Sensors & Transducers, Vol. 161, Issue 12, December 2013, pp. 274-278

www.sensorsportal.com

Sensors & Transducers

http://www.sensorsportal.com

The Improvement of Routing Protocols in Wireless Sensor Network Based on Tree Topology and PSK Algorithm

Leting TAN

Computer School of China West Normal University, Sichuan, 637000, China

E-mail: yubin685.com

Received: 29 October 2013 /Accepted: 22 November 2013 /Published: 30 December 2013

Abstract: For the high effectiveness and high security in wireless sensor network (WSN) applications, this paper improves the routing protocols based on the tree topology and PSK algorithm. It proposes the ST (security tree) topology that transforms the data delivery from nodes to cluster heads into multi-hop delivery mechanisms, reducing the energy consumption of data transmission; PSK keys are made for preventing transmission from different attacks, transferring the encrypted information between the adjacent nodes in WAN based on nodes mutual authentication. Meanwhile, according to the ST features, it also puts forward a safe routing policy with adaptive multi-path, to improve attack resistance and fault tolerance. Theoretical analysis shows that the advanced routing protocols can be low-energy, highly reliable and secure. *Copyright © 2013 IFSA*.

Keywords: Tree topology, Security routing protocol, Wireless sensor network.

1. Introduction

Because wireless sensor network (WSN) has a limited energy source and is vulnerable to outside interference and attacks, the design for efficient and secure WSN routing protocols has been a hotspot of research. Current routing protocols are generally divided into routing protocol [2], data-centric Routing Protocol [5], and location-based Routing Protocol [8].

This paper presents an efficient and safe routing mechanism- ST routing protocol based on the traditional hierarchical protocols, getting rid of the weakness, such as single-hop communication, poor extensibility and unfit for large-scale networks, and also it also applies the PSK into the ST initialization and route maintenance to realize the localized encryption and identification techniques. In this way, this protocol will have a good ability for safety, attack resistance and reliable multi-hop and multi-path, efficient and safe.

2. Generating Algorithm for PSK Keys

To prevent transmission from different attacks, it proposes that PSK keys are used to transfer the encrypted information between the adjacent nodes in WAN based on nodes mutual authentication for network security.

1) Main key k^m generates during the network initialization by reliable sink, and then, allocated to every sensor node. The node i based on the main key generates its own symmetric key $k_i = f_{k^m}(i)$, f_k for pseudo-random function [9].

2) The node pair (I, j) has to be two-way authenticated while initializing the routes. The node i sends the request for authentication message packets to the node j, including its own id and authentication code $\{i, MAC(k_i, i)\}$; when node j receives, it can calculate the k_i which can be used to

decrypt to realize the identification for i, if succeeded, then comes to the next step, otherwise ends the algorithm; The nod j conveys a confirmation message containing its id and authentication codes $\{j, MAC(k_j, j)\}$ to the node i; after receiving the messages from the node j, node i uses j to figure out the k_j which can be used to realize the identification for j, if succeeded, then comes to the next step, otherwise ends the algorithm.

3) The node pair (i, j) generates respectively the PSK keys between i and j, i.e. $k_{ij} = f_{k_j}(i)$.

4) Each node remains its own keys and PSK keys and eliminates other keys, keeping k_i and k_{ij} for the node i.

3. ST Secure Routing Protocol

3.1. ST Topology-Forming Algorithm

ECM algorithm can realize the ST initialization on the base of energy constraints, forming a basic multi-hop routing topology.

1) Basic concepts and definitions.

Maximum rated power p_m: means the largest transmitted power of all nodes in ST initialization and routing stable operation.

Neighbor node: means the node can be covered by any node α through launching the messages by p_m.

Tree T_v^l: l is the level of tree, that is, the combination times of nodes; v is the root node of the tree.

Edge-node: the node α of the tree has a neighbor node that doesn't belong to the tree, and then α is the edge node.

Edge-central node: stands for the node which has the smallest average distance from other nodes in the tree edge nodes.

Direct accessibility R_{ij}: when node i deliveries the data to the node j, $R_{ij} = 1$ while $R_{ij} = 0$.

The distance D_{ij}: equals to the round-trip time between the nodes, namely $d_{ij} = d_{ij-RTT}$.

2) ST-forming algorithm.

ST initialization can form a relatively stable routing topology. In this process, each node conducts the information interaction together with mutual authentication, setting up PSK, removing main keys and other node keys as well as initializing structures.

3) The combination of nodes.

While initialization, each node will broadcast authentication packets. After receiving the package, node a will calculate the energy consumption of each node, finding out the neighbor b with the least cost; after delivering the authentication packages to b and establishing the PSK keys, sending the combination requests with each other. If received the rejections for combination, the node will continue to calculate a new combined one with minimum energy consumption in the rest of neighbor nodes.

4) Tree combination and the generation of root nodes.

Two nodes are merged into one-level tree; two one-level trees are combined to a two-level tree, and so on. When all nodes in the network are included in the same subtree, it stops the recursion, as the Fig. 1 shows:

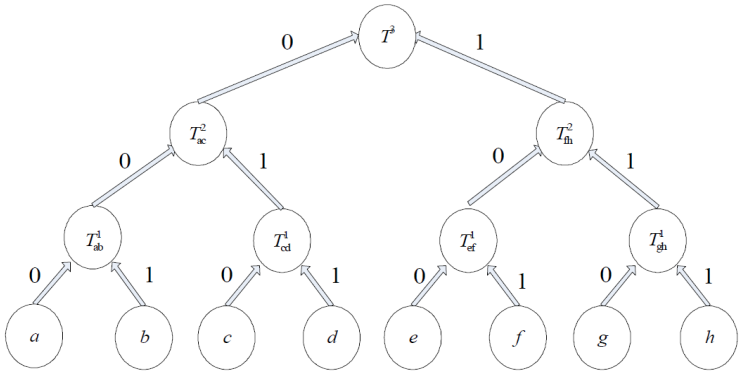

Fig. 1 The generation of ST.

Two nodes combined to a one-level tree are selected as the double root of the tree; two $l\ (l \geq 1)$ trees T_i^l and T_j^l are combined to form a $l+1$ level tree, determines their double nodes (i_1, i_2) and (j_1, j_2), while (i_1, i_2) are the two least-cost nodes between the all nodes in T_j^l and edge-centre node j in T_i^l; (j_1, j_2) are the two least-cost nodes between the all nodes in T_j^l and edge-centre

node i in T_i^l. After determining the root nodes, reconsidering the T_i^l and T_j^l to be $T_{i1,i2}^l$ and $T_{j1,j2}^l$, these two l-level trees combined form a $l+1$ level tree T_v^{l+1}, while v means imaginary root node which can become a real root node during the combination of T_v^{l+1} and other $l+1$ level trees. Obviously, each sub-tree in ST has double roots.

5) Node addressing assignment based on the tree structure.

According to the tree combination, each node α will be allocated with an exclusive network address $\alpha_{n-1}, \alpha_{n-2}, \cdots, \alpha_0$, while n stands for the tree level, α_i for the i node. Taking Fig. 1 as an example, the address is formed from low to high, while combing node a and node b, then $a_0 = 0$ and $b_0 = 1$; while combing node c and node d, then $c_0 = 0$ and $d_0 = 1$; supposing T_{ab}^1 and T_{cd}^1 are combined to form a two-level tree, allocating them respectively with one-level address of 0 and 1; supposing the selected a and c are roots, expressed as T_{ac}^2. According to the constant recursion, each node address will be assigned when a whole ST is formed.

3.2. ST Route Table

n-level tree (the highest level) is formed after the combination of ST. In forming the ST, it also generates route table of each node at the same time. The route table in each node α contains $n-1$ items, each of which has next hop node, expressed as $R_\alpha^l = (l, \beta_1^l, \beta_2^l)$, while $(0 \le l \le n-1)$, β_1^l and β_2^l are next hope nodes in l layer route item, both of which are two root nodes of l-level sub-tree exclusive of α in combining two l-level sub-trees. Each route item maintains two next hop nodes, which assure the flexibility and reliability of the route.

A l-level sub-tree contains 2^l nodes, while combining the $l+1$-level sub-tree can determine the route item in l-layer; while updating its routing table can transferring the update messages to the other nodes in the sub-tree. As ST in a large scale, not all nodes act as edge nodes; after receiving the update messages from the route table, each node will check out whether the related next hop nodes is arrived, if it is then update the table, or keep it empty.

To getting with the instable and vulnerable network topology in WSN, as well as assuring the safety and effectiveness, the route table will maintain each next hop node of availability and distance indicators, that is, maintaining R_{ab} and D_{ab} for next hop node b in node α routing table.

In Fig. 1, here is the setup procedure in node α routing table: firstly, α associates with b to T_{ab}^1, and then the combination of T_{ab}^1 and T_{cd}^1 forms a two-level T_{ac}^2; finally, T_{ac}^2 combines with T_{fh}^2 for the tree T^3 and realize the combination of ST. Based on this algorithm, the node α with its sub-tree levels in sequence adds the root nodes used in forming at all levels of the tree to the route table, as Table 1 shows. Supposing the node d in Figure 1 cannot connect to the node f or h, the second level of route table in node d is empty at this time, presented as Table 2.

Table 1. Node α route table.

Level	Next hop	Accessibility	Distance
2	f(101), h(111)	R_{af}, R_{ah}	D_{af}, D_{ah}
1	c(010), d(011)	R_{ac}, R_{ad}	D_{ac}, D_{ad}
0	b(001)	R_{ab}	D_{ab}

Table 2. Node d route table.

Level	Next hop	Accessibility	Distance
2			
1	a(000), b(001)	R_{da}, R_{dh}	D_{da}, D_{db}
0	c(010)	R_{ac}	D_{dc}

3.3. ST Route Table Maintenances

Each node based on PSK key encryption will periodically send probe packets to next hop node for its accessibility and delay specifications, in order to ensure the safety and effectiveness of the route. The node i deliveries a monitoring packet $P_i : (msg)_{k_{ij}}$ to the node j and receives and verifies P_{ackj} in the scheduled time; $R_{ij} = 1$, D_{ij} should be updated while receiving the response package or $R_{ij} = 0$, which means the node j is inaccessible. WSN topologies need to be rebuilt after large changes over time. But for the root node i in l-level, if there 1/3 nodes in route table are invalid, it should rebuild the ST topology of l-level sub-tree.

3.4. Adaptive Multi-Path Routing Algorithm

Supposing the address of node a as $A_a = A_a^{n-1} \left| A_a^{n-2} \right| \cdots \left| A_a^0 \right.$, node b as $A_b = A_b^{n-1} \left| A_b^{n-2} \right| \cdots \left| A_b^0 \right.$,

n is the highest level of ST. While a transmitting data to b, the steps of adaptive multi-hop routing algorithm are stated as follows:

1) Let $l = n-1$

2) If $A_a^l \neq A_b^l$, turn to (3); or $l = l-1$, return to (2)

3) Searching the item of l-level in a route table, namely $R_\alpha^l = (l, \beta_1^l, \beta_2^l)$; if β_1^l or β_2^l isn't empty, turn to (5).

4) If $R_{a\beta_1} = R_{a\beta_2} = 0$, namely β_1^l or β_2^l is empty, then $l = l-1$, return to (3).

5) If $R_{a\beta_1} = 1$ and $R_{a\beta_2} = 0$, then select β_1^l as next hop node; if $R_{a\beta_1} = 0$ and $R_{a\beta_2} = 1$, then select β_2^l as next hop node, turn to (7).

6) If $R_{a\beta_1} = R_{a\beta_2} = 1$, select the node with short distance as next hop node.

7) Delivery data to next hop node, and then repeating the data delivery with this algorithm until it ends.

For example, node d gets ready for transmitting data to node h. From the topology structure in Fig. 1, the addresses of these two nodes are respectively $R_d = 011$ and $R_h = 111$. Comparing the highest address in sequence, cause $A_d^2 \neq A_h^2$, it can find out the second level route item $R_d^2 = (2,,)$ in node a from the Table 2. And it also can find the first level item $R_d^1 = (1, a, b)$ in node d, according to the multi-hop routing algorithm, selecting a as next hop node and directly transmitting the message to the node a. Repeating the algorithm by node a, cause $A_a^2 \neq A_h^2$, it can seek out the second route item $R_a^2 = (2, f, h)$, selecting h as next hop node, and then ends delivery.

4. Performance Analysis

4.1 Route Efficiency and Reliability

Route using multi-stage and double next hop node, can increase the routing scalability and does not affect its reliability, even some attacked intermediate nodes are unable to provide routing services for the moment.

Definition 1: From the source node to the destination node, the accessible probability E_{num} is the indirect probability, num as the number of routing nodes can be selected by each hop in the route.

For WSN in a n-level ST, the total nodes are expressed as 2^n and the width of node address as n, the largest physical hop between as $N_m \leq n$. The reason for the empty item in route table is that, one is inaccessible because of distance, the other is not working properly due the node is attacked, while distance is not considered in this algorithm, and then ignored. Supposing the normal working probability as p, the route table in node i contains n items with total $2n$ next hop nodes, while the effective nodes are $2np$. If there is a normal route in the selective $2np$ next hop nodes, each node will delivery the data to the next hop node. In this way, the route is accessible, when all the hops are accessible, then it is reliable. Thus, the accessibility of WSN in a 2^n size can be presented as below:

$$E = \left[\frac{2np!}{i!(2np-i)!} p^i (1-p) \right]^n, \quad (1)$$

Compared to the general multi-hop routing mechanism, each hop just has one node for selection, then $E_1^n = p^n$. The following is the comparison of their accessibilities:

$$\frac{E_{2np}^n}{E_1^n} = \left[\frac{2np!}{i!(2np-i)!} p^{i-1} (1-p) \right]^n, \quad (2)$$

When $p = 0.8$, $n = 3$ and $2np \approx 5$, then $E_5^n = 0.999$ and $E_1^n = 0.512$. It is thus clear that without updating the route table, the accessibility of this algorithm will have a significant improvement compared with the single route maintenance accessibility.

4.2. Security

Supposing the needed minimum time of a node captured by the attacker as $T_{\min}$, generally the initialized time T_{est} of ST is a few seconds, so can suppose $T_{est} < T_{\min}$. $T_{\min}$ Later, no any nodes remain the main key k^m. Even $T_{\min}$ later, an attacker captures a node which has already completed the key allocation and generation, and then the attacker cannot access to the key information and main keys of other nodes, effectively preventing the attacker from further attacks.

The ST formation based on distance naturally avoids the black-hole attack. With the flexible route, the routing protocol enables an effective node getting over of the attacks from wormhole, jamming and other network flow restrains.

The ST forming algorithm completely determines the network topology, preventing the attacks form malicious routing loops, DOS and hello flood based on the route; due to the malicious nodes hard added to the routing topology, it can effectively inhibit the selective forwarding attacks; ST forming algorithm based on authentication mechanism can effectively prevent Sybil node into the network; meanwhile,

using bi-directional authentication mechanism in maintenance can actively suppress the attacks from false routing information and sinkhole.

For the internal attacks, a node in the route table maintains the next hop node information. When an attacked node gets the trust from its next hop node, its extension is limited, which can delay the attack velocity.

5. Conclusions

In this paper, it presents the ST topology formation algorithm, and also constructs a route table with multi-layer structures based on this algorithm. And then, it proposes the adaptive multi-path routing mechanism and related routing algorithm, better controlling the node communication consumptions and improving the reliability and flexibility of the route. In order to improve the WSN security, it designs a PSK key generation algorithm based on the PSK to realize the authentication in forming ST protocol and maintaining route table. Finally, though the theoretical analysis, it demonstrates the routing protocol with high efficiency, high reliability and security.

References

[1]. L.-Y. Sun, X. Huang, C. Wei, M. Xia, Data fusion algorithm of wireless sensor networks based on neutral network, *Chinese Journal of Structural Chemistry*, 1, 2011, pp. 122-127.

[2]. A. Manjeshwar, D. P. Agrawal, Teen: a protocol for enhanced efficiency in wireless sensor networks, in *Proceedings of the 15th Parallel and Distributed Processing Symposium*, San Francisco, IEEE Computer Society, 2001, pp. 2009-2015.

[3]. W. Chao, X.-Y. Jia, L. Qiang, Secure routing algorithm for wireless sensor networks based on reliability, *Journal on Communications*, Vol. 11, 2008, pp. 105-112.

[4]. W. Di, H. Gang, N. Gang, L. Wei, Z. Zhuo, Research on Secure routing protocol for wireless sensor networks, *Chinese Journal of Sensors and Actuators*, Vol. 7, 2008, pp. 1195-1201.

[5]. J. Kulik, W. R. Heinzelman, Negotiation based protocols for disseminating information in wireless sensor networks, *Wireless Networks*, Vol. 8, Issue 23, 2002, pp. 169-185.

[6]. Y. Zhong, S. Yang, Adaptive energy-saving routing algorithm for large scale wireless sensor networks, *Computer Engineering and Applications*, Vol. 1, 2013, pp. 89-93.

[7]. O. Goldreich, S. Goldwasser, S. Micali, How to construct random functions, *Journal of the ACM*, Vol. 33, Issue 4, 1986, pp. 210-217.

[8]. Y. Yu, D. Estrin, R. Govindan, Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks, *UCLA-CSD TR-01-0023*, Los Angeles, 2001, pp. 1-11.

[9]. P. Biswas, T. C. Lian, J. C. Wang, Y. Y. Ye, Semi definite programming based algorithms for sensor network localization, *ACM Transactions on Sensor Networks,* Vol. 2, Issue 2, 2006, pp. 188-220.