Construction of WSN Based on Polynomial Node Capture Attack and Defense Methods

Gan Hong
Guangzhou City Construction College
Guangzhou, 510925, China

Pan Dan
Guangzhou City Construction College
Guangzhou, 510925, China

***Abstract*—Wireless sensor network (WSN) in the presence of node capture attack, put forward a kind of node capture attack detection method of defense, the method based on polynomial in two variables will be node key information and node deployment time and identification for binding, when negotiating session keys between nodes, nodes need to validate each other deployment time and the current time the difference, and combined with the base station a verification node legitimacy. Programmed in stop an attacker captured using node eavesdropping network communication at the same time, to prevent capture nodes and legitimate node establishes a session key, effectively preventing the capture of nodes to join the network. Through the analysis that the scheme of the safety and low system cost.**

Key words-WSN; symmetric polynomials; node capture attack; defense

I. Introduction

Wireless sensor networks have been widely applied, such as surveillance and tracking of a target, environmental sampling, remote control of the plant and the sanitary supervision. A typical sensor nodes by low cost hardware, power, communication and computing capacity constraints, the traditional security mechanism can not be applied to the sensor nodes, so that the wireless sensor networks face many aspects of security challenges, such as Lu Yuan, node capture attack (node capture attack), and key management and Dos attack. Node capture attack is considered the most serious threat to security of [1], it is easy to launch, and difficult to be detected, and it is the copy attack, Sybil, wormhole attacks such as foundation, black hole.

Node capture attack, attack action can be divided into three stages [2]:

1. Physical capture sensor node, compromise them and get the sensitive information, such as the key;

2. Will be compromised nodes (compromised node) redeployed in the network;

3 .Launch attacks within.

At present, against node capture attack defense program mostly used to study key management scheme to prevent attackers eavesdropping network communication, such as virtual key ring (virtual key ring) [3] threshold secret sharing scheme with model [4], such programmers, must capture the amount of nodes attacks to network threat, thus effectively preventing an attacker would have to capture after listening to other nodes and compromise safety communication between nodes, and can prevent the attacker will capture the node (capture node) redeployed in the network to perform other types of attacks; and a few proposal is the study of sensor network in a variety of internal attack and defense mechanisms, such as Sybil [5], [6][8] replication nodes attack attack. Guard against node capture and attack the most effective method is to prevent an attacker using a captured node eavesdropping network communication at the same time, prevent the capture of nodes in the network to deploy.

In this paper, based on two Yuan of symmetric polynomials proposed a guard against node capture attack scheme, scheme binding node deployment time and node identification as a polynomial in two, when the node into the key stage, nodes using deployment time for mutual authentication, when using the deploy time cannot determine whether the node is legal, nodes through sending authentication request, using the base station node legitimacy verification. The scheme is based on two Yuan polynomial complexity to prevent attackers use to capture useful information interception of network nodes, while preventing the capture of node and its neighbor nodes to establish a session key, so as to prevent its redeployment to the network for the purpose of.

II. network model

If the wireless sensor network is based on the clustering of heterogeneous network, there are3 different nodes, respectively, for the base station (BS), cluster head node and a common node. Figure 1 shows a schematic diagram of sensor network.

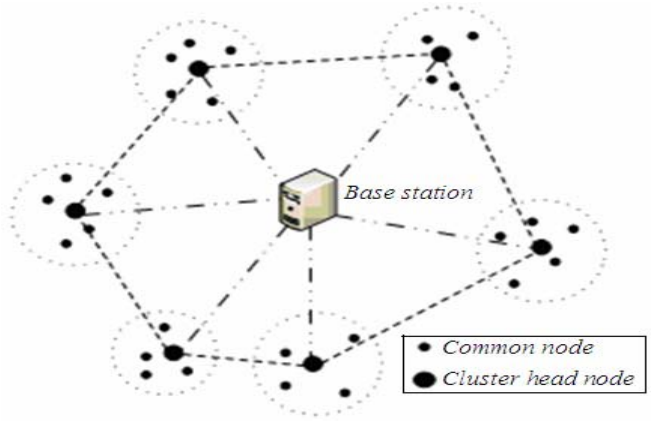
The base station is in charge of the whole network control and receiving the cluster head node to send data. Base station communication range to cover the entire network, as a network control center, the general deploy in unattended operation environment.

The cluster head node is responsible for the collection of data and the received data preprocessing and then transmitted to the base station.

Common node is responsible for the collection of data, and then transmits the data to the cluster head node.

In each node, energy, storage space and computing are most common node base station, the weakest.

Assuming that the network of sensor nodes in the [7] time synchronization mechanism, so as to solve the time synchronization problem between sensor nodes, nodes in the network deployment to a location on instant record his current time.



III. Based on the polynomial key distribution scheme

The sensor nodes deployed in monitoring region before the specified, by the server generates a random finite field GF (P) in two Yuan of symmetric polynomial:

$$f(x,y) = \sum_{i,j=0}^{t} a_{ij} x^i y^j$$

Among them, P is a prime number, t therefore the degree of a polynomial, and the" symmetry" of the meaning is that for any X and y, these polynomials satisfy f (x, y) =f (y, X). This polynomial must be kept confidential, each node before deployment to pre-install the polynomial. Table 1 shows the symbols used in this paper.

Table 1 symbols

Name	meaning
BS	base station
Chi	cluster head node
Sk	common node
I	IDi node identification
I	ti node deployment time
T1	attackers breached the cluster head nodes in the shortest time
T2	attackers breached the common nodes in the shortest time
H (x)	on the X hash algorithm
Ki-j	node i calculation and node j symmetric key
F (x y)	t two order polynomial
|	connection symbol
K (x) x	with K encryption keys
Ni	node i generated random numbers
$Conf_i$	base station for node I certification number calculation
K (MAC (M))	K, M key encrypted message authentication codes

A Node initialization

The first node will own deployment time value Ti and mark IDi, then into the primitive polynomial f (H (Ti |IDi), y), and permanently delete the original polynomial. Cluster head node and the common node must be in T1and T2time key establishment, cluster head nodes safety is higher than that of ordinary nodes, so the attacker breached the cluster head node all the time size from ordinary nodes, i.e. T1 > T2.

B Key establishment stage

1) Cluster head node and the base station the session key agreement

Cluster head node after initializing, first with the base station to establish a session key. Specific key negotiation process is as follows.

1) cluster head node sends message to the base station

The CHi→ BS: tCHi, IDCHi

The base station first to the CHi identity verification, and judge tCHi and the current time value is less than T1, if not, because the attacker breached a cluster head nodes of the shortest time is T1, then the base station rejects and CHi to establish the key; if yes, the base station to the cluster head node deployment time and identity hash operation, and generates a random number NBS into two yuan, generation and CHi session key KBS-CHi:

KBS-CHi=f (H (tCHi |IDCHi), NBS)

2) base station returns a confirmation message

Reply message base station CHi, that agreed to establish a session key.

The BS→ CHi: NBS, KBS-CHi (MAC (NBS)), OK

CHi formation and BS session key:

KCHi-BS=f (H (tCHi |IDCHi), NBS)

2) Cluster head node session key agreement

① CHi radio and a Hello message

CHi: Hello, tCHi, IDCHi *

CHj receives the Hello message, check the cluster head node CHi deployment time and current time difference is less than T1, if not, refusing to establish a key; if yes, then the calculation with CHi session key is KCHj-CHi, then send a message to the cluster head node CHi.

KCHj-CHi=f (H (tCHj |IDCHj), H (tCHi |IDCHi))

② CHj send a message to CHi

The CHj→ CHi: tCHj, IDCHj, KBS-CHj (MAC (tCHj |IDCHj)), OK

Cluster head node CHi check the CHj deployment time and the current time value is less than T1, such as less than, then computing and cluster head node CHj session key

KCHi-CHj=f (H (tCHi |IDCHi), H (tCHj |IDCHj))

Such as greater than T1, cluster head node CHi for CHj verification, validation of the method is the node CHi to generate a random number by the node CHj to the base station, the base station generates a certification number is sent to the node CHi, to verify the legitimacy of the node CHj. Node CHi generates a random number NCHi, and calculate the f (H (tCHi |IDCHi), NCHi).

③ CHi send a message to CHj

CHj: CHi →KCHi-BS (tCHi, IDCHi, NCHi)

④ CHj forward CHi message to BS

BS: CHj →KCHj-BS (IDCHj, KCHi-BS (tCHi, IDCHi, NCHi))

BS calculated authentication number:

ConfCHi = f (H (tCHi |IDCHi), NCHi)

⑤ BS calculation results can be returned directly to the CHi, cluster head node CHi check the confCHi and their results are the same, such as the same, and the node CHj to establish a session key KCHi-CHj; such as different or not received from the base station news refused and node CHj to establish a session key.

3) Common node and the cluster head nodes in the session key agreement

① the node Sk transmits a request message to the cluster head node CHi

The Sk→ CHi: Hello, TK, IDk, Nk

CHi calculation of the current time and TK value is less than the time of T2, such as greater than, refused to establish key. Such as less than, generating key KCHi-Sk, and send a message to BS.

KCHi-Sk=f (H (tCHi |IDCHi), H (TK |IDk))

② CHi send a message to BS

BS: CHi →KCHi-BS (IDCHi, TK, IDk, Nk)

Base station calculates certification number confk = f (H (TK |IDk), Nk), and the message to the cluster head node CHi.

③ BS certification number confk send CHi

CHi: BS →KBS-CHj (confk)

Cluster head node CHi decryption by confk.

④ CHi sends the authentication number to Sk

The CHi→ Sk: tCHi, IDCHi, confk, KCHi-Sk (MAC (tCHi |IDCHi confk, OK |))

Node Sk authentication confk and their calculated results such as equal, equal and cluster head node CHi key KSk-CHi.

KSk-CHi= f (H (TK |IDk), H (tCHi |IDCHi))

IV. Safety analysis

The analysis of the security of the scheme. The first description of an attacker using a captured nodes may pose a threat, on one hand, the attacker tries to capture the nodes of the key information for interception of network security communication, on the other hand, the attacker may be captured using nodes and networks in other normal node establishes a session key, thereby realizing the purpose of network attack.

In this scheme, an attacker would have to capture a node, the node can only access to capture with other nodes in the session key, and cannot use these key direct communication between other nodes listen. For each node in the network when deployed in the network, generates a polynomial, the polynomial bound deployment time and node ID, so that each node in the polynomial and the other nodes are not the same, and the session key only by the communication node both deployment time and node ID nodes, a session key can only be used a communication node, which cannot be used with the node and other nodes to communicate. Therefore, the attacker access to key information cannot be used for capturing node listens to other secure communication among nodes.

The attacker could capture node to deployed in the network to launch other types of attacks, if the attacker successfully captures the deployment of nodes in the network, the network security caused great influence. However, it must be in the implementation of these prior to the attacks with other nodes for establishing a session key, which can receive messages sent to other nodes, or convert other nodes of the message, in order to achieve the purpose of network attack. An attacker can forge node identification and deployment time, in an attempt to establish a session key and the other nodes. The following were the cluster head node and a common node safety analysis.

If a cluster head node CHi for capturing node C (I), C (I) with other nodes to establish a session key, there are three kinds of cases: C (I) and BS negotiating session key, C (I) and adjacent cluster node CHj negotiating session key, C (I) receives the ordinary node Sk session key establishment request.

The first case: capture the node C (I) and BS negotiating session key. Capture the node C (I) IDC (I) transmits the identification and deployment time tC (I) to the BS request to establish a session key, BS receiving the news, first verify that tC (I) and the current time value is less than T1, if not, the base station node C (I) to establish a key; if less than, BS tC (I) and IDC (I) into the polynomial in two variables, calculation of KBS-C (I) =f (H (tC (I) |IDC (I)), NBS), and NBS sent to the node C (I) KC (I), node calculation -BS=f (H (tCHi|IDCHi), NBS), because the attacker must pass through the base station for forgery to deployment time difference between verification, deployment time tC (I)≠ tCHi, so KBS-C (I) ≠ KC (I) -BS, thus capturing node C (I) and the base station to establish a session key.

Second: capture the node C (I) and adjacent cluster node CHj negotiating session key. The first case is knowable, capturing node forged through the deployment time and not with other nodes for establishing a session key. Now consider the following two possible.

A node C (I) request adjacent cluster head node CHj to establish the key node receiving the node C, CHj (I) key establishment request, to verify that the tC (I) and the current time value, if tC (I) =tCHi, the difference must be greater than T1, node CHj refused to establish a key, if tC (I)≠ tCHi, KCHj-C (I)≠ KC (I) -CHj; the other is a new cluster head nodes and the node C CHj request (I) to establish the key, if the new node CHj to validate the C (I) deployment time, with the establishment of key, because the tC (I)≠ tCHi, so KCHj-C (I)≠ KC (I) -CHj. If tC (I) =tCHi, CHj validation node node C (I) is a node in a network, send a message (tCHj, IDCHj, NCHj) to C (I) nodes to transmit to the base station, by the node C (I) unable to establish connection with the base station, therefore, the node CHj does not receive the station back value, is not associated with the node C (I) to establish a session key.

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