Third: capture the node C (I) and the common node Sk negotiating session key. With the second case similarity, node Sk nodes need to C (I) submit message to the base station, base station generates a certification number by the node C (I) returns to the node Sk can establish a session key. Because the node C (I) unable to establish connection with the base station, therefore, the node Sk is associated with the node C (I) to establish a session key.

If a node Sk for capturing node C (I), which sends the session key establishment request to the cluster head node node node CHi, CHi verification of C (I) tC (I) deployment time and current time difference, if tC (I) =tk, because an attacker would have to capture a common node of the most short time. For T2, the difference must be greater than T2, the node CHi refuses to establish a connection. If node C (I) forged through the deployment time for node CHi agreed key establishment, because tC (I) ≠ TK, then KCHi-C (I)≠ KC (I) -CHi, C (I) node to node CHi to establish a session key.

V. Overhead analysis

Hypothesis of sensor network in n m ordinary nodes, a cluster head node. A variety of network types of node communication overhead are not the same, only ordinary nodes and cluster head nodes to communicate, then the whole network node communication overhead for the 2n; cluster head nodes, respectively and the base station neighbor cluster head node, node communication, the cluster head node and a base station to establish key communication overhead for2m, and the ordinary communication node cost is 4N, with each cluster head node average number of neighbors is D1, the average number of neighbors certification for D2, then the cluster head nodes communication overhead for the (1+d1+3d2) m; base station communication is mainly used with the cluster head nodes session key establishment, and for general node and part of the cluster head nodes certification, the communication cost is m+2n (2d2+2). Therefore, the scheme of various types of nodes in the communication overhead such as shown in table 2.

Table 2 the node communication overhead

Node type	communication overhead
Common	node 2n
Cluster head node	(1+d1+3d2) M
Base station	(2d2+2) m+2n

The scheme uses a t symmetric polynomial to establish a session key, so the attacker in the capture (t+1) a node can calculate the T of symmetric polynomials information. In this plan, node establishes a session key computational overhead is calculated a yuan t degrees symmetric polynomial =a0+a1x+... +atxt, due to the computational overhead is far less than the calculation of addition multiplication overhead, so the main consideration cost less operational mode, namely multiplication overhead, assuming that variables of each power operation of the second, for example have been calculated by X3, calculation of X4clock one multiplication, so, this scheme requires 2t-1multiplications.

While in storage overhead, this scheme only needs to store an element t polynomial, polynomial coefficients for each hypothesis in occupying a storage space, its storage space for t+1.

VI. The ending

Node capture attack is a serious threat to security of wireless sensor network attack means, and the current research focused on capturing node deployed in network launched internal attack, and to prevent such attacks is the most effective method to prevent capture should be added to the network node to other nodes and conversation. In this paper, based on two yuan of symmetric polynomial presents a defense nodes capture attack scheme, this scheme will each node having a key and the identity and deployment time for binding, the attacker can only access to the capture of node and its neighbor nodes of the session key, prevent the attacker captured using node listens for other network communication; and when the capture node requests and the nodes in the network to establish the key, combined with the deployment time and base station for validation, prevent the capture of node and its neighbor nodes to establish a session key, to prevent capture node launch attacks within the threat.

Reference

[1] Wen Qiwen, Lu Jian Zhu in.WSN based on polynomial secure key establishment scheme [J]. Computer Engineering,2011,15(5):156-157

[2] Liu Yanan, King arrow, Du Shiga . Wireless sensor network threshold secret sharing model [J]. Journal of Electronics & information technology,2011,33(8):1913-1918.

[3] volts for flying, Qi. To realize the position and time binding key distribution -- defense sensor network node replication attacks the new method [J]. Journal on communications,2010,4(31):16-25.

[4] Liao Yaohua, Wang Xiaoming. A wireless sensor network node replication attack resistance of new method [J]. computer engineering and applications,2011,47(22):64-47.

[5] Qinling Mountains; Hu Rongqiang;; wireless sensor network node [J] effective energy consumption minimization strategy; Wuhan University of Technology;2010(2):78-79

[6] Deng Yaping; Wang Xu; belt; mobile node in wireless sensor network time synchronization method for [J]; computer engineering and design;2010(1):127-128

[7] Feng Xin; Yang Huamin; Song Xiaolong; WSN; improved node replication attack detection method [J]; computer engineering,2011,23(8):35-36.

[8] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing forwireless networks. Proc. of 2nd ACM Mobile Ad Hoc Networking and Computing (MobiHoc'01), pp. 299--302, 2011.

[9] L. Buttyan, J. P. Hubaux. “Stimulating Cooperation in Self-OrganizingMobile Ad Hoc Networks”, ACM Journal for Mobile Networks (MONET), special issue on Mobile Ad Hoc Networks, 2010, p 570 -592.

[10] N. Nasser, Y. Chen. “Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks”. 2010.ICC '07. IEEE International Conference on Communications, pp.1154-1159, 24-28 June 2010.

[11] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan. "Enhanced Intrusion Detection Techniques For Mobile Ad Hoc Networks." IETUK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2009), Dr. M.G.R. University, Chennai, Tamil Nadu, India. Dec. 20-22, 2009. pp.1008-1013.

[12] Y. Zhang, W. Le, Y. Huang. “Intrusion Detection Techniques for Mobile Networks”, Wireless Networks Journal, vol. 9, no. 5, 2011, pp1–16.

[13] P. Brutch, C. Ko. “Challenges in Intrusion Detection for Wireless Ad hoc Networks”, SAINT Workshops, 2011. pp. 368~373