ saves data packet $O_j$

$O_i \to O_j$: Packet $O_i$ depends on packet $O_j$.

8) $Fresh(O_j)/No$: timestamp of packet $O_j$ is fresh, then referred to as $Fresh(O_j)$, otherwise $Fresh(O_j)/No$

### 3.2 Rule Descriptions

1) *Rule I:* For normal node $N_i$, $O_j(Ty) \neq Broadcast \wedge N_i \notin Ms \succ Delete(N_i, O_j)$, The symbol "$\succ$" represent "Deduced", the same below

2) *Rule II:* For normal node $N_i$, $O_j(Ty) = Broadcast \wedge N_i \in Ms \succ Delete(N_i, O_j)$

3) *Rule III:* For node $S_i$, $\mathrm{Re}member(S_i, O_j) \succ S_i$ know $O_j$

4) *Rule IV:* For normal node $N_i$, $Verify(N_i, O_j) : No \succ Delete(N_i, O_j)$.

5) *Rule V:* For normal node $N_i$, $Verify(N_i, O_j) : Yes \succ N_i$ believes $O_j$

6) *Rule VI:* For normal node $N_i$, $Fresh(O_j) : No \succ Delete(N_i, O_j)$

### 3.3 Attack Behavior Model

According to the above definition, we would analyze the behavior of the node and known attack methods, and draw the following six kinds of attack behavior models.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1) Interrupting

$\mathrm{Re}\,cv(C_i, O_j)$;

$Delete(C_i, O_j)$;

When an adversary node receives a packet, the node does not forward it in accordance with the requirements of the routing protocol, but interrupt the transmission of the packet. It is generally called passive denial of service.

2) Modifying

$\mathrm{Re}\,cv(C_i, O_j)$;

$Modify(C_i, O_j(\ldots))$

$Send(C_i, O_j)$;

When a malicious node receives a packet, it modifies the contents of the packet, and then forwarded it. This behavior leads normal node receives error information.

3) Spoofing

$\mathrm{Re}\,cv(C_i, O_j)$;

$Null(C_i, O_j)$

$Send(C_i, O_j)$;

When an adversary node receives a packet, the node forwards directly without any modification, hide itself address. It generally lead the normal node mistaken there is a connection with other normal nodes.

4) Replaying

$\mathrm{Re}\,cv(C_i, O_j)$;

$O_i \rightarrow O_j : Send(C_i, O_j)$;

When a malicious node receives a packet, it sends a response packet due to the dependencies relationship of packet. This behavior would result in a wrong direction of the route. It is generally called a black hole attack.

5) Flooding

$Make(C_i, O_j) : O_j(Ty) = Broadcast$;

$Send(C_i, O_j)$

An adversary node transmits initiatively packets. If a great number of packets are sent in a short period of time, the normal node's buffer would overflow. It is generally called the Active Denial Service attacks.

6) Tampering

$C_j, Knows\ \ O_j : Modify(C_i, O_j(Tm))$

$Send(C_i, O_j)$

If the timestamp or sequence number is designed in routing protocol, an adversary could use this way to deceive the normal node. The adversary node sends outdated routing information. This behavior would cause normal nodes send packets according to the out-of-date routing information.

### 3.4 Routing Protocol Security Analysis

LEACH is the first hierarchical routing protocol in WSN. This hierarchical routing protocols that compares with single-layer routing protocol has better scalability, the convenience of data fusion, lower power consumption. So, we will analysis for the security of LEACH under above attack models.

#### 3.4.1 Under 'Interrupting' model

Assuming that the attack node is the 'm + n', others are normal nodes (below).

$$[X \cdots X1X \cdots X] \xrightarrow{delete} [X \cdots X0X \cdots X]$$

1) If $O_j(Ty) = Broadcast$

After *rule VI* was carried out, if the front 'm + n - 1' elements are 0, then the attack node is the only path of the source and the destination node is shown During the network topology does not change, the source and the destination node can not communicate; If the front 'm + n - 1' elements are not all 0, the network topology may lead to increase the number of destination node hop. If it exceeds $O_j(TTL)$, the destination node is unreachable.

2) If $O_j(Ty) \neq Broadcast$

The node $S_i$ that belongs to

$O_j(Ms) = \{N_1, N_2 \cdots N_n\}\ \mathrm{Re}\,cv(N_i, O_j)$.

The transmission of $O_j$ has no influence.

#### 3.4.2 Under 'Modifying' model

$$[X \cdots X1X \cdots X] \xrightarrow{Modify1} \begin{bmatrix} X & \cdots & X & 1 & X & \cdots & X \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}$$

The normal node Ni receives a packet $O_j$, then

$Verify(N_i, O_j)$

If the packet is error, then $N_i$ discusses it. The network has no influence. Otherwise, normal node will believe it is a legitimate packet, and continue to transmit it. But in the end to the Cluster head or sink, this attack will cause a portion of the data can not be identified, and be discarded eventually

#### 3.4.3 Under 'Spoofing' model

This attack mode does not affect the transmission of the corresponding packets. But, the information

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

in the packet is not integral. This normal node performs Remember, and then obtains a wrong path. Otherwise, it does not affect network traffic.

### 3.4.4 Under 'Replaying' model

$O_i \to O_j$ ;

$$[X \cdots X1X \cdots X] \xrightarrow{Modifyl} \begin{bmatrix} X & \cdots & X & 1 & X & \cdots & X \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix}$$

Because the routing information 'Ms' has be known, the malicious packet preceding the normal reply packet reaches the source node for packet $O_j$, so that the source node selection by $C_i$ path as the path to the destination node. LEACH can not do anything, because it does not verify the legitimacy of the routing information source.

### 3.4.5 Under 'Flooding' model

$$\xrightarrow{makee} [0 \cdots 010 \cdots 0]$$

When the 'Flooding' model was carried out by an attack node $C_i$, if $C_i$ only sends a small number of packets, the network will not have a big impact. A large number of packets are transmitted in a short period of time. The normal node resources are occupied. At last, the buffers of normal nodes overflow. LEACH has no any measures to defense this attack. A typical attack is "Hello Flooding".

### 3.4.6 Under 'Tampering' model

The routing protocol has the operation of timestamp or serial number. The adversary node chooses an operating $Modify(C_i, O_j(Tm))$, in order to ensure the freshness of the message. The normal node $N_j$ checks packets $Fresh(O_j): No$ , and then $Delete(C_i, O_j)$ according to *Rule VI*, has no influence, or else, believe $O_j$ according to *Rule V*.

On the other hand, the decision based on the timing is just not enough. If a malicious node tampers with itself role, or participates in the cluster head competition, LEACH protocol has no good ideas. It is why Sybil attack is one of greater harm for the hierarchical structure of WSN.

In summing up, we can see that there are no any security considerations in LEACH protocol from the above analysis. The six attack model, especially 'Flooding' and "Tampering" make the LEACH protocol great harmful. It also is reason that the Sybil and "Hello Flooding" attack become the hotspots of security research on LEACH [25].

## 4. COUNTERMEASURES

The diversity of applications and scenarios decides that a single way could not solve the security issues of routing protocol. So, the solutions of these security issues need combine the particular scenario and routing protocols, take targeted security schemes. These schemes should either optimize from protocol itself, or enforce the key management mechanisms. Below we will propose some general methods to guide and develop the routing protocol security countermeasures.

### 4.1 Existing Routing Protocol Extensions

1) Routing Protocol Extensions and Revision

Currently, in the design of the secure routing protocol, some minor modifications were taken to achieve security goal, Such as SRD etc. On the other hand, many attacks are launched based on routing competitive conditions. When the routing need be chosen, we avoid a variety of competitive conditions. Some attack would be prevented.

2) Symmetric Cryptography Mechanism in route discovery and routing packets certification

Because resources consume so much, asymmetric cryptographic scheme should not be used in transmission of perception layer. Some methods, such as the Password MAC of SPINS and INSENS, one-way hash function and one-way authentication scheme, are worth learning. These methods are also to achieve broadcast or multicast certified. However, if using a single encryption does not meet demand, the combined use of the symmetric key algorithm and public key of the key technology could be considered to reduce the amount of computation, without lowering the security strength of the premise.

### 4.2 Hybrid Security Mechanism

The computing capability of single node is so limited that some complex security routing algorithms are not implemented. In response to this situation, some auxiliary information, which includes the node group, PHY and location, should be considered to meet with the certification management and key management.

1) Secure localization technology

Secure localization includes two aspects:

- A node could determine itself precise geographical coordinates;
- A malicious node could not masquerade as spurious location.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The localization technology is applied in the security defense to implement routing certification. In conjunction with other security technology, this technology will improve the security of routing. With secure positioning capability, the routing protocols can effectively solve the problem, such as wormhole attacks and Sybil attack.

2) Intrusion Tolerance Technology

Due to the vulnerability of the security, the intrusion tolerant technology should be taken to mitigate the destructed scope of intruders. Redundant multi-path routing algorithm is a typical representative of the intrusion tolerance, redundancy-based defense measures applicable to WSN. Its ability could tolerate failure and intrusion.

3) Defense against Node Capture Attack

Because multiple nodes perceive an object together, the finite nodes were even captured, at the initial stage; the overall operation of the network is not affected. The key issue is that the adversary could not crack and steal important information from the captured nodes. The better approach is dynamic call of the code, in other words, the core codes do not boot from the memory, but dynamically load to the node at the beginning of the deployment. In addition, other mechanisms can be considered. For example, nodes could execute self-destruct code in the case of non-normal startup.

### 4.3 Anonymous Technology

The existence of active attacks causes a great deal of security threats to the networks of perception layer. So, we should use anonymous technologies to prevent passive attacker detecting network topology and critical node.

1) Hidden Node Attributes

The pseudo identity is taken to hide the true identity, as well as nodes communicate each other by using the pseudo identity instead of the true identity, change the pseudo-identity regularly or irregularly rather than hide their identity through encryption node identity.. This way will greatly increase the computational overhead of the intermediate forwarding node and the destination node for such passive attackers. Those malicious nodes that are deployed by the passive attacker have to try all possible shared keys to decrypt the message packet to determine that they are not the destination node or forwarding node.

2) Light Onion Routing

The Onion Routing mechanism is that selects of some intermediate targets to compose a multi - segment path, and encrypts the data and address of the posterior path packet as the preceding path packets to transmit. The destination node address is hidden away. Thereby, the multi-grade confusion concealed path is obtained. The data packet uses different encryption keys from back to front and layer by layer so that the target node that receives this packet could only decrypt the outermost layer in figure 2 [26]. Each node to forward this package only knows two adjacent, so an attacker cannot obtain the entire path more information.

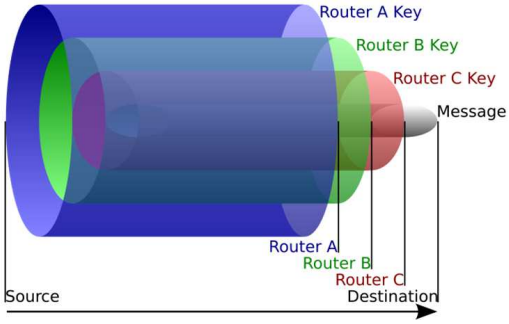


*Figure 2: Onion Routing Diagram*

Of course, onion routing protocol that is implemented on the networks of perception layer need be lightly processed. In general, we take the hash and the exclusive OR operation to achieve onion-layered blinded data, in order to reduce the resource of the capacity and computation.

3) Avoid the use of obfuscation techniques

We should avoid wholly using these obfuscation techniques, such as selective packet reorganization, padding, delay, traffic temptation and etc. The reorganization requires the intermediate node must know the whole path structure, and then can be resorted. So, the flexibility of the routing algorithm is not high, and the energy consumption increases. The padding will increase the load on the wireless link. The delay could prevent adversary track, but may also provide time for an attacker. The traffic temptation makes the network energy consumption excessive. The design of security can selectively use the techniques above.

## 5. CONCLUSION

Although many routing protocols have been designed, the goal of these protocols seldom aims at security. On the other hand, many research focus on security of routing protocol in WSN or Ad hoc, but many of them elevate security by abandoning the performance. The diversity of scenario and application determine any solo solution could meet the demand of routing protocol security.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In this paper, we propose a simplified attack detection method to check the security leak of routing protocol, and then give the analysis process with LEACH protocol. At the same time, we put forward some security countermeasures, which are common suggestions to solve issues of protocol security. Among them, the hybrid security mechanism is research hotspot in the future.

## ACKNOWLEDGMENT

This work is partially supported by the National Science and Technology Major Project of China (2011ZX03005-002) and the Equipment Functional Development of Technological Innovation Projects from CAS (YG2010060)

## REFRENCES:

[1] International Telecommunication Union (IUT), ITU Internet Reports 2005: The Internet of Things, 2005

[2] C. E. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In ACMSIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, London, England, 1994.8: pp: 234~244..

[3] S. Murthy and J. J. Garcia-Luna-Aceves. An Efficient Routing Protocol for Wireless Networks. ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, 1996, l(2). pp: 183-197.

[4] C-C. Chiang, H. K. Wu, W. Liu and M. Gerla. Routing in Clustered Multi-hop Mobile Wireless Networks with Fading Channel. Proceedings of IEEE SICON'97, 1997.4 pp:197-211.

[5] G. Pei, M. Gerla and T-W. Chen. Fisheye State Routing: A Routing Seheme for Ad hoc Wireless Networks. In Proceedings of IEEE/ ICC'00, 2000.6.

[6] D. Johnson and D. MaltZ. Dynamic Source Routing in Ad hoc Wireless Networks. Mobile Computing, 1996, Ch.5, pp: 53-81.

[7] C. E. Perkins, E. M. Royer and S. R. Das, Ad hoc on-demand distance vector (AODV) routing. IETF Internet Draft. 2001. http://www.ietf.org/internet-drafts/draft-ietf-manetaody-08-txt.

[8] Z. J. Haas and M. R. Pearlman. The Zone Routing Protocol (ZRP) for Ad hoc networks. Internet Draft hdraft-haaszone-routing-protocol-00.txti, 1997, pp: 153-181.

[9] Y, Yu, D, Estrin nad R. Govindan. Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks. UCLA Computer Science Department Technical Report, UCLA-CSD TR-O1-0023, 2001, pp: 1-11

[10] S. B. Wu and K. S. Candan. GPER: Geographic Power Efficient Routing in Sensor Networks. In Proceedings of 12th IEEE International Conference on Network Protocols (ICNP'04), 2004, pp: 161-172.

[11] B. Karp and H. T. Kung. GPSR: Greedy perimeter stateless routing for wireless sensor networks, In Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Boston, MA. 2000, pp: 243-254.

[12] W Heinzelman, A. Chandrakasan and H. Balakrishnan. Energy-Efficient Communication Protocol for Wireless Micro-sensor Networks. In Proceedings of the 33 Hawaii International Conference on System Sciences.2000, pp:223.

[13] A. Manjeshwar and D. P. Agarwa. TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks. The 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing.2001, pp: 2009-2015.

[14] F. Ye, H. Luo, J. Cheng, S. Lu and L. Zhang. A two-tier data dissemination model for large-scale wireless sensor networks. In Proceeding of the ACM Conference. on Mobile Computing and Networking, 2002, pp: 148-159.

[15] W. R. Heinzelman, J. Kulik and H. Balakrishnan. Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, In Proceeding of the 5th ACM/IEEE Mobicom Conference (MobiCom1999), Seattle, WA, August, 1999, pp: 174-185.

[16] C Intanagonwiwat, R Govindan and D Estrin. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. In Proceedings of ACM MOBICO'00, 2000, pp: 56-67.

[17] S. Hedetniemi, S. Hedetniemi and A.Liestman. A Survey of Gossiping and Broadcasting in Communication Networks. Networks, 1988(18) pp: 319–349

[18] P. Papadimitratos and Z. Haas, Secure routing for mobile Ad Hoc networks, In Proeeedings of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, January 27-31, 2002.

[19] D. B. Johnson, D. A. Maltz and etc. The Dynamic Source Routing Mobile Ad Hoc Networks (DSR), INTERNET-DRAFT, draft-ietf-manet-dsr-10.txt, Protocol for July 2004.

[20] K. Sanzgiri, B. Dahill , B.N. Levine, C. Shields, E. M. Belding-Royer. A Secure Routing Protocol for Ad Hoc Network. In Proceedings of IEEE International Conference on Network Protocols (ICNP), November, 2002.

[21] Y. C. Hu, D. B. Johnson and A. Petrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In Proceedings of the 4th IEEE workshop on Mobile Computing Systems & Applications (WMCSA2002), Calicoon, NY, June, 2002, pp: 3-13.

[22] M. G. Zapata, Secure Ad Hoc On-Demand Distance Vector Routing. ACM Mobile Computing and Communications Review, Vol6, No.3, 2002, pp: 146-107.

[23] P. Papadimitratos and Z. J. Haas, Secure Link State Routing for Mobile Ad Hoc Networks, IEEE W6rkshop on Security and Assurance in Ad Hoc Networks, Orlando, FL, January, 28, 2003.

[24] D. E. Bell and L. J. LaPadula . Secure Computer System : Unified Exposition and Multics Interpretation. Tech Report MTR-2997, The MITRE Corporation, Bedford, MA, 1975-07.

[25] S. S. Chen, G. Yang and etc.. LEACH protocol based security mechanism for Sybil attack detection. Journal on Communications, Vol. 32, No. 8, 2011, pp: 143-149

[26] http://en.wikipedia.org/wiki/Onion_routing