# Key Management Scheme for Wireless Sensor Networks

Yongjian Wang and Jing Zhao(✉)

National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, People's Republic of China
zhaojing_is_me@hotmail.com

**Abstract.** The paper designs a key management scheme for wireless sensor network that can resist key attack against the network. The scheme gives full play to the cluster head's resources such that the head can carry most of the computation, storage and communication overhead by the cluster head, and thereby achieves the minimum energy consumption of the cluster members and anti capture target, and key attack can resist wireless sensor network effectively. Through the simulation of the key management program in the authorization certificate issuance mechanism, and the development of the corresponding changes in the value of the parameters to assess the performance of each mechanism, it comes to the overall performance of the mechanism ultimately and how the value should be set to get the best performance. Simulation results show that compared with the traditional scheme, the proposed model can effectively improve the node's anti capture ability and reduce the node energy consumption.

**Keywords:** Wireless sensor networks · Key management
Authorization certificate issuing

## 1 Introduction

The wireless sensor network is a new type of wireless network technology that is completely different from the traditional wireless network. It relies on the wireless link to transmit data, which relieves the dependence on the wired network. It is more efficient, with high coverage, scalability and Reliability and other advantages to overcome the Ad Hoc network, wireless LAN, wireless personal area network, wireless MAN some restrictions, so wireless sensor networks are increasingly concerned by academics and the industry, especially wireless sensor network security issues [1–3]. The wireless sensor key management scheme is the security foundation of the wireless sensor network. In essence, the classical cryptographic scheme is used to solve the security of the wireless sensor network and prevent the network from being attacked.

In the paper, the wireless sensor network is distributed in a cluster, a cluster has a cluster head and a plurality of cluster members, the topology can be seen in Fig. 1. The cluster head is no special line communication equipment, computing, storage, communication and energy in other areas have higher ability; cluster members are ordinary sensor capacity low, to reduce the energy consumption, the provisions in the cluster members can only communicate with the cluster head.


C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 272–283, 2018.
https://doi.org/10.1007/978-3-319-90802-1_24

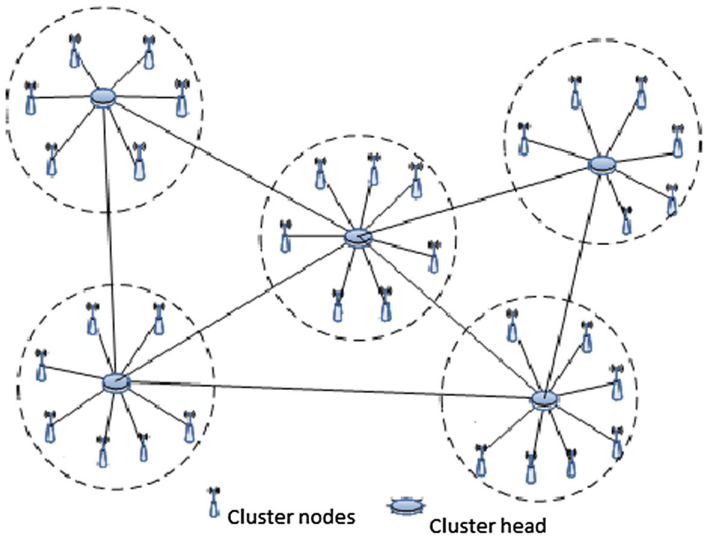


**Fig. 1.** Topology of wireless sensor network

There is a great difference in the wireless sensor network in this cluster and the cluster members of the allocation of resources, because the cluster head can carry high computation and communication overhead, so the key management can be used between a plurality of cluster head nodes distributed management, which can improve the anti capture and reduce storage. The cluster head is not balanced with the members of the cluster, and the traditional scheme of the flat network is directly applied to the inner layer with low efficiency and poor security. For example, Boujelben et al. Proposed probabilistic scheme is difficult to achieve full connectivity of the network, and the cluster head and cluster members have a large amount of key storage [4].

## 2 Key Management Architecture

Key management architecture mainly includes the initial key and certificate distribution module, identity based private key and certificate distribution module, key and storage module, key and certificate update module and authentication service module.

In the initial key and certificate assignment module, the following functions are mainly included: the offline CA assigns the public and private key pairs and the public key certificate for itself and each registered system member (user, regional router, backbone router); the offline CA assigns public and private key pairs for the system, and shares the system private key in the backbone router. The main function of identity based private key and certificate allocation module is the virtual CA which is formed by the backbone router. The main function of key and certificate storage module is to store public key certificate, authorization certificate and identity based private key. The main function of the key and certificate update module is to update the public key pair, the identity based private key, the public key certificate and the authorization certificate

when the system is abnormal and the system members join or leave. The main function of the authentication service module is to authenticate the user and authenticate the identity of each other before the members in the same area, adjacent or non-adjacent areas communicate with each other [5–8].

### 2.1 Preparation Knowledge

The N protocol is a set of N interactive probability algorithms. Each algorithm is a probabilistic polynomial complexity of interactive Turing machine, with participants $Ji$ expressed the $i$ algorithm. Each participant $Ji$ input $\alpha i \in \{0,1\}^*$. Random input $ri \in \{0,1\}^*$ and safety parameter $k$ input length. Non adaptive actual attacker $A$ is another interactive Turing machine, described by participants in the behavior of the adversary intrusion. The attacker's $A$ input includes the identity of the affected party and their respective inputs. The additional auxiliary input received by attacker $A$ is represented by $z$. The random input for $A$ is $r0$. If an attacker controls at least $\lambda$ participants, the attacker is bounded by $\lambda$. In each round of the calculation process, the honest party first generates the round of messages according to the protocol. The attacker mastered all the messages sent to the invaded participant. Then the adversary generates a message that is sent by the invading party. If the attacker is passive, then these messages are determined by the protocol. The active attacker generates the message sent by the participating party in any malicious way. The result is that all participants generate their own local output. The Honest Party's output is completely in accordance with the agreement, and the participants are exposed to a special symbol that they have been invaded. The attacker outputs an arbitrary function of its view. The attacker's view is composed of the following parts: auxiliary input, random input, input and random input of the participating party, and the message sent and received by the participating party during the whole calculation. Without losing generality, the attacker's output is assumed to consist of all of its views [9–12].

$ADVR\pi, A(k, \vec{\alpha}, z, \vec{r})$ represents the output of an attacker in the actual model, where $z$ is an auxiliary input $\pi$ is running protocol, $\vec{\alpha} = (\alpha 1, \alpha 2 \ldots . . \alpha n)$, $\vec{r} = (r0, r1 \ldots . . rn)$, $\alpha i$ and $ri$ are the input and random input of the $Ji$, $r0$ is the random input of the attacker. $EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})i$ is the output of the participant $Ji$. If $Ji$ is honest, then its output follows the protocol execution; If $Ji$ is invaded, then $EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})i = \perp$. In the actual protocol security model, the output of the protocol is $(EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})1, EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})2 \ldots . . . EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})n)$

**Definition 2-1 Calculates indiscernibility.** Called two random variable family $\{Xi|Xi \in Di, i \in I\}$, $\{Yi|Yi \in Di, i \in I\}$ polynomial time calculation cannot be distinguished (Use $\stackrel{c}{\equiv}$ to express), If the probability algorithm for each polynomial level is $M'$, each polynomial $P(n)$, and all the big integers $n$, it will have $|pr\{M'(Xi, i) = 1\} - pr\{M'(Yi, i) = 1\}| < 1/p(|i|)$

**Definition 2-2 Probabilistic polynomial computing Turing machine.** Given polynomial $P : N \rightarrow N$, for any interactive Turing entity M, at any time it runs (that is, any configuration of M), M the total number of steps up to $p(n)$, and $n = k + nI - no - k * nN$, $k$ is a security parameter, $nI$ is the total number of bit that is

currently written to the M input tape, $nN$ is the number of different Turing machines that have been written by M.

### 2.2 Key Distribution Management Scheme

Set $Ga, Gb$ as the $P$ order large prime multiplication group, $g$ as the generator of $Ga$, the bilinear pairings is $e(Ga, Ga) \rightarrow Gb$, where $e(R, g^r PK) = I$, $H$ is a collisionless hash function. The publicly parameters are $(Ga, Gb, g, P, e(R, g^r PK) = I)$. Cluster members (except cluster heads) use the formula $h = H(ID)$ to calculate the value of the cluster member $ID$, and make $PK = g^h$, then register $PK$ as identification of the cluster member in the cluster header.

#### 2.2.1 Initialization Phase

The initial stage is implemented in the robust subset of cluster head in the wireless sensor network. The so-called robust subset means: Each cluster member is communicated with a subset of the cluster head to obtain a session key, each such set of cluster header is called a robust subset. Cluster head that satisfies the condition randomly selects $\sigma$ where $\sigma \in Zp^*$, the cluster head generates the shared value $\{\sigma i\} i \in P$ of their $\sigma \in Zp^*$ according to the access structure $\Gamma$ (A subset of ownership structure). Sharing scheme to resist active attackers, active attackers can invade a subset of the attacker structure $A$. Each cluster head can get the share value $\{\sigma i\} i \in P$ of $\sigma \in Zp^*$, but the cluster head which not in the $\Gamma$ can't get any information about $\sigma \in Zp^*$. For every robust subset $R$, to meet any $B \in A$, there are $R - B \in \Gamma$. The process of generating shared value $\sigma \in Zp^*$ in $R$ in a distributed manner is as follows:

Each cluster head $Ji \in R$ randomly selects a $x \in Zp^*$ and uses the vector space verifiable secret sharing scheme to distribute the fragments of $x$ in the cluster head set $J$. $p$ and $q$ are prime numbers, and satisfy the conditions $q|p-1$. $g$ is a generator of $q$ order multiplication subgroup of $Zp^*$. Select a random vector $\vec{\eta} i = (\eta i^{(1)}, \eta i^{(2)} \ldots \eta i^{(r)}) \in (Zq)^r$, so that $\vec{\eta} i \cdot \psi(E) = xi$ is established, where $\psi : S \cup \{E\} \rightarrow (Zq)^r$ is a function that makes $P \in \Gamma$ if and only if $\psi(E) \in \langle \psi(Ji) \rangle Ji \in P$, $E$ is an entity outside the set $J$. $Ji$ sends fragment $xij = \vec{\eta} i \cdot \psi(Sj)$ to each cluster head $Jj$ in $J$, and $Ji$ also broadcasts a the promised value $\eta tt = g^{\eta i^{(t)}}$ for $\eta i^{(t)} (1 \leq t \leq r)$. Each participant $Jj \in J$ verifies the correctness of the fragment $xij$ that sent by $Ji$ by verifying whether the equation $g^{xij} = \prod_{t=1}^{r} (\eta it^{\psi(Jj)^{(t)}})$ is established. If the verification is not passed, $Jj$ opens a complain to the $Ji$. If the set of participant which have sent a complain to $Ji \in J$ does not belong to a subset of $A$, that is, there is an honest participant sends a complain to $Ji$, then the $Ji$ is rejected (terminated); Otherwise, that is, the complaint received by the $Ji \in J$ only from the attacker, then $Ji$ open the fragments $xij$ which be complained. If the above equation is not valid, then the $Ji$ is rejected (terminated). $Con \subset R$ represents the set of participants through the validation phase. The secret key $\sigma = \sum_{i \in Con} xi$ is randomly generated by $Con \subset R$. Each cluster head $Jj \in J$ calculates the fragmentation of $\sigma$, the fragmentation formula is $\sigma j = \sum_{i \in Con} xij$. Where

$Ej = g^{\sum_{i\in Con} xij} = \prod_{i\in Con} g^{xij} = \prod_{i\in Con}\prod_{t=1}^{r}(\eta it^{\psi(Sj)^{(t)}})$, The initial stage of cluster heads is defined as $(\ldots.xi,\ldots..\perp\ldots) \rightarrow (\sigma 1, \sigma 2\ldots..\sigma n)$, Where $xi$ is the input of the participants in $R$, the attacker no input.

### 2.2.2 Key Computation Phase

After generating the secret sharing value $\sigma$, all cluster heads can know the public commitment value $Ei = g^{\sigma i}(1 \le i \le n)$ of the $\sigma i$, and the current cluster member can get a session key $K$. Each cluster head $Ji \in Con$ broadcasts a ciphertext $(ri, si)$. The goal of this stage is to obtain the ciphertext $(ri, si)$ of plaintext $h^{\sigma i}$. The keyquery and calculation process is defined as $(\ldots.(ai, bi, h), \ldots.) \rightarrow (\ldots..(ri, si), \ldots.)$, where $ai, bi \in Zp^*$.

### 2.2.3 Key Generation and Distribution Phase

Each cluster head which output $(ri, si)$ (other outputs is L.) can form a subset of $\Gamma$. The cluster head selects $l \in RZ_P^*$ to send to the trusted network requester at first, cluster member calculates $R = g^{\frac{1}{h+l}}$ and sends it to the cluster head, the cluster header to verify whether the $e(R, g^l PK) = I$ is established to determine whether the members of the cluster are legitimate, then the cluster head in the permission set $C \in \Gamma$ can calculate the ciphertext $(r, s)$ of the session key $K = h^{\sigma}$:

$$r = \prod_{Ji\in C} ri^{\lambda i^Q} = g^{\sum_{Ji\in Q}\lambda i^Q \cdot bi} \bmod p, \quad s = \prod_{Ji\in C} si^{\lambda i^Q} = h^{\sigma}(yj)^{\sum_{Ji\in Q}\lambda i^Q \cdot bi} \bmod p$$

where $\lambda i^Q$ is the reconstruction factor, to make $\psi(E) = \sum_{Ji\in Q}\lambda i^Q \psi(Ji)$, $\sigma = \sum_{Ji\in Q}\lambda i^Q \cdot ai \bmod q$ is established, the cluster head $Ji \in Q$ will send the ciphertext $(r, s)$ to the cluster member $Uj$.

## 3 Authorization Certificate Issuing Mechanism

Before the two node communication, it will first go through the verification of each other's license certificate is legitimate before the formal communication. Authorization certificate is issued by the backbone router virtual CA. The paper uses the threshold-based multi-signature mechanism to issue the authorization certificate, and the reliability of the certificate is proved by mathematics. Authorization certificate issuing mechanism is as follows. N backbone router nodes choose to calculate open parameters; select a secure hash function; select a large prime p, q is a prime factor of p − 1. α is a q order generator of $Z_p^*$, $Z_p^*$ is a modular P integer group. Generally, $2^{511} \le$ p $\le 2^{512}$; $2^{159} \le$ q $\le 2^{160}$; calculation and disclosure $y = \alpha^s \bmod$ p; participant $B_i \in A$, calculation and disclosure $y_r = \alpha^{s_{ir}} \bmod$ p; The user U sub-signature is given by the formulas (3-1) and (3-2):

$$\delta_r = \mathrm{H}\ (\mathrm{m})b_r + (c_{i_r} + 1)s_{i_r} \bmod \mathrm{q} \tag{3-1}$$

$$sig_r(\mathrm{m}) = (w_r, \delta_r) \tag{3-2}$$

In the formula (3-1), $b_r$ is an integer randomly chosen [0, q − 1], m is user information, $c_{i_r}$ and $s_{i_r}$ can be obtained by formulas (3-3) and (3-4):

$$c_{i_r} = \prod_{1 \le j,r \le t, j \ne r} \frac{x_{i_j}}{x_{i_j} - x_{i_r}} \left(x_{i_r} = i_r\right) \tag{3-3}$$

$$s_{i_r} = h(x_{i_r}) \bmod \phi \ \left(x_{i_r} = i_r\right) \tag{3-4}$$

In the formula (3-2), $w_r = \alpha^{b_r} \bmod \mathrm{p}$ is published to all users, $sig_r(\mathrm{m})$ is the signature of the end user U. After receiving the sub-signature $sig_r(\mathrm{m})$, the end user U verifies whether the sub-signature is valid by the formula (3-5).

$$\alpha^{\delta_r} = w_r^{H(m)} y_r^{(c_{i_r}+1)} \bmod \mathrm{p} \tag{3-5}$$

Proof of formula (3-5):

$$\alpha^{\delta_r} = \alpha^{[H(m)b_r + (c_{i_r}+1)s_{i_r} + n_0 q]}$$

(Parameter $n_0$ is an integer; the other parameters are the same as the previous description)

$$= \alpha^{H(m)b_r} \alpha^{(c_{i_r}+1)s_{i_r}} \alpha^{n_0 q}$$

($\alpha^{n_0 q}$ equal unit element)

$$= \alpha^{H(m)b_r} \alpha^{(c_{i_r}+1)s_{i_r}}$$

$$w_r^{H(m)} y_r^{(c_{i_r}+1)} \bmod \mathrm{p}$$

$$= (\alpha^{b_r} + n_1 \mathrm{p})^{H(m)} (\alpha^{s_{i_r}} + n_2 \mathrm{p})^{(c_{i_r}+1)} \bmod \mathrm{p}$$

$$= \alpha^{H(m)b_r} \alpha^{(c_{i_r}+1)s_{i_r}} \bmod \mathrm{p}$$

If the Eq. (3-5) is established, the sub-signature is legal, otherwise the sub-signature is illegal.

## 4 Experiment Simulation and Result Analysis

### 4.1 Simulation Scenarios

Under the Window XP system, the paper uses the OPNET 10.5A simulation software to simulate the authorization of the key management scheme of wireless sensor network. The time distribution of authorization certificate issued by the main simulation

obtaining the initial key in different interval time and different requests and different threshold T, success rate and average distribution trend of delay, how to set the retransmission interval time, request time distribution and the threshold value of t to ensure the best performance of authorization certificate issued [13, 14].

An authorization certificate is issued for a simulation scenario with the following parameters:

(1) Scene scale: 300 m × 300 m;
(2) Main node types: 1 CA (Offline-CA), 32 Backbone-Router, 2 Zone-Route, 16 gt;
(3) Auxiliary node type: role configurator, application configurator, statistics center;
(4) Node transmission rate: backbone network using 54 Mbps, the regional network using 11 Mbps;
(5) The interval of retransmission (0.01 s, 0.60 s) (Fig. 2).

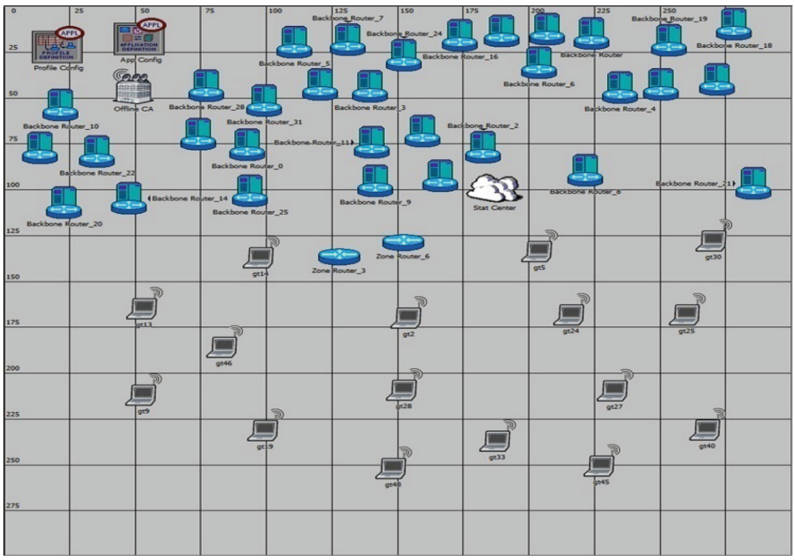

**Fig. 2.** Authorized certificate issued simulation scene

## 4.2 Simulation Results and Analysis

The simulation results of the success rate and average delay of the authorization certificate are shown in Figs. 3, 4, 5, 6, 7 and 8 in the case of the retransmission interval, the time distribution and the different thresholds of the different request issuing certificates: the abscissa is the time interval request issued by thee certificate of authorization; the success rate in the e curve diagram, the ordinate is the success rate in thee diagram, the average delay; authorization certificate issued, the ordinate is the average delay time distribution, unit is the second (s).

When the limit of system t value is 1, from the graph presented in Figs. 3 and 4 certificate success rate and average delay, the following conclusions can be drawn:

(1) When the interval is less than or equal to 0.03 s, the success rate is 0, and the average delay is also 0, which shows that when the t = 1, the backbone of the router in the shortest distance between the two adjacent routers is longer than 0.03 s.
(2) When the time interval is greater than 0.04 s, (0–1) to (0–5) the distribution of the success rate of the curves, and they were 100%, this shows that in the interval time is greater than 0.04 s, the success rate is not affected by request time distribution and retransmission interval time issued by the certificate of authorization.
(3) When the time interval is greater than 0.04 s, the average delay of the authorization certificate is not affected by the request time distribution and retransmission interval time issued by the certificate of authorization, the average delay of floating around 0.034 s, it will have a little change.

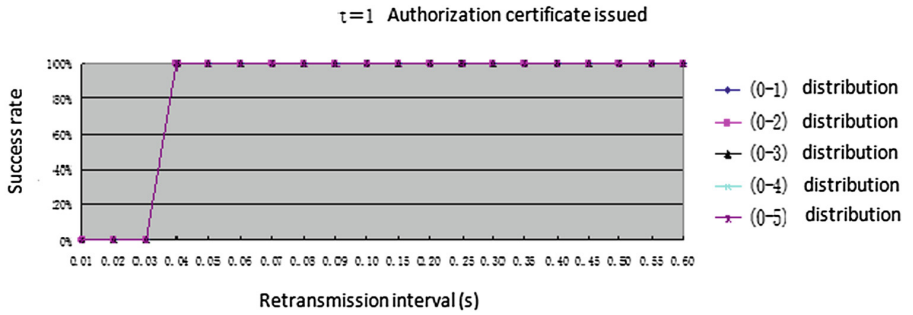


**Fig. 3.** t = 1 The success rate of the certificate issued

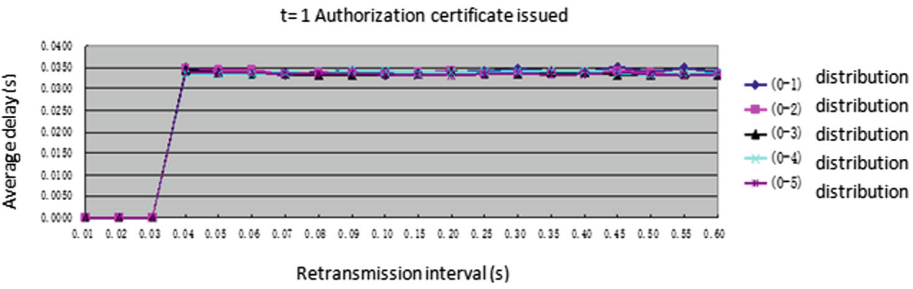


**Fig. 4.** t = 1 Average delay of authorization certificate

When the value of the threshold system t is 2, the success rate and the average delay graph of the certificate issued from Figs. 5 and 6 can be concluded as follows:

(1) As with t = 1, the success rate and average delay are 0 when the interval is less than or equal to.
(2) Retransmission interval is greater than 0.04 s, the interval time is 0.04 s, request distribution (0–1) distribution of the pole, (0–1) to (0–5) the distribution of the success rate was 100% and the curves, the success rate is: success rate is not affected by the request issued by the certificate of authorization of the time distribution of the cause; this is because the poles when t = 2, request authorization certificate for the 0.04 s and the retransmission interval (0–1) issued by the time in the distribution, there is a conflict caused by the relatively large, the success rate is 57%.
(3) Retransmission interval is greater than 0.04 s (0–1), in addition to the distribution of the average delay of volatility is relatively large, (0–1) to (0–5) at about 0.07 s the average delay distribution, it will have little change..

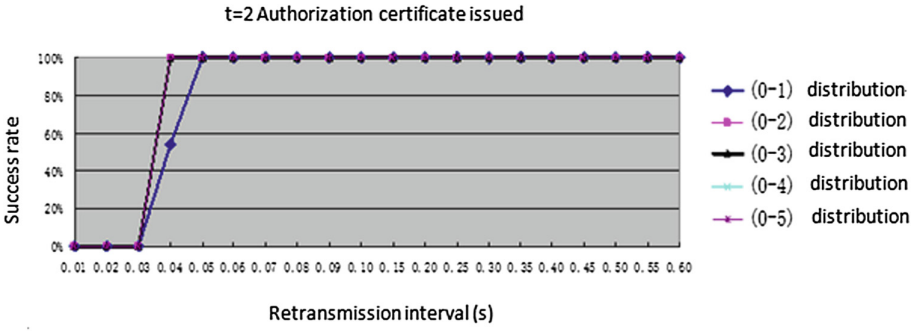


**Fig. 5.** t = 2 The success rate of the certificate issued

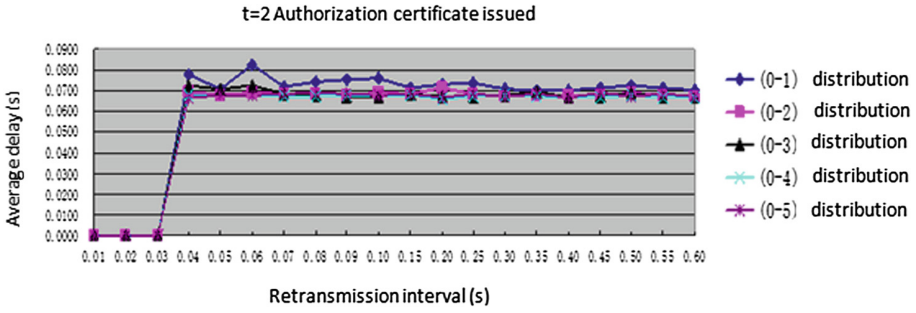


**Fig. 6.** t = 2 Average delay of authorization certificate

When the value of the threshold system t is 3, the success rate and the average delay graph of the certificate issued from Figs. 7 and 8 can be concluded as follows:

(1) When the interval is less than or equal to 0.03 s, the success rate is 0; after the interval is greater than 0.05 s, the success rate curve of (0–1) to (0–5) distribution coincidence, and the success rate of 100%;
(2) Retransmission interval between 0.03–0.05 s, (0–1) to (0–5) the success rate distribution curves are extreme, that when t is 3, interval between 0.03–0.05 s, (0–1) to (0–5) Certificate Authority issued certificate issued by the authorized distribution of failure process due to the existence of conflict;
(3) Retransmission interval is greater than 0.05 s, in addition to (0–1) the average delay curve fluctuates much distribution, (0–2) to (0–5) the average delay distribution curve is smooth, and are concentrated in the vicinity of 0.105 s.

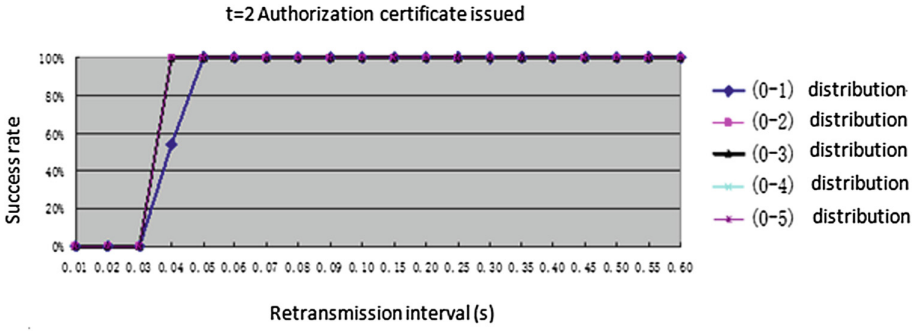


**Fig. 7.** t = 3 The success rate of the certificate issued

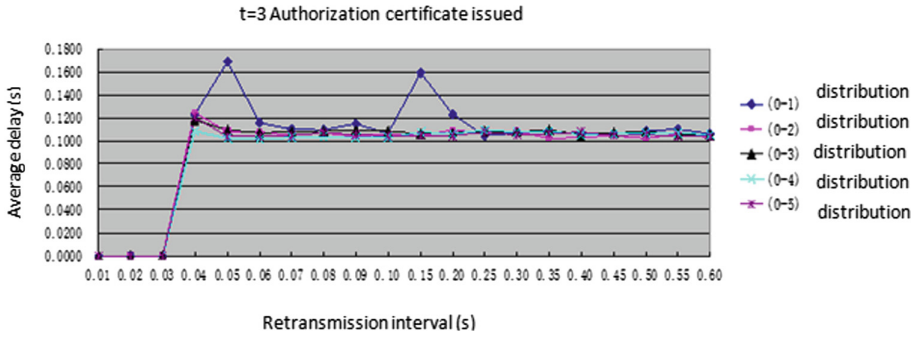


**Fig. 8.** t = 3 Average delay of authorization certificate

From the longitudinal comparison of the success rate and the average delay in Figs. 3, 4, 5, 6, 7, 8, 9 and 10, the following conclusions can be drawn:

(1) The retransmission interval should be at least greater than the distance between the nearest node of the backbone router and the backbone router;
(2) When the retransmission interval is greater than a certain threshold, the time distribution of the issuing certificate will have little effect on the success rate and the average delay;
(3) Retransmission interval is greater than a certain threshold value, the success rate of 100%, with the increase of t value, the threshold is more and more big, such as when t = 1, the threshold is 0.04 s; when t = 2, the threshold is 0.05 s; when t is 3, the threshold is 0.06 s;
(4) When the t value is low, the time distribution of the issuing certificate has little effect on the success rate, especially when t = 1, but with the increase of t value, the influence is more and more big;
(5) When the average delay is large, it will eventually approach a certain value. And with the increase of t value, this value is getting bigger and bigger;
(6) When t is the value, the greater the retransmission interval, the higher the success rate of the certificate issued, when the retransmission interval reaches a certain threshold, the success rate is 100%, the retransmission interval value is not the bigger the better, Otherwise it affects the delay in issuing a certificate of authorization.

## 5 Conclusion

The paper designs a set of wireless sensor network key management scheme, associating key information and node ID, which can effectively resist key attack in wireless sensor network, at the same time, the wireless sensor network model based on region can be used to deal with any scale of wireless sensor network and integrate different characteristics of subnet (such as sensor networks, Ad Hoc network access). When an area router suspects that a user's authorization certificate is false, the public key certificate issued by the offline CA can be used to verify the validity of the user; the user can grant the identity based private key and authorization certificate by any *t* backbone routers in *n* backbone routers; there are at least two backbone routers connected to Internet in the backbone network, and there are two regional routers connected to the backbone network, which improve the fault tolerance of the system.

## References

1. Huanyi, C., Qingsong, C.: Ad hoc technology and WMANET network architecture. Commun. World **1**, 44–45 (2003)
2. Brunno, R., Conti, M., Gregori, E.: Mesh networks: commodity multi-hop ad hoc networks. IEEE Commun. Mag. **43**(3), 123–131 (2005)

3. Whitehead, P.: Mesh networks: a new architecture for broadband wireless access systems. In: Radio and Wireless Conference, Denvor, CO, USA, pp. 43–46. IEEE Press, Piscataway (2000)
4. Li, C.: Study and research on wireless network authentication technology security based on 802.1x protocol. Comput. Secur. (10), 4–12 (2006)
5. Fowler, T.: Mesh networks for broadband access. IEE Rev. **47**(1), 17–22 (2001)
6. Rayner, K.: Mesh wireless networking. Commun. Eng. **1**(5), 44–47 (2003)
7. Tabata, K., Kishi, Y., Konishi, S., Nomoto, S.: A study on the autonomous network synchronization scheme for mesh wireless network. In: 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communications Proceedings, Beijing, China, pp. 829–833. IEEE, Piscataway (2003)
8. Kishi, Y., Konishi, S., Nanba, S., Nomoto, S.: A proposal of millimeter-wave multi-hop mesh wireless network architecture with adaptive network control features for broadband fixed wireless access. In: Proceedings RAWCON 2001, IEEE Radio and Wireless Conference, Waltham, MA, USA, pp. 17–20. IEEE, Piscataway (2001)
9. Akyidiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Comput. Netw. **47** (4), 445–487 (2005)
10. Prasad, N.R., Alam, M., Ruggieri, M.: Light-weight AAA infrastructure for mobility support across heterogeneous networks. Wirel. Pers. Commun. **29**(3–4), 205–219 (2004)
11. Houyou, A.M., De Meer, H., Esterhazy, M.: P2P-based mobility management for heterogeneous wireless networks and mesh networks. In: Cesana, M., Fratta, L. (eds.) EuroNGI 2005. LNCS, vol. 3883, pp. 226–241. Springer, Heidelberg (2006). https://doi.org/10.1007/11750673_18
12. Luo, H., Lu, S.: Ubiquitous and robust authentication, services for ad hoc wireless networks. Technical report 200030. UCLA Computer Science Department (2000)
13. Mizrak, A.T., Chen, Y.C., Marzullo, K., et al.: Detecting and isolating malicious routers. IEEE Trans. Dependable Secure Comput. **3**(3), 230–244 (2006)
14. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. In: First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK 2003, pp. 113–127 (2003)