Advances in Computer Science Research, volume 65

3rd International Conference on Communications, Information Management and Network Security (CIMNS 2018)

A Novel Sub-regional Key Management Scheme for Distributed Wireless Sensor Network

Yinghong Liu[1] and Yuanming Wu[2,*]

[1]School of Automation Engineering, University of Electronic Science and Technology of China
[2]School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China
[*]Corresponding author

***Abstract*—Encryption technique is one of the key technologies in wireless sensor networks. In this paper, a novel key management scheme of sub-regional based on bivariate symmetric polynomial key is proposed for distributed wireless sensor network (WSN). A certain amount of bivariate symmetric polynomials are stored in sensor nodes by sub-regional, it makes the intersection of key rings in any adjacent sensors not empty. We choose the hash function of all the common bivariate symmetric polynomials of the two communication nodes as the session keys. At the same time, our scheme also solves the contradictory problem among energy overhead, encryption techniques. A compromised solution is found to optimize the performance of wireless sensor network with the sound key management scheme proposed in this paper.**

Keywords—wireless sensor network; key management; bivariate polynomial; security; sub-regional

I. INTRODUCTION

With the increasing popularity, the security of wireless sensor networks (WSNs) has gradually attracted the attentions of the general public. Different performance requirements will be needed for the different applications in the wireless sensor network, such as security, lifespan and energy overhead. For example, high security is needed in battlefield and hospitals to ensure confidentiality and integrity of data transmission over the network.

The defenses against outside attack are data encryption and message authentication, and the network would have better confidentiality by preventing data packet eavesdropping, tampering. Depending on the difference of the application environments and architectures of WSNs, the classic key management schemes are divided into three categories: the centralized pre-distribution key scheme [1], the elements-based key scheme [2] and the pre-shared key distribution scheme [3] .The first one has a high security and reliability, but it is rarely used due to the strong dependence on the base station. The second one requires that all sensor nodes to be deployed in the ranks at the intersection of the grid, which would reduce the flexibility of the network greatly. As for the pre-shared key distribution scheme, it cannot provide sufficient security when the number of compromised nodes increases, with a high energy overhead because of updating the network key frequently in a long time.

The rest of the paper is organized as follows. The problem and main ideas with crucial techniques are discussed in Section II. The details of our key management scheme are presented in Section III. The basic structure of the simulation network model is illustrated in Section IV. Finally, some conclusions are drawn in section V.

II. PROBLEM DESCRIPTION AND MAIN IDEA

How many polynomials have to be stored in sensor nodes in such a way that the intersection of key rings between the same area and different areas is not empty?

In this paper, a sub-regional key management scheme based on the bivariate symmetric polynomial is presented. Firstly, the sensors are deployed in the monitoring area randomly and uniformly, bivariate symmetric polynomials are distributed as the key elements in the corresponding nodes according to a certain rules, the negotiation and management of session key is carried out after the deployment of bivariate symmetric polynomials, this allocation scheme will support the dynamic addition of nodes and improve the scalability of the network very well. Secondly, in this paper, the keys are stored in sensors in such a way that the intersection of key elements of nodes in any two regions is not empty , which will up for the shortcomings of the key management scheme in [4] and improve the security of the network greatly. Finally, the way that the bivariate symmetric polynomials are taken as the key elements to generate the session keys will improve the anti-capture ability of the sensors. Each node stores a certain amount of polynomials will store the memory overhead and computation overhead of the network. Meanwhile, the proposed scheme will enrich the diversity of keys and improve the survivability of the network.

As shown in Figure 1, the sensor nodes A, B, C, D, E, F and G, their session keys are not same.

Copyright © 2018, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

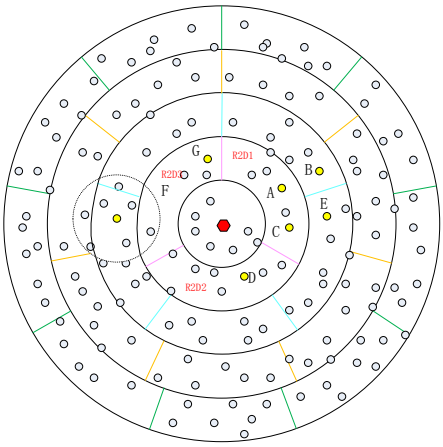

FIGURE I. NETWORK DEPLOYMENT DIAGRAM

III. THE DETAILS OF OUR SCHEME

In this paper, the key management scheme comprises three phases: initialization phase, the common keys discovery phase and key path establishment phase.

A. Initialization Phase

Firstly, the base station generates a number of bivariate symmetric polynomials randomly. As shown in Figure 1, each concentric ring is divided into some sub-regions. The sensor nodes of the whole network store the initial key K_{init}. Secondly, the key elements in sensor nodes are deployed in two steps: (1)The sensors in the first ring are deployed the polynomial$f_{r1}(x,y)$, the sensors in the second concentric ring store the polynomials $f_{r1}(x,y)$ and $f_{r2}(x,y)$, and the sensor nodes in the third concentric ring store the polynomials $f_{r2}(x,y)$and$f_{r3}(x,y)$, like this, the sensors in the nth concentric ring store the polynomials$f_{r(n-1)}(x,y)$and$f_{rn}(x,y)$. (2) The concentric rings is divided again, the sensor nodes in the area R_2D_1 store the polynomials $f_{d1}(x,y)$ and $f_{d2}(x,y)$, the sensor nodes in the area R_2D_2 store the polynomials$f_{d2}(x,y)$and$f_{d3}(x,y)$, like this, the sensor nodes in the area R_2D_nstore the polynomials$f_{dn}(x,y), f_{d1}(x,y)$. Finally, the sensor nodes in the area R_2D_1 store the polynomials $f_{r1}(x,y), f_{r2}(x,y), f_{d1}(x,y), f_{d2}(x,y)$, and the nodes in the area R_2D_2 store the polynomials$f_{r1}(x,y), f_{r2}(x,y), f_{d2}(x,y), f_{d3}(x,y)$with the given rules. The session key is generated by the hash chain based on the common polynomial(s) between the two communication nodes.

B. Common Keys Discovery Phase

The sensor nodes begin to enter the common keys discovery phase after all the sensor nodes are deployed with the corresponding key elements. At this phase, each node broadcasts a simple *HELLO* message to their neighbors, and the neighbor nodes send a reply message to the source node after they receive the broadcast message. All the nodes calculate the bivariate symmetric polynomials stored in the node by the ID and send a message to their neighbors again. The neighbors receive a key message, including the values of bivariate symmetric polynomials, and find the common values to generate the session key after analysis and comparison. Suppose node u and v are the two communication nodes.

Step1. The node u broadcasts a simple *HELLO* message to its neighbor, the message includes a random number Nonce and its own identifier ID_u, namely, $E_{K_{init}}(ID_u, Nonce_{ID_u})$. ($E_{K_{init}}$represents the message which is encrypted with the key K_{init})

Step2. The identifier ID_u is substituted in the polynomials $f_1(ID_v, y_1), f_2(ID_v, y_2), f_3(ID_v, y_3), f_4(ID_v, y_4)$, by the neighbor node v to calculate the values of $K_{1(ID_v, ID_u)}, K_{2(ID_v, ID_u)}, K_{3(ID_v, ID_u)}, K_{4(ID_v, ID_u)}$ after the node v receives the broadcasts message. And then the node v sends a message including $E_{K_{init}}(ID_v), MAC(K_{1(ID_v, ID_u)}, K_{2(ID_v, ID_u)}, K_{4(ID_v, ID_u)}, Nonce_{ID_u} + 1, ID_v)$ to the node u.

Step3. The neighbor node u receives the message and gets the identifier ID_v by decrypting the message, then put the identifier ID_v into the polynomials $f_1(ID_u, x_1), f_2(ID_u, x_2), f_3(ID_u, x_3), f_4(ID_u, x_4)$ to calculate the value of $K'_{1(ID_u,ID_v)}, K'_{2(ID_u,ID_v)}, K'_{3(ID_u,ID_v)}, K'_{4(ID_u,ID_v)}$, finding the common values by comparing the eight values stored in the node u ($K'_{1(ID_u,ID_v)}$,$K'_{2(ID_u,ID_v)}$, $K'_{3(ID_u,ID_v)}$, $K'_{4(ID_u,ID_v)}$) and node v ($K_{1(ID_v,ID_u)}$,$K_{2(ID_v,ID_u)}$, $K_{3(ID_v,ID_u)}$, $K_{4(ID_v,ID_u)}$). Assuming $K_{1(ID_v, ID_u)} = K'_{1(ID_u,ID_v)}$, $K_{2(ID_v, ID_u)} = K'_{2(ID_u,ID_v)}$, $K_{3(ID_v, ID_u)} = K'_{3(ID_u,ID_v)}$, $K_{4(ID_v, ID_u)} = K'_{4(ID_u,ID_v)}$, then $K_{vu} = (K_{1(ID_v,ID_u)}||K_{2(ID_v,ID_u)}||K_{3(ID_v,ID_u)}||K_{4(ID_v,ID_u)}$ is the session key between the nodes u and v. Next, the message $E_{K_{init}}(Nonce_{ID_u}, K'_{1(ID_u,ID_v)}, K'_{2(ID_u,ID_v)}, K'_{3(ID_u,ID_v)}, ID_u)$ would be sent to the sensor node v by node u.

Step4. The sensor node v decrypts the message and gets the key elements $K_{1(ID_u,ID_v)}$,$K_{2(ID_u,ID_v)}$,$K_{3(ID_u,ID_v)}$ and $K_{4(ID_u,ID_v)}$. Then session key $K_{vu} = (K_{1(ID_v,ID_u)}||K_{2(ID_v,ID_u)}||K_{3(ID_v,ID_u)}||K_{4(ID_v,ID_u)}$ can be generated by the common values. Finally, the sensor node v sends a confirmation message to show the session key between the sensor node u and v is established by now.

In our scheme, the hash function is generated as the communication session key by all the same bivariate symmetric polynomial(s) in any two neighbor nodes, the number of different nodes with the common values of bivariate polynomials has three possibilities: 4, 3, 1. The length of hash chain which is composed of the session key has the following three possibilities: as shown in Fig.1, the sensor nodes A and B are in the different areas of the different concentric rings, the number of their common polynomials is 1, so the session key is $K_{AB} = f_{r2}(x,y)$. The sensor nodes A and C are in the same area of the same concentric ring, the number of the same polynomials is 4, namely, $f_{r1}(x,y)$,$f_{r2}(x,y)$,$f_{d1}(x,y)$,$f_{d2}(x,y)$, the session key between sensor nodes A and C is $K_{AC} = f_{r1}(x,y)||f_{r2}(x,y)||f_{d1}(x,y)||f_{d2}(x,y)$. The node A and D are in the different areas of the same concentric ring, the number of the same polynomials is 3, namely, $f_{r1}(x,y)$, $f_{r2}(x,y)$, $f_{d2}(x,y)$, so the session key between sensor nodes A and D is $K_{AD} = f_{r1}(x,y)||\ f_{r2}(x,y)||\ f_{d2}(x,y)$.

C. Key Path Establishment Phase

Key path establishment phase refers to the phase that a session key is established between nonadjacent nodes after the adjacent nodes establishing session keys.

Step1. The sensor node u sends a request message including the identifier ID_u and a random number Nonce to the sensor node v.

Step2. The sensor node v sends a reply message after receiving the request message which including the identifier ID_v and the configuration message to approve of establishing a key path to the sensor node u. The node u establishes an optimal key path by the interest function $W(x,y) = a * \left(\frac{1}{d_{n_i}}\right) + b * (C/C_{max}) + c * (E_{n_i}/E_v)$.

Step3. Repeats the step 2 until all session keys are established.

IV. The Basic Structure Of The Simulation Network Model

The simulation network model used in the new scheme is already built while the scheme proposed in our paper is analyzed theoretically and verified by the simulations in this section.

A. Assumptions

A key management scheme of sub-regional based on bivariate symmetric polynomials is proposed and the distributed network model is taken in our scheme. Assuming:

(1) The base station is worthy of confidence and cannot be captured by the adversary, it is not involved in the key negotiation process. The communication range of the base station covers the whole sensor network with unlimited computing, communication and storage capabilities.

(2) All sensors have the same battery power, memory storage size, CPU processing capacity and radio transmission range. They are deployed in a monitor area uniformly and randomly, all nodes remain stationary after deployment.

(3) All sensors are not captured by the adversary before the base station distributes the key elements to them.

B. The criteria of sub-region division

A circular region with the radius of $R = 50m$is divided into a series of concentric rings by r=10m.

The average number of nodes in each concentric circle is

$$\frac{\pi R^2}{\pi (nr)^2} = \frac{N}{X_n} \quad (1)$$

n is the nth concentric circle, R is the monitor area radius; r is the sensor node communication radius; N is the total number of sensors in the monitor area; X_n is the total number of sensors in the nth concentric circle.

According to the formula (1), $(X_1 - 1)$ is the number of physical neighbor sensor nodes.

The number of nodes in the node's communication radius:

$$\frac{\pi R^2}{\pi r^2} = \frac{N}{X_1} \quad (2)$$

X_n is the number of sensors in the n^{th} circle.

$$W_n = \frac{X_n - X_{n-1}}{X_1} \quad (3)$$

W_n is the number of sub-regions in the n^{th} concentric ring.

Table 1 illustrates the parameters adopted in practical simulations.

TABLE I. SIMULATION PARAMETERS

PARAMETER	*VALUE*
Simulation area	50m*50m
Node Number	200
Node placement	Random and uniform
Radio range	10m
E_{init}	2J
$E_{receive}$	28.6uJ
E_{send}	59.2uJ
E_{mul}	3.2uJ
$E_{r_{init}}$	760uJ

C. Performance Analysis

1). Storage energy overhead

In our scheme, an initial key K_{init} needs to occupy 16 bits memory, the coefficient of each bivariate symmetric polynomial stored in each sensor needs to occupy the $\log(2p)$ bits memory, node u need S (in our scheme, S = 4) polynomials of t degree, $f(u, y_i)$, namely each polynomial occupy $(t+1)\log(2p)$ bits, assuming the length of the key is 32 bits, p is 2^{32}. In the phase of discovery of the shared key, the sensors establish a session key through exchange of message *HELLO*, each sensor node needs to maintain a physical neighbor node list (the list records the ID of all the physical neighbor nodes) temporarily. And if each ID needs to occupy 16 bits memory, the number of the physical neighbor nodes is $(X_1 - 1)$, it needs to occupy $16 * (X_1 - 1)$ bits memory totally. Suppose the storage energy overhead is

$$E_s = S * (t+1)\log(2p) + 16 * (X_1 - 1) + 16$$
$$= 4 * (t+1)\log(2p) + 16 * X_1. \quad (4)$$

2). Communication energy overhead

The communication energy overhead is calculated by the times of communication and communication amount. The establishment of the communication key in our scheme needs to communicate three times. In the initialization phase, the polynomials are assigned in all sensors by the base station, each sensor node needs to receive four polynomials, where the energy consumption per node is $E_{r_{init}}$.

Assuming that node u broadcasts a packet of k_1 bytes to node v and node v returns a packet of k_2 bytes to node u, the energy overhead of the packet from node u to node v is E_{t1}, the energy overhead of the packet from node v to node u is

E_{r2}, the energy overhead of the packet from node v to node u is E_{t2}, the energy overhead of the packet from node u to node v is E_{r1}, so

$$E_0 = 2E_{r1} + 2E_{t1} + 2E_{r2} + 2E_{t2} \quad (5)$$

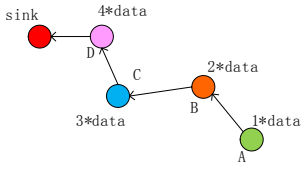

FIGURE II. DATA TRANSFER PROCESS

As shown in Figure 2, suppose the sensor node A needs to send a data packet to the sink node, the sensor node A has a secure link which is A-> B-> C-> D-> sink, that is node A sends a packet to node B, node B forwards the packet (including the packet receives from node A) to node C after receiving the packet from node A, and so on, node D forwards four data packets to the sink node.

The energy overhead of transmitting a data packet to others by the node $n_i{}^{th}$isEt_{n_i}, P_{n_i} is the number of packets (including the data packets that the node itself needs to be sent).(i=1,2,…,N)

$$E_{send}(n_i) = P_{n_i} * Et_{n_i} \quad (6)$$

The energy overhead of receiving a data packet from others by the node $n_i{}^{th}$ is Er_{n_i}, P_{n_i} is the number of packets.(i=1,2,…,N)

$$E_{receive}(n_i) = (P_{n_i} - 1) * Er_{n_i} \quad (7)$$

$$E_M = \sum_{i=1}^{N}(E_{send}(n_i) + E_{receive}(n_i) + E_{r_{init}}) \quad (8)$$

3). Calculation energy overhead

Solving a bivariate symmetric polynomial [6] needs$(t+1)^2$times multiplications, $t$times additions, so the calculation is $E_f = (t+1)^2E_{mul} + tE_{plus}$. The addition calculation energy overhead can be ignored because of$E_{plus} \ll E_{mul}$.

It requires eight times arithmetic of bivariate symmetric polynomial to establish a session key encryption each time, two times hash function operation, the calculation energy overhead of hash function is E_h each time, $W$is the number of times of key distribution, so the total calculation energy overhead of the network is$E_c = W(8E_f + 2E_h)$.

The total Energy consumption for the network:

$$E = E_c + E_M + E_S \quad (9)$$

As shown in Figure 3, the energy overhead of the key management proposed in our scheme is 1/10 of the SKM.

The degree of the polynomial has an obvious impact on energy overhead of the network. As shown in Figure 4, the greater the degree of the polynomial is, the more energy will be consumed in the network.

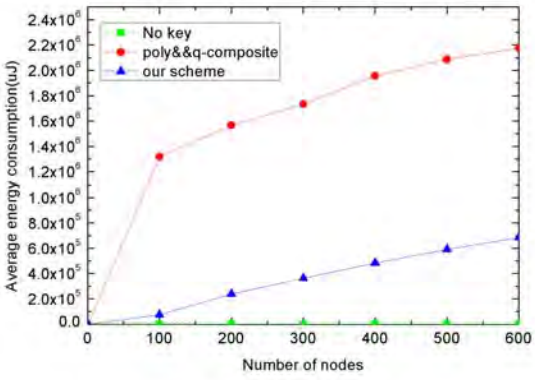

FIGURE III. THE ENERGY OVERHEAD AMONG DIFFERENT SCHEMES

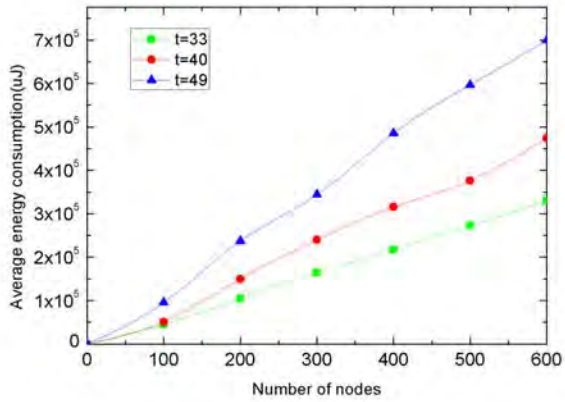

FIGURE IV. THE ENERGY OVERHEAD WHEN t=33, 40, 49

V. CONCLUSIONS

In this paper, a key management scheme of sub-regional based on bivariate symmetric polynomial key is proposed. Firstly, the sensors are deployed in the monitoring area randomly and the corresponding polynomials are stored in the sensor by region. And it increases the flexibility of the network with respect to the grid-based key distribution scheme in [5].Secondly, a certain number of key elements are stored in sensors by sub-regional in some certain rules, which make a higher connectivity among the sensors in the monitoring area. Finally, a hash function is generated by all of the common bivariate symmetric polynomials between any two communication nodes as the session key (according to the key distribution scheme in our scheme, the length of the hash chain that consists of the session keys has three possible: 4, 3, 1). The probability of unaffected communication link is closer to 0 among non-compromised sensors when t=49, the energy overhead is one magnitude less than the scheme in [6] under the same conditions.

ACKNOWLEDGEMENT

This work is supported by the Fundamental Research Funds for the Central Universities (ZYGX2015J054).

REFERENCES

[1] Neuman B C, Ts'o T. "Kerberos: an authentication service for computer network", IEEE Communications., vol. 32, no. 9, pp. 33-38, 1994.

[2] Messai M L, Seba H, Aliouat M. "A lightweight key management scheme for wireless sensor networks," The Journal of Supercomputing,vol. 71, no. 12, pp.4400–4422, 2015.

[3] Cheng X., Zhang X., Wu Y. "Analysis of WSN energy loss based on key pre-distribution Scheme", Communications Technology, vol.48, no.12, pp.1415–1420, 2015.

[4] Mary E. A.. "A novel hybrid key management scheme for establishing secure communication in wireless sensor networks," Wireless Personal Communication, vol.82, no. 3, pp. 1419–1433, 2015.

[5] Wang N C, Chen Y L, Chen H L. "An efficient grid-based pair-wise key pre-distribution scheme for wireless sensor networks," Wireless Personal Communication, vol. 78, no. 2, pp. 801–816, 2014.

[6] Kong T, Tao Q, Wu Y. "Research of Encryption in WSN based on Binary Symmetric Polynomial", Communications Technology, vol.48, no.8,pp.962–967,2015.