Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 596352, 13 pages
http://dx.doi.org/10.1155/2013/596352

Research Article

Load-Balanced Secure Routing Protocol for Wireless Sensor Networks

Wang Xin-sheng,[1] Zhan Yong-zhao,[1] and Wang Liang-min[2]

[1] *School of Computer Science and Telecommunication Engineering, Jiangsu University, China*
[2] *Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University, China*

Correspondence should be addressed to Wang Xin-sheng; wxs@ujs.edu.cn

Received 28 February 2013; Accepted 28 May 2013

Academic Editor: Lu Liu

To solve the problems of limited energy of the nodes and security of routing in wireless sensor networks, load-balanced secure routing protocol (LSRP), a load-balanced secure routing protocol for wireless sensor networks, is proposed. Based on structured topology of hexagonal mesh, hops at different directions are calculated on the optimal route for transmitting data packets in LSRP. Depending on characters of hops, the nodes can rapidly find a route among multiple optimal routes by the policy of the twice probability routing selection. Data breach is prevented by data encryption, and data security is realized by one-way hash key chain and symmetric key authentication. LSRP offers preventions against usual attacks, and it also takes into account traffic load balance. Analysis and simulation results show that LSRP has better performance on traffic load balance and security.

1. Introduction

As a convenient tool to capture information, wireless sensor networks can access information in fields that are beyond the arm of flesh. Special fields of application such as military and antiterrorism require security of sensitive data, which arouses scholars' attention on the security of wireless sensor networks [1, 2]. However, complex security measures based on cryptography are inapplicable owing to the calculation and storage capability of the nodes of wireless sensor networks. Open wireless communications means with limited band width facilitate attacks such as eavesdropping and DoS. The multihop transmission and self-organization approach causes deficiency of key infrastructure and possibility of malicious nodes to mix in the network to implement insider attack. All of these problems pose a greater security challenge to wireless sensor networks than traditional network [3].

The discovery of self-organizing routing, the approach of multihop data forwarding, and the mode of open wireless communication pose two threats to routing security in wireless sensor networks [4]: on one hand, there might be potential threats to security in the course of packet transmission, such as eavesdropping, altering, and discarding, which will result in breach, inauthenticity or loss of the content; on the other hand, the attackers might manipulate the packets on communication links to attack the network through routing and cause performance deterioration or even breakdown of the network. This makes routing security an important subject in studies about the security of wireless sensor networks. A series of secure routing protocols have been proposed against various kinds of routing attacks. For example, GPSR [5] can detect black hole regions through periodic broadcast probe request and effectively detect and counteract sinkhole attack and wormholes attack. SRWA [6] uses mobile agent to reduce false positive to defense wormholes attack. SeRWA [7] protocol uses symmetric key cryptography to defense wormhole attack and can find a secure route against a wormhole attack. SPINS [8] can realize authentication, encryption and refreshing of data and authentication of broadcast packets under the condition of limited resources, and effectively detect and counteract data eavesdropping, altering, and replay attacks. EENDMRP [9] uses the multiple paths and digital signature crypto system to transmitted data packets and effectively prevent selective forwarding, sinkhole, and altering attacks. By importing tokens, SRD [10] can detect and prevent acknowledgement

spoofing and false routing information attack. SDDR [11] uses the μTESLA (microtimed, efficient, streaming, loss-tolerant authentication) algorithm in order to prevent black hole and acknowledgement spoofing attacks. INSENS [12] and TRANS [13] adopt measures like link-layer encryption and authentication, multipath routing, identity authentication, two-way connection authentication, and authentication broadcast to effectively prevent false routing information, Sybil attack, and HELLO FLOOD attack. ATSR [14] uses accurate location information to implement a distributed trust model to prevent selective forwarding and Sybil attacks. Multipath and multibase station routing [15] can effectively prevent HELLO FLOOD attack and replay attack through the key and one-way hash key chain assigned by multitree key protocol. Multipath routing [16, 17] can effectively prevent particular attacks with the feature of attracting all traffic to pass the malicious nodes, such as wormhole, sinkhole, and selective forwarding attacks. By checking the credit of the nodes, ARRIVE [18] can effectively prevent selective forwarding attack. However, these algorithms and protocols are mainly targeted at one or several types of attacks and have disadvantages in excessively large load of calculation and communication.

Taking both security and energy saving into consideration so as to extend the service life of the network is still a burning problem. By combining topology generation and routing discovery, this paper reduces the complexity of routing discovery by combine topology generation and routing discovery, based on this, puts forward a secure routing protocol based on the twice probability routing selection, LSRP (load-balanced secure routing protocol). LSRP realizes routing security by one-way hash key chain and symmetric key cryptography and balances network load through optimizing routing to extend the service life of the network. Section 2 elaborates the routing protocol LSRP. Section 3 analyzes the security of LSRP and makes comparison with relevant tasks. Section 4 gives demonstration through simulation.

2. Load-Balanced Secure Routing Protocol (LSRP)

Topology control can effectively reduce energy consumption of wireless sensor network [19]. The literatures [20–23] reach the conclusion after analysis and comparison that hexagonal mesh structure can use redundant nodes to store energy and as a result has prominent advantage in effectively lengthening the service life of the network. Meanwhile, regular-shaped topology also provides applicable rules for route discovery and positioning of malicious nodes. On the basis of the approach stated in the literature [15], this section adds security design and puts into effect a secure way to generate hexagonal mesh topology, and then secure routing protocol LSRP is set up on this topology. LSRP realizes routing discovery and selection, data packet transmission and security authentication, and defense against routing attack.

2.1. Generation of Network Topology. Sensor nodes are deployed to the detected region by scattering. Before that, symmetric key K_a corresponding to the base station and temporary shared symmetric key K_{temp} are saved at each node. The latter one will be deleted after the node completes topology construction. Upon being scattered to the target region, nodes form a structured network topology made up of the same hexagonal cell in logic by broadcast communication. Formation of the topology includes four phases as follows.

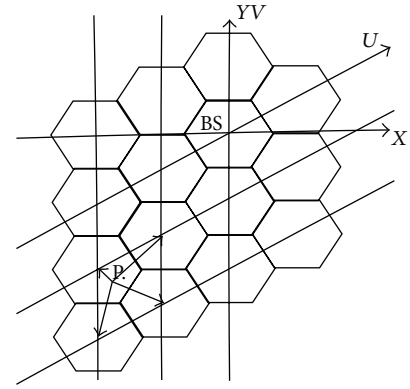


Figure 1: Calculate the ID of the RC of node P.

(1) Node initialization. In this phase, nodes acquire own and neighbors' locations. The node obtains the respective position (x, y) through GPS, then broadcasts Hello packet $((x, y), \text{MAC}_{K_{\text{temp}}}((x, y)))$ at a distance of $2a$. a is the side length of the regular hexagonal cell (shortened as RC) while $\text{MAC}_{K_{\text{temp}}}((x, y))$ is the message authentication code generated by using K_{temp} for verifying the authenticity of (x, y). The node receives Hello packet and verifies the authenticity of (x, y) through K_{temp} and $\text{MAC}_{K_{\text{temp}}}((x, y))$. After Hello packet passes authentication, the node saves the position information of neighboring nodes.

(2) Cell partition. In this phase, nodes determine which RC they affiliate to. BS broadcasts partitioning message which contains the location of BS and a. To facilitate easier notations, we introduce set of coordinates (u, v) where the V-axis coincides with the Y-axis, and U-axis is 30 degrees tilted counterclockwise from the X-axis. The (u, v) coordinates of RC center are referred to as the ID of RC. Once node P receives the partitioning message, it calculates the IDs of the four adjacent RCs, as shown in Figure 1. P then calculates the distances between itself and these RCs' centers and adapts the ID of the RC whose center is closest to it.

(3) Active node election. In this phase, active node is picked out according to the following rules: assuming G is a node coordinates set in an RC, one node whose coordinate is $\text{Min}_G\ (x, y)$ is picked out. This is the active node of the RC it belongs to. $\text{Min}_G\ (x, y)$ is defined as below: set G as the node's coordinate set; $(x, y) \in G$; any (x_0, y_0) meets the criteria of $(x_0, y_0) \in G$ and is different from (x, y); if (x, y) meets the criteria: $x < x_0$ or $x = x_0$ and $y < y_0$, then (x, y) is the minimum coordinate of G, written as $\text{Min}_G\ (x, y)$. All other nodes then enter into sleep state. Sleep node periodically sends an inquiring message to the active node, and the active node either keeps it asleep or lets it become new active node to continue its work.

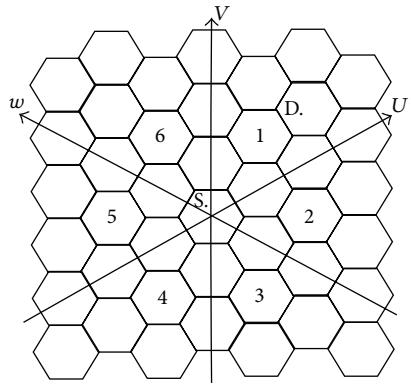


Figure 2: U, V coordinate system.

(4) Secure architecture construction. In this phase, secure architecture is constructed, that is, the communication relations are set up between RCs. Each RC's active node broadcasts request packet $((u, v), \mathrm{MAC}_{K_{\mathrm{temp}}}((u, v)))$. (u, v) is the coordinate of the node sending request packet. The active node receives request packet and verifies its facticity. Then, according to (u, v) and the node's own coordinate, the active node will be able to determine whether the node sending packet is the active node of the neighboring RC. If it is, add it to the table of neighboring RCs.

2.2. Routing Discovery and Selection. According to the fact that LSRP is based on hexagonal mesh topology, a routing discovery and selection method is designed.

The main idea of the method is as follows. First of all, calculate the number of hops in U, V, and W directions from the source node to the destination node. Then, choose the transmission routing according to the policy of the twice probability routing selection, that is, according to certain probability, choose a direction R_1 among U, V, and W, and randomly generate the number of continuous hops, T_1, in R_1 direction according to certain probability rules by referring to the total number of hops in R_1 direction and that of other directions. The packet will take T_1 hops continuously along R_1 direction. If there are unfinished hops along other directions, choose another direction R_2 according to certain rules. If there are T_2 hops along R_2 direction, take T_2 hops continuously along R_2 direction. And the like, until it comes to the destination node.

The detail of routing discovery and selection is as follows.

2.2.1. Routing Discovery. As shown in Figure 2, routing discovery is to calculate the number of hops along the shortest path from S to D, that is, u, v, w (u denotes u hops in direction U. v denotes v hops in direction V. w denotes w hops in direction W). Among u, v, w, at least one is equal to 0.

According to the above result, we designed Algorithm 1 to calculate the initial values of u, v, and w. In OPA_uvw algorithm, the case that two out of three directions of hops are zero is considered, which states that only one optimal path between source node and destination node. For the case, u, v, and w are updated, and two new paths whose hops are one more than that of the optimal path are added for improving performance on traffic load balance.

2.2.2. Routing Selection. According to the type of node, routing selection is divided into the following two types.

(1) Source Node Routing Selection. After source node S monitor one event, it needs to select one path in advance to transmit the event message to destination node D, that is, it needs to determine routing information (u, v, w, t, s) and routing direction. t denotes direction of packet forwarding for next hop node. s denotes hops in direction t. According to characters of u, v, and w, OPA_$uvwts$ algorithm for the twice probability routing selection to calculate the values of routing information is designed as shown in Algorithm 2.

(2) Intermediate Node Routing Selection. After intermediate node has received the data packet, it needs to determine next hop routing information (u, v, w, t, s) and direction. According to routing information (u, v, w, t, s) in the data packet, update_$uvwts$ algorithm is designed for computing next hop routing information and direction as shown in Algorithm 3.

2.3. Data Packet Transmission. Data packet is forwarded according to the routing computed by above routing algorithm. In order to strengthen security, acknowledgement packet, alert packet, and notice packet are additionally introduced in LSRP. Acknowledgement packet is for detect selective forwarding attack. Alert packet is for transmitting alert message containing the position of the attackers to the source node. Notice packet is for transmitting message of attack existence in the path to the source node.

The routing transmission of different types of packets is shown in Figure 3.

The realization process of the data packet transmission is as below.

Set S as the source node, B as the intermediate node, and D as the destination node.

Step 1. S: generate ($\mathrm{encry}_{\mathrm{data}}$, $\mathrm{MAC}_{\mathrm{SD}}(\mathrm{encry}_{\mathrm{data}})$, $\mathrm{MAC}_{\mathrm{OHK}}(\mathrm{counter})$, $\mathrm{routing}_{uvwts}$, direction).

Step 2. S $\rightarrow$ B: {$\mathrm{routing}_{uvwts}$, $\mathrm{encry}_{\mathrm{data}}$, counter, $\mathrm{MAC}_{\mathrm{SD}}(\mathrm{encry}_{\mathrm{data}})$, $\mathrm{MAC}_{\mathrm{OHK}}(\mathrm{counter})$}.

Step 3. B: verify_cout(counter), update_$uvwts$ ($\mathrm{routing}_{uvwts}$).

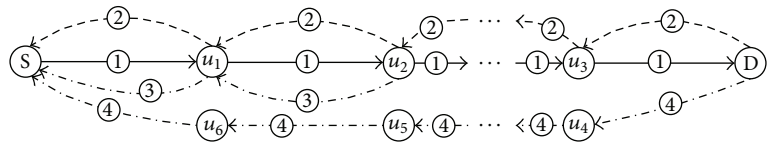
Step 4. B $\rightarrow$ B: {$\mathrm{routing}_{uvwts}$, $\mathrm{encry}_{\mathrm{data}}$, counter, $\mathrm{MAC}_{\mathrm{SD}}(\mathrm{encry}_{\mathrm{data}})$, $\mathrm{MAC}_{\mathrm{OHK}}(\mathrm{counter})$}.

Step 5. B $\rightarrow$ D: {$\mathrm{routing}_{uvwts}$, $\mathrm{encry}_{\mathrm{data}}$, counter, $\mathrm{MAC}_{\mathrm{SD}}(\mathrm{encry}_{\mathrm{data}})$, $\mathrm{MAC}_{\mathrm{OHK}}(\mathrm{counter})$}.

Step 6. D: verify_cout(counter), verify_MAC ($\mathrm{encry}_{\mathrm{data}}$), decrypt($\mathrm{encry}_{\mathrm{data}}$), judge_attack().

Detailed descriptions about the data packet transmission are given below.

Step 1. The source node S constructs the data packet shown in Figure 4. The routing information (u, v, w, t, s) and



① Data packet transmission
② Acknowledgement packet transmission
③ Alert packet transmission
④ Notice packet transmission
S: Source node sending data packet
D: Destination node receiving data packet
u_1, u_2, u_3: intermediate nodes sending data, alert, and acknowledgement packets or generating alert packet and acknowledgement packet
u_4, u_5, u_6: intermediate nodes sending notice packet

Figure 3: Routing transmission of different types of packets.

Input: source node S (u_s, v_s), destination node D (U_d, V_d)
$u_D = u_d - u_s$; $v_D = v_d - v_s$;
neither of u_D and v_D is 0
{if u_D and v_D have opposite signs,
{if $|u_D| > |v_D|$, then $(u, v, w) = (u_D + v_D, 0, v_D)$
if $|u_D| < |v_D|$, then $(u, v, w) = (0, v_D + u_D, u_D)$
if $|u_D| = |v_D|$
{$w = v_D$
//convert one-way path to multi-way path; sign (x) means the sign of x
if $|w| > 1$, then $(u, v, w) = (\text{sign}(w)(-1), \text{sign}(w)(1), \text{sign}(w)(|w| - 1))$
if $|w| = 1$, then $(u, v, w) = (0, 0, v_D)$}}
if u_D and v_D have the same sign, then $(u, v, w) = (u_D, v_D, 0)$}
if one between u_D and v_D is 0 and the one not equal to 0 is larger than 1
{ //convert one-way path with number of hops over 1 to multi-way path
if $|v_D| > 1$, then $(u, v, w) = (\text{sign}(v_D)(1), \text{sign}(v_D)(|v_D| - 1), \text{sign}(v_D)(1))$
if $|u_D| > 1$, then $(u, v, w) = (\text{sign}(u_D)(|u_D| - 1), \text{sign}(u_D)(1), \text{sign}(u_D)(-1))$}
if between u_D and v_D, one is 0 and the other is equal to 1, then $(u,v,w) = (u_D, v_D, 0)$
Output: (u, v, w)

Algorithm 1: OPA_*uvw*.

Input: (u, v, w)
if one among u, v, w is 0, set $w = 0$ (similar treatment in the case of $u = 0$ or $v = 0$)
{the active node randomly chooses one direction in U and V by the principle of equal probability,
supposing U direction is chosen (similar treatment for V direction)
direction = sign(u)
//t takes value 1, 2, 3, standing for U, V, W direction respectively
if $|v| = 1$, then $(u, v, w, t, s) = (\text{sign}(u)(|u| - 1), v, w, \text{sign}(u)(1), (|u| - 1))$
if $|v| \neq 1$
{ randomly select a figure $u1$ among $1 \sim |u|$ by the principle of equal probability,
if $u1 > 1$, then $(u, v, w, t, s) = (\text{sign}(u)(|u| - 1), v, w, \text{sign}(u)(1), (u1 - 1))$
if $u1 = 1$, then $(u, v, w, t, s) = (\text{sign}(u)(|u| - 1), v, w, \text{sign}(v)(2), |v| - 1)$}}
if none among u, v, w is 0
{choose one direction randomly in U, V *and* W by the principle of equal probability
supposing U direction is chosen (similar treatment for V or W direction)
direction = sign(u)
if $u \cdot v < 0$ and $v \cdot w > 0$, then $(u, v, w, t, s) = (0, v, w, \text{sign}(w)(3), |w|)$
if $u \cdot v > 0$ and $v \cdot w > 0$, then $(u, v, w, t, s) = (0, v, w, \text{sign}(v)(2), |v|)$
if $u \cdot v > 0$ and $v \cdot w < 0$, then $(u, v, w, t, s) = (u, 0, 0, \text{sign}(u)(1), |u|)$}
Output: (u, v, w, t, s) and direction

Algorithm 2: OPA_*uvwts*.

Input: (u, v, w, t, s)
Assuming t is U direction (For V or W direction similarly processing)
if next hop node in t direction is normal node
{ direction = sign(u)
If $s > 1$, then $(u, v, w, t, s) = (\text{sign}(u)(|u| - 1), v, w, t, (s - 1))$
If $s = 1, v \neq 0$, then $(u, v, w, t, s) = (\text{sign}(u)(|u| - 1), v, w, \text{sign}(v)(2), |v|)$
If $s = 1, w \neq 0$, then $(u, v, w, t, s) = (\text{sign}(u)(|u| - 1), v, w, \text{sign}(w)(3), |w|)$
If $s = 1, v = 0, w = 0$, then $(u, v, w, t, s) = (0, 0, 0, 0, 0)$;
If $s = 0$, it means that event packet reaches destination node }
if next hop node in t direction has been marked with failure node
{ if $v \neq 0$, then $\{(u, v, w, t, s) = (\text{sign}(u)(|u| + 1), \text{sign}(v)(|v| - 1), w, t, s + 1)$,
direction = sign(v)(2)}
if $w \neq 0$, then $\{(u, v, w, t, s) = (\text{sign}(u)(|u| + 1), v, \text{sign}(w)(|w| - 1), t, s + 1)$,
direction = sign(w)(3)}
if $v = 0, w = 0$, then $\{(u, v, w, t, s) = (u, 0, \text{sign}(u)(-1), t, s)$,
direction = sign(u)(2)}}
Output: (u, v, w, t, s) and direction

Algorithm 3: update_$uvwts$.

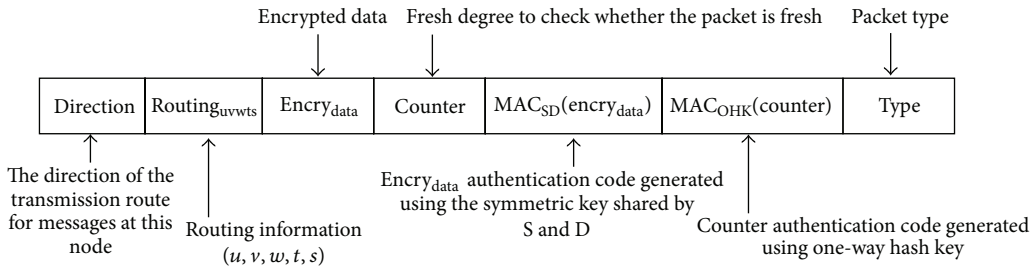


Figure 4: Format of data packet.

transmission direction can be got by OPA_uvw algorithm and OPA_$uvwts$ algorithm (see Algorithms 1 and 2).

Step 2. S sends the data packet to the intermediate node at next hop.

Step 3. The intermediate node receives the data packet, firstly verifies the fresh degree of the packet via counter, and then according to the received (u, v, w, t, s) and above update_$uvwts$ algorithm it calculates the routing$_{uvwts}$ and direction from the intermediate node to the destination node D.

Step 4. The intermediate node sends the data packet to the neighboring downstream intermediate node along the transmission direction outputted in Step 3. Next, it does the following operations.

(1) If it is the node that generates acknowledgement packet, it constructs the acknowledgement packet shown in Figure 5.

$K_{i,j,}$ the current one-way hash key used in MAC$_{OHK}$ (ACK) is calculated by

$$K_{i,j} = F^{N_t - \text{int}((T_c - T_b)/L)}\left(K_{i,n}\right). \quad (1)$$

N_t is the total number of one-way hash keys that can be used by the node; T_b is the time of the key used by the node at the beginning; T_c is the current time of the node; L is the life cycle of one-way hash key; $K_{i,n}$ stands for the last key in the node's one-way hash key chain; int denotes rounding function.

Direction comes from the data packet saved in the buffer. The acknowledgement packet is sent towards upstream in the opposite direction to data packet transmission.

TTL is determined by the policy preset in the protocol, that is, the number of hops required to arrive at the previous node generating acknowledgement packet.

(2) Waiting acknowledgement packet from its downstream node. If receiving acknowledgement packet in prescribed time, it does the following operations.

(i) Check whether the one-way hash key, $K_{i,j,}$ used by the packet is valid.

If $K_{i,j,}$ meets the below criterion:

$$\frac{(T_{c2} - T_{c1})}{L} - m > 1; \quad (2)$$

T_{c2} is the time of the acknowledgement packet received this time; T_{c1} is the time of the acknowledgement packet received last time generated by the same node; L is the life cycle of one-way hash key; m meets the criterion: $K_{i,p} = F^m(K_{i,j})$;

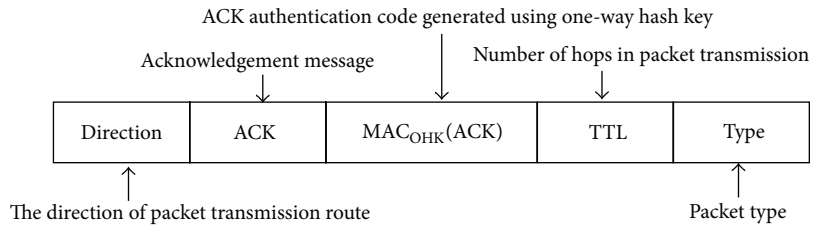


Figure 5: Format of acknowledgement packet.

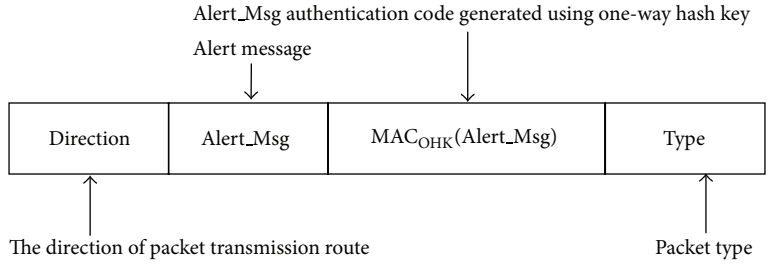


Figure 6: Format of alert packet.

$K_{i,j}$ and $K_{i,p}$ are the one-way hash keys received this time and last time from the node generating the acknowledge packet; then $K_{i,j}$ is considered invalid, send the alert packet illustrated in Figure 6 to S.

Alert_Msg contains information identifying its downstream neighboring node as a malicious node. Direction comes from the data packet saved in the buffer. The alert packet is sent towards upstream in the opposite direction to data packet transmission.

(ii) If the time to receive the acknowledge packet overruns the expected time, send the alert packet to S.

(iii) Check whether ACK is authentic via $\mathrm{MAC}_{\mathrm{OHK}}(\mathrm{ACK})$. If not, discard the packet.

(iv) Add 1 to the number of acknowledgement packets received. If it is under the expected value and overruns the stipulated time limit, send the alert packet to S; if it is up to the expected value, delete the data packet temporarily saved in the buffer.

(v) If TTL > 0, deduct one from TTL value and send the acknowledgement packet to the upstream nodes.

Step 5. The intermediate node sends the data packet to D according to the routing information.

Step 6. The destination node receiving the data packet makes the following four operations.

(1) Via $\mathrm{MAC}_{\mathrm{SD}}$ ($\mathrm{encry}_{\mathrm{data}}$), check whether $\mathrm{encry}_{\mathrm{data}}$ is authentic. If not, discard the packet.

(2) Check the authenticity of counter via $\mathrm{MAC}_{\mathrm{SD}}$ (counter), and then check whether the packet is fresh by comparing it with relevant values of the current node. If not fresh, discard it.

(3) Decipher the data content of the packet.

(4) Check whether there is attack.

Set the number of packets received by D from S as S_r, and the number of packets already sent by S as S_s. S_r needs to be initialized and recalculated at certain interval or after attack is repaired. S_l is the number of packets sent by S contained in the last packet received at last calculation cycle or in the first packet received after attack is repaired, while σ is an adjustable parameter related to the network's packet loss rate. If

$$\frac{\left|S_s - S_l - S_r - 1\right|}{\left|S_s - S_l\right|} < \sigma, \tag{3}$$

it means that the packet is normally received and update S_r with $S_r + 1$; otherwise, it means that there is attack. D will set S to alert state and use other secondary routes (referring to the routes comprised of nodes surrounding the optimal route with one hop more than the optimal route) to send the notice packet illustrated in Figure 7 to inform S about intruding node likely to make selective forwarding attack. When S receives the notice packet, it changes the data packet transmission mode, from regular mode to detection mode.

3. LSRP Performance Analysis

We evaluate LSRP comprehensively both in theory and by simulation, with focus on analyzing its security and traffic load balance.

3.1. LSRP Security Analysis. LSRP safeguards network security from the below aspects.

(1) Defense against eavesdropping attack. In order to capture high-sensitive data transmitted between the nodes, the attacker tries to get relevant information by eavesdropping the communication link.

To make sure the packet content is breach-proof, before transmission, LSRP encrypts the packet content, as described in Step 1 of above data packet transmission, and generates encrypted message $\mathrm{encry}_{\mathrm{data}}$. This can prevent outsider

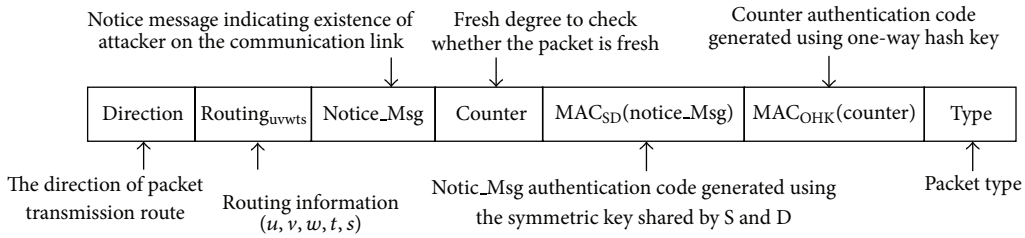


Figure 7: Format of notice packet.

attackers from eavesdropping the communication link to intercept the packet and steal its content.

(2) Defense against altering attack. If these exists insider attacker in the communication link, the insider_attacker can send a counterfeit packet to the receiver by altering the data packet and result in the receiver's making incorrect judgment or operation.

LSRP uses symmetric key and one-way hash key to generate authentication code to prevent the packet from being altered. For example, in Step 1 of above data packet transmission, symmetric key shared by S and D is used to generate MAC_{SD} ($\text{encry}_{\text{data}}$) for $\text{encry}_{\text{data}}$, while in Step 4 of data packet transmission, one-way hash key is used to generate MAC_{OHK} (ACK) and MAC_{OHK} (Alert_Msg) for the acknowledgement packet and alert packet, respectively. After receiving the packet, the receiver verifies the authentication code. If the packet information is inconsistent, it is ascertained that the packet content has been altered and hence there exists altering attack in the communication link.

(3) Defense against replay attack. The attacker intends to drain network energy and interfere in normal packet transmission by continuously replaying the old packet.

LSRP prevents the packet from being replayed by outsider attackers by inserting counter tag, which indicating fresh degree of the packet, and its authentication code into the packet. For instance, in Step 1 of data packet transmission, counter and MAC_{OHK} (counter) are used. As each receiver has a corresponding counter in itself, by comparing it with counter in the packet, it can determine whether the packet is fresh or not. If not, discard the packet. MAC_{OHK} (counter) guarantees the authenticity of counter. In this way, replay attack can be prevented. Moreover, thanks to the application of counter, that is, packet fresh degree, cycling attack [24] is also counterchecked.

(4) Defense against Wormholes and Sinkhole attacks. In Wormholes attack, the attacker receives the information at one end of the network through low-latency link and at the same time by virtue of its high performance sends the information to the cahoot at the other end to replay it, so as to produce high-performance communication link, attract the nodes to use the link where the attacker lurks, and then carry out larger sabotage by combining selective forwarding attack. In Sinkhole attack, a compromise node is produced to attract almost all traffic within certain region to pass through it, creating a sinkhole centering on the attacker, and then to carry out larger destruction by combining selective forwarding attack.

From the perspective of security, one important advantage of routing protocols based on geographical position is that it makes it difficult for the attackers to make Wormholes and Sinkhole attacks [24]. LSRP belongs to this category and can well defend against Wormholes and Sinkhole attacks. Routing protocols constructing topology initiated by base station, such as REAR [25], are prone to Wormholes and Sinkhole attacks. In the construction of the topology used by LSRP, the geographical positions of the base station and local nodes, the side length of RC and localized interaction are adopted, which make Wormholes unable to come into being. As the transmission route of data packet is realized by the policy for the twice probability routing selection proposed in this paper, the traffic is naturally routed to the physical position of the base station and is hardly attracted to other places to form sinkhole. Consequently, LSRP is almost immune to Wormholes and Sinkhole attacks.

(5) Defense against Sybil attack. A feature of Sybil attack is that the attacker keeps changing identity to attract as many packets as possible to go through it in the disguise of nodes at different positions and then carries out larger sabotage by combining selective forwarding attack. Sybil attack poses huge threat to multipath routing and geographical position based routing. Routing protocols mentioned in the literatures [5, 16, 17, 21, 26] are prone to Sybil attack.

LSRP is a routing protocol based on geographical position and therefore prone to Sybil attack. LSRP defends against Sybil attack by using symmetric key. In order to make Sybil attack, the attacker needs to put the disguised node in the transmission route of data packet. According to LSRP, to become a transmitting node in the route, the node needs to save its information in the neighboring nodes. One node accepts another node as its neighboring node in the course of topology construction. In the topology construction process given in Section 2, message authentication code generated using K_{temp} is used for identity authentication between the nodes. Without K_{temp}, the attacker cannot pass packet authentication, accordingly cannot disguise a node to become the neighboring node of other legal nodes and hence incapable of making attack.

Even if the attacker captures the node and gets the symmetric key, in LSRP, it is difficult to disguise itself as other nodes and make Sybil attack, for the below reasons: in LSRP, as each node and the base station share a unique symmetric key and the ID of each node is verified via the symmetric key, the attacker can hardly get the symmetric key of several nodes by capturing one node to disguise itself as several nodes. Hence, it is hard to make Sybil attack in this way.

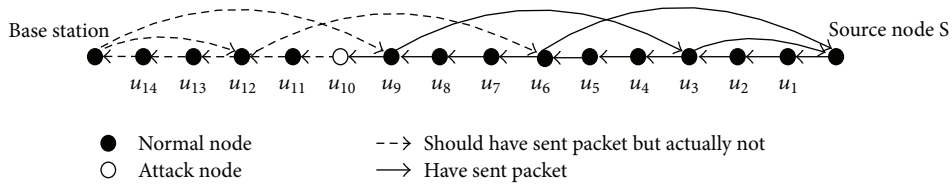


Figure 8: The case that the attacker discards data packet and does not return acknowledgement packet.

(6) Defense against HELLO FLOOD attack. In HELLO FLOOD attack, by right of high-power transmission, the attacker makes many nodes believe that it is their neighbor and causes those nodes send packets to an unknown place. As a result, the network is plunged into a mess.

Similar to the defensive measures against Sybil attack, LSRP also uses symmetric key to defend against HELLO FLOOD attack. HELLO FLOOD implements attack by making many legal nodes believe it is their neighbor, while the key of Sybil attack also lies in turning the attacker into the neighboring node of the legal nodes. These two types of attacks differ in the radiated power and the destruction target of the attackers. The approach for verification of legal neighboring nodes adopted in the defense against Sybil attack is also applicable in the defense against HELLO FLOOD attack. With it, the attacker is unable to win the legal nodes' trust and is rejected from adding to the neighbor table of the legal nodes. Hence, HELLO FLOOD attack is effectively prevented in the same way.

(7) Defense against selective forwarding attack. In selective forwarding attack, the attacker gains its end to sabotage network information by forwarding some information only and discarding the other. For some other attacks aimed at routing, such as Wormholes, Sinkhole, Sybil, they usually unite with selective forwarding attack to exert huge destructive force. Therefore, defending against selective forwarding attack is of great importance. Moreover, as this attack discards packet selectively and is more concealed, defense is even more difficult and the countermeasures are more complicated.

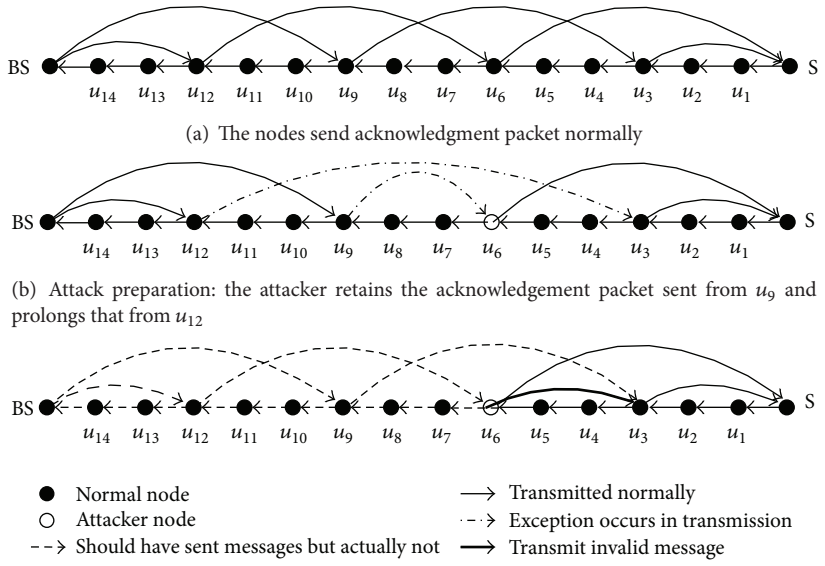
In LSRP, selective forwarding attack is detected by checking the number of packets sent by the source node and the number of packets already received from the source node accord with formula (3). When an attack is detected, in Step 4 of data packet transmission, a measure for positioning and detecting selective forwarding attack is provided to search for the position of the intruding node. This measure can detect the position of the attacker in the case of the following three attacks with time- and acknowledgement-based multihop detection technology:

(i) The attacker randomly discards packets and does not return acknowledging packets. LSRP chooses some nodes from the route to return acknowledgement packet to its upstream nodes, who then decide whether the neighboring downstream node is an attacker according to the number of received acknowledgement packets. For example, in the case of Figure 8, the attacker u_{10} discards the packet from u_9; therefore u_{10}'s downstream nodes are unable to send acknowledgement packet, which causes u_9, u_8, and u_7 to receive one acknowledgement packet only (if there is no attack, two acknowledgement packets should be received by each node). Then, u_9 generates an alert packet, reporting that u_{10} is an attacker, and sends it to S. u_8 and u_7 might also generate alert packet, but S can fix on the position of the attacker according to the last "time node seeing the previous data packet." Therefore, the judgment can be formed that the attacker specified by u_9 is the real attacker.

(ii) When the attacker finds that there is attack detection action, it does not discard the packet but intentionally prolongs the time to return acknowledgement packet. Delayed reply of acknowledgement packet causes upstream nodes far away from the attacker unable to receive the acknowledgement packet and consequently generates an alert packet by mistake, which causes legal nodes to be mistaken for the attacker. In Step 4 of data packet transmission, LSRP validates whether the downstream neighboring node is an attacker by checking the interval between sending the data packet and receiving the acknowledgement packet. If the interval overruns certain threshold value, it is affirmed that the downstream neighboring node is an attacker.

(iii) The case as illustrated in Figure 9 occurs. It is divided into two stages: attack preparation and attack implementation. At the former stage, the attacker intercept the acknowledgement packet, so as to intercept the one-way hash key K_x needed for fabricating an acknowledgement packet at next stage. At the later stage, the attacker discard new receiving data packet, fabricates a new acknowledgement packet with key K_x and sends it to the upstream. In this case, despite the acknowledgement packet is used for detection, it is hard to find the attacker's position though it has discarded the data packet. Regarding this problem, LSRP realizes prevention of malicious altering of packets by stipulating the Time to Live of each key in one-way hash key chain. When a node receives an acknowledgement packet, formula (2) is used to check if the key is within the valid time. If yes, keep upward transmission; otherwise, generated an alert packet and send it to S.

(8) Defense against acknowledgement spoofing attack. In acknowledgement spoofing attack, the attacker eavesdrops the packet sent to other neighboring nodes, sends acknowledgement spoofing packet to the source node that sends the



(a) The nodes send acknowledgment packet normally

(b) Attack preparation: the attacker retains the acknowledgement packet sent from u_9 and prolongs that from u_{12}

(c) Attack implementation: the attacker sends counterfeit acknowledgement packet of u_9 to upstream

Figure 9: One case of selective forwarding attack.

packet and makes it believe that a weak link is robust or an expired link is "alive"; hence packet loss is incurred.

This kind of attack can be regarded as a particular case of selective forwarding attack, because the destination node cannot receive packets sent by the source node as the attacker sends false acknowledgement packet and leads to data packet loss. LSRP can find out the position of the invalid RC by the approach of detecting the position of the intruding node in selective forwarding attack and treats the invalid RC as the attacker of selective forwarding. In this way, though the real attacker sending the false acknowledgement packet is not dealt with, it is not capable of acknowledgement spoofing attack anymore, because a better communication link is chosen to realize secure packet transmission. Hence, acknowledgement spoofing attack is effectively prevented.

3.2. LSRP Traffic Load Balance Analysis. As a secure routing protocol, LSRP features routing selection based on hexagonal mesh topology, one prominent advantage of which is that the route is determined only in relation with the node's coordinate, dispensing with generation of aroute leading to the destination node by flooding or searching for other destination nodes in other directions. It can save the energy consumed in routing searching. DPRA [15] is also a routing protocol based on hexagonal mesh topology, but it has only realized routing selection, and hasn't taken routing security into account. In addition, though DPRA is intended to pick out a suitable routing via the probability formula $P = (P_u, P_v, P_w) = (|u| + |v| + |w|)^{-1}(|u|, |v|, |w|)$ to balance network traffic load, it is still inferior to LSRP in traffic load balance. This section analyzes traffic load balance of LSRP in comparison with DPRA.

We analyze the load of RCs passed by packets when packets are sent from the source node S (u_s, v_s) to the destination node D (u_d, v_d). Suppose $w = 0$ (analysis is the same in the case of $u = 0$ or $v = 0$). $P_{i,j}$ is set to denote the probability of packet's passing through intermediate RC node $M(u_k, v_k)$, $i = |u_k - u_s|$, $j = |v_k - v_s|$.

(1) When M falls into the middle RCs as shown in the shaded part of Figure 10, the $P_{i,j}$ of LSRP and DPRA accords with formula (4) and (5), respectively,

$$P_{i,j} = \frac{1}{2} \cdot \frac{1}{|u|} + \frac{1}{2} \cdot \frac{1}{|v|}, \tag{4}$$

$$P_{i,j} = P_{i-1,j} \frac{|u| - i + 1}{|u| + |v| - i - j + 1} + P_{i,j-1} \frac{|v| - j + 1}{|u| + |v| - i - j + 1}. \tag{5}$$

From formula (4) and (5), we know that in LSRP the probability of packet's passing through M is $(1/2)(1/|u| + 1/|v|)$, while that in DPRA is related both to the values of u and v and to the node's position; therefore load balance in LSRP is superior to that in DPRA.

(2) When M falls into the surrounding RCs in 1, 2, 3, and 4 parts of Figure 10, traffic load balance is analyzed as follows.

(i) When M is a node of part 1, the $P_{i,j}$ of LSRP and DPRA accords with formula (6) and (7), respectively, with value falling into $[1/2|u|, 1/2]$ and $[\prod_{t=0}^{|u|-1}((|u| - t)/(|u| + |v| - t)), |u|/(|u| + |v|)]$, respectively,

$$P_{i,j} = \frac{1}{2} \cdot \frac{|u| - i + 1}{|u|}, \tag{6}$$

$$P_{i,j} = \prod_{t=0}^{i-1} \frac{|u| - t}{|u| + |v| - t}. \tag{7}$$

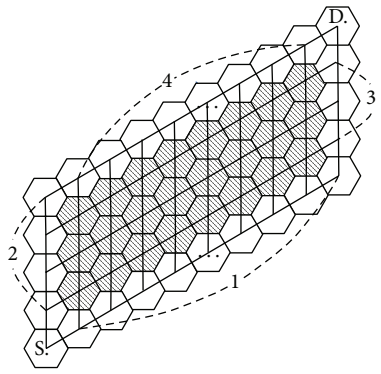


Figure 10: RCs traversed by the data packet.

(ii) When M is a node of part 2, the $P_{i,j}$ of LSRP and DPRA accords with formula (8) and (9), respectively, with value falling into $[1/2|v|, 1/2]$ and $[\prod_{t=0}^{|v|-1}((|v|-t)/(|u|+|v|-t)), |v|/(|u|+|v|)]$, respectively,

$$P_{i,j} = \frac{1}{2} \cdot \frac{|v| - j + 1}{|v|}, \tag{8}$$

$$P_{i,j} = \prod_{t=0}^{j-1} \frac{|v| - t}{|u| + |v| - t}. \tag{9}$$

(iii) When M is a node of part 3, the $P_{i,j}$ of LSRP and DPRA accords with formula (10) and (5), respectively, with value falling into $[(1/2)((1/|v|) + (1/|u|)), (1/2)((1/|u|) - (1/|v|) + 1)]$ and $[\prod_{t=0}^{|v|-2}((|v|-t)/(|u|+|v|-t)), |v|/(|u|+|v|)]$,

$$P_{i,j} = \frac{1}{2} \cdot \frac{1}{|u|} + \frac{1}{2} \cdot \frac{j}{|v|}. \tag{10}$$

(iv) When M is a node of part 4, the $P_{i,j}$ of LSRP and DPRA accords with formula (11) and (5), respectively, with value falling into $[(1/2)((1/|v|) + (1/|u|)), (1/2)((1/|v|) - (1/|u|) + 1)]$ and $[\prod_{t=0}^{|u|-2}((|u|-t)/(|u|+|v|-t)), |u|/(|u|+|v|)]$,

$$P_{i,j} = \frac{1}{2} \cdot \frac{i}{|u|} + \frac{1}{2} \cdot \frac{1}{|v|}. \tag{11}$$

The above analysis shows that the probability of packets' passing through M node in 1, 2, 3, and 4 regions in LSRP and DPRA falls into interval $A = [\min(1/2|u|, 1/2|v|), \max((1/2)((1/|v|)-(1/|u|)+1), (1/2)((1/|u|)-(1/|v|)+1))]$ and interval $B = [\min(\prod_{t=0}^{|u|-1}((|u|-t)/(|u|+|v|-t)), \prod_{t=0}^{|v|-1}((|v|-t)/(|u|+|v|-t)), \max(|u|/(|u|+|v|)), |v|/(|u|+|v|)]$. As $A \subset B$, it can be deduced that node load balance in 1, 2, 3, and 4 regions in LSRP is superior to that in DPRA.

4. Simulation Experiment

We evaluated LSRP in depth through simulation in NS2. As a security mechanism has been added and the protocol itself is secure, experimental evaluation mainly focuses on load balance of network traffic and energy consumption of the network. As for the scenario of experiment, assuming that 3000 nodes are randomly generated and distributed over 632 RCs on an $800 \times 800\,m^2$ site, each RC only has one active node, the sensitive radius of the nodes in the RC is 20 m and the communication radius is 40 m. The experiment uses the same energy consumption model as described in literature [27], with the initial energy of each node set to 100 J.

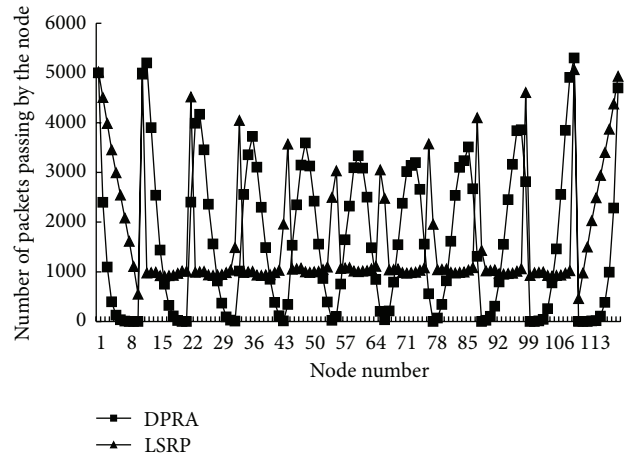


Figure 11: Load from the node (−10, 10) to the node (0, 0).

4.1. Network Traffic Load Balance. Figures 11 and 12 map the simulation results of sending 10000 data packets from the source nodes RC(−10, 10), RC(−10, 6) to the destination node RC(0, 0), respectively. In the chart, Node No. refers to the sequential number of the nodes ordered in u direction on multiple optimal routes. From Figures 11 and 12, it can be seen that LSRP features better load balance than DPRA under the condition that hops in U, V, and W directions are balanced or not balanced. They also show that the more unbalanced the hops in U, V, and W directions, the better load balance is realized by LSRP than by DPRA. The experiment figures reflect that LSRP has indeed improved traffic load balance.

4.2. Network Energy Consumption. In order to defend against various kinds of attacks, in addition to symmetric key and one-way hash key chain, LSRP also adds acknowledgement packet, alert packet and notice packet. Transmitting these three kinds of packets intended to defend against selective forwarding attack increases energy consumption. By comparing the solution to defend against selective forwarding attack in LSRP with that proposed in the literature [28] by Xiao et al., we illustrate the issues of energy consumption of the nodes and delay of data packets.

Figures 13 and 14 examine the energy consumption situation of the nodes when the transmission interval is 0.02 seconds (i.e., conditions with packet loss; Figure 15 shows a situation of packet loss when 1000 data packets are sent at different intervals and without attack), under the condition of without attacker or with attacker. From the charts, we can

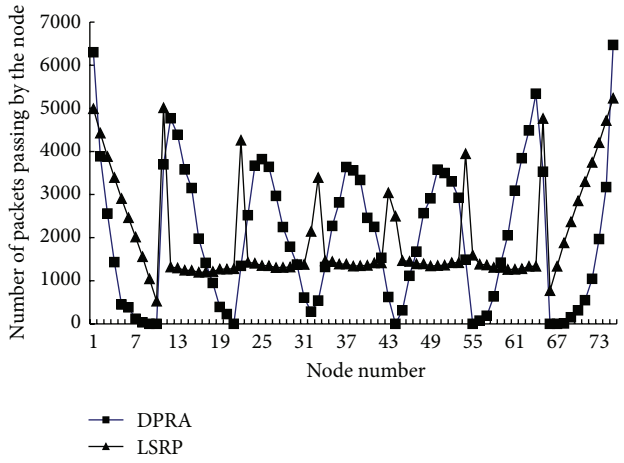


Figure 12: Load from the node (−10, 6) to the node (0, 0).

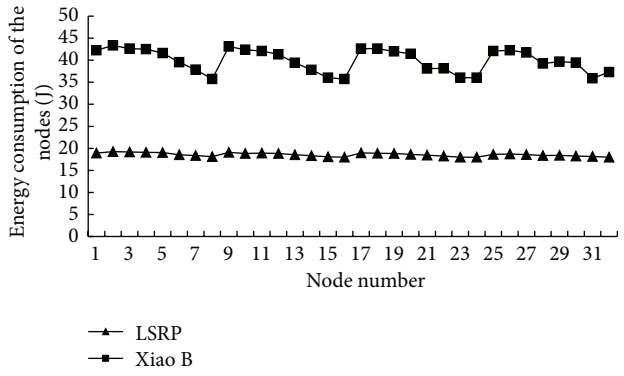


Figure 13: Energy consumption of each node on the optimal route after 1000 packets are sent from the source node (−7, −3) to the destination node (0, 0), without attack.

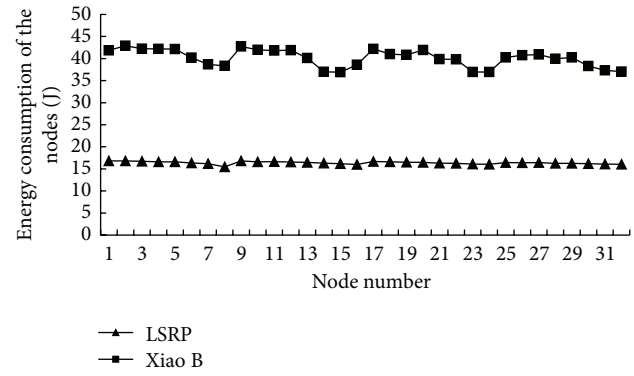


Figure 14: Energy consumption of each node on the optimal route after 1000 packets are sent from the source node (−7, −3) to the destination node (0, 0), with one node making attack.

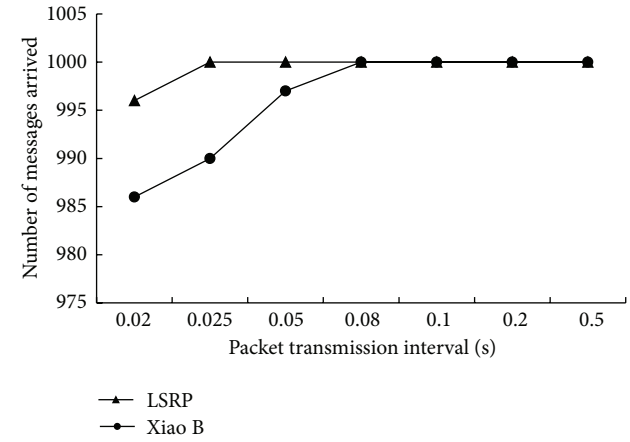


Figure 15: The number of messages received by the destination node after 1000 packets are sent from the source node (−7, −3) to the destination node (0, 0), without attack.

see that in LSRP energy consumption at each node is lower than that in Xiao's solution. This is because LSRP only invokes attack detection solution when attack is spotted and returns to the status of no attack detection after the attacker is located and dealt with; while in Xiao's solution, attack detection is done every time a data packet is sent, therefore extra energy is consumed.

Figure 16 examines the average energy consumption of the nodes under different transmission intervals. The chart shows that in the case of the same transmission interval, the average energy consumption in LSRP is less than that in Xiao's solution. This is because LSRP only invokes attack detection solution when attack is spotted and returns to the status of no attack detection after the attacker is located and dealt with; while in Xiao's solution, attack detection is done every time a data packet is sent, therefore extra energy is consumed. Meanwhile, Figure 16 also reveals the trend of descending at first and then ascending gradually of the average energy consumption, that is network energy consumption is closely related to the frequency of packet transmission. Descending at the beginning is because the network becomes less busy and less crowded, packet loss is reduced, and accordingly the number of alert packets decreases; consequently, energy consumption of the nodes is reduced. Later, the average energy consumptions mounts up because under no network congestion and no packet loss, as the packet transmission interval lengthens, so does the node's idle time. However, the node still consumes energy at idle time, so more and more energy is consumed.

Figures 17 and 18 examine delay of data packets under without attacker and with one attacker. The charts show that delay of data packets is relevant to the frequency of packet transmission. In the case of short transmission interval, the packet arrival time in LSRP is much shorter than that in Xiao's solution. This is also because LSRP only invokes attack detection solution when attack is spotted; therefore the number of acknowledgement packets is less than that of Xiao's solution, so is packet delay or congestion. When packet transmission interval is larger than 0.08 seconds and lengthens gradually, the arrival time of LSRP is a little shorter than and very close to that of Xiao's solution. This is because as the transmission interval lengthens, so does the node's idle time. The percentage of energy consumed at idle time

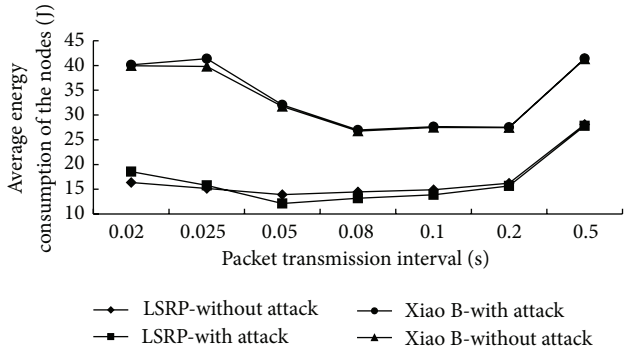


Figure 16: Average energy consumption of the nodes on the optimal route after 1000 packets are sent from the source node (−7, −3) to the destination node (0, 0).

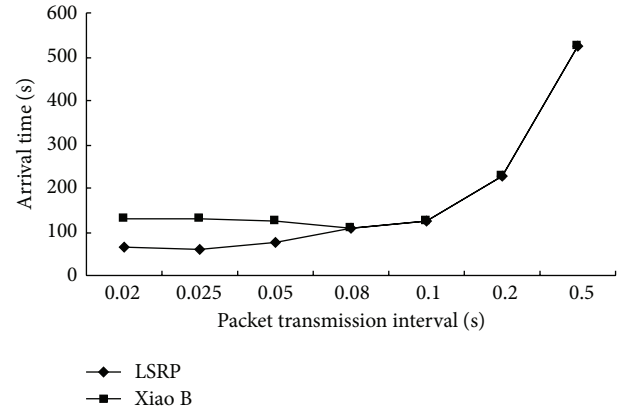


Figure 17: Time to arrive at the destination node after 1000 packets are sent from the source node (−7, −3) to the destination node (0, 0), without attacker.

increases and energy consumption of the node hinges on its idle time.

5. Conclusion

With rapid development of wireless sensor network applications, to guarantee routing reliability of the sensor network is a fundamental requirement to the security of the entire network and has become the major challenge in the research on wireless sensor security applications. This paper proposed an load-balanced WSN secure routing protocol, LSRP. Based on energy-saving hexagonal mesh topology, LSRP realizes security control over sensor network routing by making use of encryption technology, one-way hash key chain, and symmetric key technology and topology structure based on geographical position. In addition, through the policy of the twice probability optimized routing selection, it allows each RC to share data transmission more evenly, balances network traffic load, and effectively prevents some RCs from dying too quickly, and consequently lengthens the life cycle of WSN.

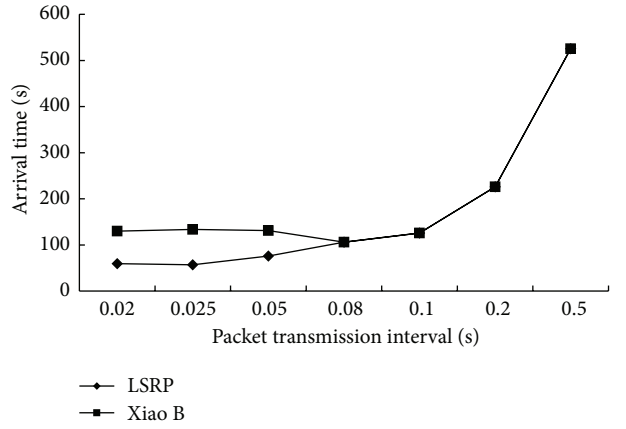


Figure 18: Time to arrive at the destination node after 1000 packets are sent from the source node (−7, −3) to the destination node (0, 0), with one attacker.

Acknowledgments

This work is supported by the Natural Science Foundation of China under Grant no. 61272074, the Natural Science Foundation of Jiangsu Province under Grant no. BK2011464, and the project of the Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education and the Foundation of Jiangsu University under Grant nos. 12JDG104 and 12JDG103. And the author Wang Liang-min is supported by the Disguised Researcher Program of Jiangsu Province of China (2012-wlw-020), and the academic leader is supported by Qinglan Project of Jiangsu Province of China.

References

[1] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.

[2] M. Sadeghi, F. Khosravi, K. Atefi, and M. Barati, "Security analysis of routing protocols in wireless sensor networks," *International Journal of Computer Science Issues*, vol. 9, no. 1, pp. 465–472, 2012.

[3] X. Ren, "Security methods for wireless sensor networks," in *Proceedings of the IEEE International Conference on Mechatronics and Automation (ICMA '06)*, pp. 1925–1930, June 2006.

[4] Q.-Q. Pei, Y.-L. Shen, and J.-F. Ma, "Survey of wireless sensor network security techniques," *Journal of China Institute of Communications*, vol. 28, no. 8, pp. 113–122, 2007.

[5] B. Karp and H. T. Kung, "GPSR: greedy Perimeter Stateless Routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 243–254, August 2000.

[6] T. J. Sebastian, "Secure route discovery against wormhole attacks in sensor networks using mobile agents," in *Proceedings of the 3rd International Conference on Trendz in Information Sciences and Computing (TISC '11)*, pp. 110–115, December 2011.

[7] S. Madria and J. Yin, "SeRWA: a secure routing protocol against wormhole attacks in sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1051–1063, 2009.

[8] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[9] M. G. Shiva, R. J. D'Souza, and G. Varaprasad, "Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks Source," *IEEE Sensors Journal*, vol. 12, no. 10, pp. 2941–2949, 2012.

[10] C. Yin, S. Huang, P. Su, and C. Gao, "Secure routing for large-scale wireless sensor networks," in *Proceedings of the International Conference on Communication Technology (ICCT '03)*, pp. 1282–1286, Institute of Electrical and Electronics Engineers, April 2003.

[11] N. El-Bendary, O. S. Soliman, N. I. Ghali, A. E. Hassanien, V. Palade, and H. Liu, "A secure directed diffusion routing protocol for wireless sensor networks," in *Proceedings of the 2nd International Conference on Next Generation Information Technology (ICNIT '11)*, pp. 149–152, June 2011.

[12] J. Deng, R. Han, and S. Mishra, "INSENS: intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp. 216–230, 2006.

[13] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys' 03)*, pp. 324–325, Association for Computing Machinery, November 2003.

[14] M. García-Otero, T. Zahariadis, F. Álvarez et al., "Secure geographic routing in ad hoc and wireless sensor networks," *Eurasip Journal on Wireless Communications and Networking*, vol. 2010, Article ID 975607, 2010.

[15] M. A. Hamid, M. Mamun-Or-Rashid, and S. H. Choong, "Defense against lap-top class attacker in wireless sensor network," in *Proceedings of the 8th International Conference Advanced Communication Technology (ICACT '06)*, pp. 314–318, February 2006.

[16] 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)*, p. 12, Institute of Electrical and Electronics Engineers, June 2007.

[17] N. Nasser and Y. Chen, "SEEM: secure and energy-efficient multipath routing protocol for wireless sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2401–2412, 2007.

[18] C. Karlof, Y. Li, and J. Polastre, "ARRIVE: algorithm for robust routing in volatile environments," Tech. Rep. UCB/CSD-03-1233, Computer Science Department, University of California at Berkeley, 2002.

[19] P. Santi, "Topology control in wireless ad hoc and sensor networks," *ACM Computing Surveys*, vol. 37, no. 2, pp. 164–194, 2005.

[20] H. Zhang and A. Arora, "GS3: scalable self-configuration and self-healing in wireless sensor networks," *Computer Networks*, vol. 43, no. 4, pp. 459–480, 2003.

[21] X. Wang and T. Berger, "Topology control, resources allocation and routing in wireless sensor networks," in *Proceedings of the IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS '04)*, pp. 391–399, IEEE Computer Society, October 2004.

[22] X. Wang and T. Berger, "Self-organizing redundancy-cellular architecture for wireless sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '05)*, pp. 1945–1951, Institute of Electrical and Electronics Engineers, March 2005.

[23] X.-S. Wang, Y.-Z. Zhan, and L.-M. Wang, "STCP: secure topology control protocol for wireless sensor networks based on hexagonal mesh," in *Proceedings of the4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08)*, pp. 1–4, IEEE Computer Society, 2008.

[24] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[25] H. Hassanein and J. Luo, "Reliable energy aware routing in wireless sensor networks," in *Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS '06)*, pp. 54–62, Institute of Electrical and Electronics Engineers Computer Society, April 2006.

[26] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Personal Communications*, vol. 7, no. 5, pp. 16–27, 2000.

[27] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[28] B. Xiao, B. Yu, and C. Gao, "CHEMAS: identify suspect nodes in selective forwarding attacks," *Journal of Parallel and Distributed Computing*, vol. 67, no. 11, pp. 1218–1230, 2007.