Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 928174, 11 pages
http://dx.doi.org/10.1155/2015/928174

Research Article

A Novel Digital Certificate Based Remote Data Access Control Scheme in WSN

Wei Liang,[1] Zhiqiang Ruan,[2] Hongbo Zhou,[1] and Yong Xie[1]

[1]*Department of Software and Engineering, Xiamen University of Technology, Xiamen, Fujian 361024, China*
[2]*Department of Computer Science, Minjiang University, Fuzhou, Fujian 350108, China*

Correspondence should be addressed to Zhiqiang Ruan; rzq_911@163.com

Received 12 November 2014; Accepted 17 April 2015

Academic Editor: Fei Yu

A digital certificate based remote data access control scheme is proposed for safe authentication of accessor in wireless sensor network (WSN). The scheme is founded on the access control scheme on the basis of characteristic expression (named CEB scheme). Data is divided by characteristics and the key for encryption is related to characteristic expression. Only the key matching with characteristic expression can decrypt the data. Meanwhile, three distributed certificate detection methods are designed to prevent the certificate from being misappropriated by hostile anonymous users. When a user starts query, the key access control method can judge whether the query is valid. In this case, the scheme can achieve public certificate of users and effectively protect query privacy as well. The security analysis and experiments show that the proposed scheme is superior in communication overhead, storage overhead, and detection probability.

1. Introduction

The WSN is a dynamic wireless network formed by multiple microsensor nodes. It can be used for continuous environment monitoring. The nodes have the features of low consumption and low cost. Furthermore, they can realize data collection, data interaction, data transmission, and distributed cooperation [1–3]. However, WSN has some shortages, such as intrinsic vulnerability, limit sensor nodes, random deployed nodes, dynamic change of network topology, and unstable wireless channel. Furthermore, since WSN is always deployed in rugged environment, uninhabited area, or enemy positions, some unique security risks exist, such as intercept, leakage, denial of service, false injection, tampering, and replay attacks [4, 5].

In this case, it is an important issue to create a safe and reliable working scene for WSN, which relates to practicability and promotion of WSN. The features of sensor nodes are seriously limited in terms of calculating speed, power supply energy, communication ability, and storage space. Consequently, it is necessary to design an effective security mechanism under the limit conditions. In this way, the data stored in sensor nodes will be complete, confidential, and reliable and have the ability against intercept and capture in data transmission. The unauthorized query and sensitive information leakage of users are prevented.

Recently, data collection in sensor network needs users to pay for the access. Meanwhile, the privacy of data access is an inevitable problem. For instance, some users are not willing to leak the information about the time of accessing, interesting data type, and retrieved nodes. The identities are expected to be unknown to network owner and other users. In this way, they can protect their benefits from being damaged by potential competitors. Therefore, it is important to realize public user authentication while satisfying user anonymous requirement. So far, anonymous authentication is widely concerned but only on authentication problem. If the identity verification is successful, the nodes will provide data for user without considering anonymity. SPYC [6] is the first anonymous access control scheme by collecting data through one or several base stations. He et al. [7] present a distributed access control with privacy support in wireless sensor networks. All of users are divided into groups. Each group has various grades. In user query, the request is sent with group identity. It can authenticate user's validity and also protect privacy of user's identity. However, this way reveals user's privacy in dividing process. Since the number of groups is

limited, user's identity and his interesting data can be deduced by network provider with exhaustive analysis method. It is not a real distributed algorithm. Bethencourt et al. [8] propose a ciphertext policy attribute based encryption, called BSW scheme. Secret sharing method is employed in encryption for strict access control. The private key is related with characteristic set in BSW. An access structure is implicated in ciphertext. If the characteristic of private key satisfies the access structure, the private key can be used for decryption. In BSW, polynomial interpolation is required to reconstruct the key. Therefore, many operations of complex matching and exponentiation should be performed in decryption. Wang and Li [9] present an authorization method based on access control list (ACL). User will obtain ACL and certificate in advance. (n, t) threshold method is used in authentication. The signature employs the asymmetric encryption. If user obtains authentication signatures from t ($t < n$) nodes, the query request will be transmitted. The node with query data will verify and respond to the request. However, the scheme is low efficient and without expandability. Long distance data transmission faces various potential attacks. Cheung and Newport [10] replace secret sharing by random elements in encryption for strict access control. The scheme is named CN. There are two shortages. On one hand, it only supports simple logic combination strategy with low descriptiveness. On the other hand, the sizes of ciphertext and key grow linearly with the increase of the number of characteristics, which degrades efficiency. Ruan et al. [11] present a group-based anonymous scheme to conceal the message transmitted between source node and target node. They further proposed a proxy signature scheme to protect the access of data [12]. However, they focus on the privacy of data but not the privacy of users, which will be solved in this paper.

In our work, each user should get certificate before data collection, and the certificate should ask for or buy from network provider. User can access data with the certificate in the network. The sensor node will verify validity of the certificate and then provide the requested data to user. Each sensor node can verify validity of the certificate, but user's identity is unknown to all entities. In our scheme, the network provider can prevent unauthorized user access and protect user privacy. The generation of certificate is based on blind signature [13]. In traditional digital signature schemes, signer knows all information about his signature. But signer cannot get what he signed in blind signature system. The proxy blind signature is generated on proxy signature and blind signature, which is widely applied in payment of electronic currency and greatly protects user's benefits. Meanwhile, the proxy blind signature is suitable for the proposed application scenarios. However, anonymity of blind signature may be utilized by hostile users for unlimited access. Consequently, a novel safe access control algorithm based on digital certificate is proposed from the view of security requirement. It can address the security issues in access control.

2. Network Model and Hypothesis

As shown in Figure 1, suppose that there are a network service provider P, an intermediate proxy A, and some users U in WSN. N nodes in WSN continuously monitor target environment and provide interesting data to users. No reliable base station in network will connect intranet with outside network. The collected data will be restored in local nodes or other nodes. Therefore, user can obtain data directly from nodes. The nodes are supposed to know their geographical location information by existing locating algorithm.

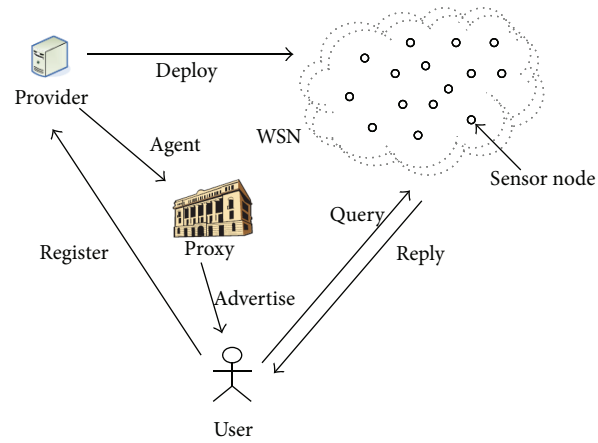


Figure 1: Distributed network access structure.

We suppose users can conspire, forge a certificate, and even capture part of nodes to obtain their interesting information. Users are not willing to reveal their identities and the way to access data but want to obtain information about other users as much as possible. Of course, they will have a sharp practice if it is profitable. Different from that of general wireless sensor network, users will not sponsor denial of service (DoS) since it is no good for data acquisition. Users will not escape access control and collect data by directly capturing many nodes since enormous costs and efforts are required. On the contrary, users will capture a small part of nodes for reuse of certificate.

3. User Authentication and Privacy Protection

3.1. Scheme Description. User access control includes three stages: proxy stage, certificate generation, and verification. The symbol description is stated as follows:

p, q: two big prime numbers satisfying $q \mid p-1$, q and $p-1$ being relatively prime,

g: an element with rank q in Z_p^*, named generator,

m: message needed to be signed,

m_w: a valid evidence of authorized intermediary proxy, including identity information about network provider, intermediary proxy, type of signed message, authorized scope, and valid date,

$x_P, x_A \in Z_p^*$: respective private keys of network provider and intermediary proxy,

$y_P = g^{x_P} (\mathrm{mod}\ p)$, $y_A = g^{x_A} (\mathrm{mod}\ p)$: respective public keys of network provider and intermediary proxy,

$H(\cdot)$, $h(\cdot)$: hash function with high security in cryptology,

$\|$: connection string.

3.1.1. Proxy Stage. Four steps are included in this stage:

(1) U sent registration information (without user's identity) to P,

(2) P randomly selects data $k \in_R Z_p^*$ and calculates $K = g^k (\mathrm{mod}\, p)$, $s = x_P + k \cdot H(m_w \parallel K) (\mathrm{mod}\, q)$,

(3) P transmits (K, s) and m_w to proxy A in a safe channel,

(4) A receives (K, s) and verifies if $g^s = y_P K^{H(m_w \| K)} (\mathrm{mod}\ p)$ is satisfied; if done, A accepts proxy task and further calculates proxy key with $s' = s + x_A$.

3.1.2. Certificate Generation. In this stage, the intermediary proxy A needs to do the following work.

(1) A randomly selects data $\lambda \in_R Z_p^*$ and calculates $t = g^{\lambda + x_A} (\mathrm{mod}\, p)$.

(2) A sends (K, t) to user U (user with certificate can access data on nodes).

(3) U receives the information and randomly selects data $a, b \in Z_p^*$ and calculates the following values:

$$\begin{aligned} \mu &= t^a \left(y_P y_A K^{H(m_W \| K)} \right)^{ab} (\mathrm{mod}\, p), \\ e &= h(m \parallel \mu) (\mathrm{mod}\, q), \\ e' &= a^{-1} e + b (\mathrm{mod}\, q). \end{aligned} \tag{1}$$

If $u = 0$, repeat step (3) until $u \neq 0$. After that, e' is sent to A.

(4) A receives e' and computes $s'' = e's' + \lambda + x_A$ as a signature of message. s'' is sent to U.

(5) U receives s'' and computes $\varphi = g^{s'' a} (\mathrm{mod}\ p)$. (m, m_w, φ, e, K) is regarded as proxy blind signature of message m, called certificate.

3.1.3. Verification. Each sensor node has y_P and y_A before deployment. Network provider can dynamically update y_P and y_A by using method in [14]. Once the certificate is obtained by user, U can access the WSN and collect data from nodes. Any node N_i that receives certificate (m, m_w, φ, e, K) will verify whether the equation $e = h(m \parallel \varphi (y_P y_A K^{H(m_W \| K)})^{-e} (\mathrm{mod}\, q)$ is satisfied. According to $e = h(m \parallel \mu) (\mathrm{mod}\, q)$, we only need to prove whether $\mu = \varphi (y_P y_A K^{H(m_W \| K)})^{-e} (\mathrm{mod}\, q)$ is satisfied. We have the following deduction process:

$$\begin{aligned} \varphi \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} &= g^{s'' a} \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} \\ &= \left(g^{e' s' + \lambda + x_A} \right)^a \\ &\quad \cdot \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} \\ &= g^{(a^{-1} e + b) s' a} \cdot t^a \\ &\quad \cdot \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} \\ &= g^{es'} \cdot g^{s' ab} \cdot t^a \\ &\quad \cdot \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} \\ &= \left(g^{s + x_A} \right)^e \cdot \left(g^{s + x_B} \right)^{ab} \cdot t^a \\ &\quad \cdot \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} \\ &= \left(g^{x_P + kH(m_W \| K)} g^{x_A} \right)^e \\ &\quad \cdot \left(g^{x_P + kH(m_W \| K)} g^{x_A} \right)^{ab} \cdot t^a \\ &\quad \cdot \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} \\ &= \left(y_P K^{H(m_W \| K)} y_A \right)^e \\ &\quad \cdot \left(y_P K^{H(m_W \| K)} y_A \right)^{ab} \cdot t^a \\ &\quad \cdot \left(y_P y_A K^{H(m_W \| K)} \right)^{-e} \\ &= t^a \cdot \left(y_P y_A K^{H(m_W \| K)} \right)^{ab} = \mu. \end{aligned} \tag{2}$$

The above expression proves the validity of certificate (m, m_w, φ, e, K). After that, N_i will check again. Only the two steps are successful: node N_i will provide data to user U according to the certificate.

3.2. Certificate Detection Algorithm. Each certificate (m, m_w, φ, e, K) consists of simple characters or digital number, which are unable to track. Hostile users may reuse their certificates and may not fear being caught. Therefore, node should verify whether the certificate is used before responding, called certificate detection. It performs before using certificate and after signature verification. The witness node is introduced for verifying abused certificates effectively.

Suppose the certificate is successfully used by user U for $a-1, a \geq 1$ times. Now, U attempts to use the uncompromised node N_i at ath time. The certificate (m, m_w, φ, e, K) is authenticated by the node N_i and should be verified if it is used. P represents the probability of certificate (m, m_w, φ, e, K) being abused in ath use (assume it is successfully used for $a - 1$ times). C denotes the communication cost for each data

transmission. M is the storage cost in ath use. N, r, c, and h are, respectively, nodes number, communication range, number of compromised nodes, and the average hops number between two nodes. In this section, three methods are presented to verify the use of certificate.

(1) Geography Mapping. Geography mapping (GM) is used in the first method. The way for selecting storage nodes is referenced. We randomly select a number of nodes as witness nodes. GPSR [13] is used to find witness nodes. Node N_i receives certificate (m, m_w, φ, e, K); after that, we randomly select b witness nodes with GPSR for certificate detection. The positions of witness nodes are calculated by $H(m, x) = \{l_i\}_{i=1}^{\beta}$. Here, H is the hash function and x is the random number. Node N_i will send m to b witness nodes and set the longest round-trip time of message. Each witness node w_i will judge if m is stored after receiving m. If not, certificate (m, m_w, φ, e, K) will be stored in local memory. Otherwise, w_i will respond to a passive message to node N_i.

Now, we will evaluate detection probability of GM method. b witness nodes are required to verify certificate (m, m_w, φ, e, K). x_i denotes the generated random number for determining witness position at ith time. One node may be selected in many times of selecting witness nodes. Assume the generated random number x_i in each time is independent. After the certificate being used for $a-1$ times, the number of witness nodes is $N_w(a-1)$. The probability of one node not being selected in $a-1$ times is denoted by $(1-b/N)^{a-1}$. In this case, the probability for one node being selected for one time at least will be $1-(1-b/N)^{a-1}$. Consequently, we have $N_w(a-1) = N(1-(1-b/N)^{a-1})$. If $b/N \ll 1$ is satisfied, we have $N_w(a-1) \approx N(1-(1-b(a-1)/N))$.

The nodes that are selected as witness nodes are unknown to user U. He can only capture some nodes randomly. Assume there are c nodes being compromised and $c < N$. The probability for witness node being compromised is $c(1-(1-b/N)^{a-1}) \approx (a-1)bc/N$. $b(a-1)(1-c/N)$ nodes are not compromised. If none of them is being selected as witness nodes, ath certificate detection fails and the probability is $(1-b/N)^{b(a-1)(1-c/N)}$.

Consequently, in GS method, the probability for verifying ath certificate abuse is

$$p = 1-\left(1-\frac{b}{N}\right)^{(a-1)b(1-c/N)} = \frac{b^2(a-1)(N-c)}{N^2}, \quad (a \geq 2). \tag{3}$$

ath detection requires $C = (b+\omega)h$ message transmissions. Here, ω is the number of uncompromised nodes that send passive message to node N_i. If $(a-1)b$ witness nodes are uncompromised, the probability for each node responding to a passive message is b/N. In this case, there are totally $\omega = (a-1)b^2/N$ passive messages. We have $C = (1+(a-1)b/N)bh$. Furthermore, the storage cost is $M \approx ab$.

(2) Path Feedback. The second method employs path feedback (PF). It is founded on GM and realized by using the broadcast feature of wireless signal. In the procedure of sending certificate (m, m_w, φ, e, K) for detection request, all nodes within communication radius of transmission path can receive request message. If one node finds m is stored by itself, it will send a passive message to source node. With the same number of b, PF can greatly improve detection probability of certificate. For example, assume that node w_i is one of b witness nodes selected by node N_i at ath time and it is not selected in $a-1$ times. In this case, w_i will record m. V is supposed to be a node at path, which acts as witness of certificate and can receive the detection request from node N_i to w_i. Different from GM method, PF allows node V at path to send a passive message to node N_i.

Now, we calculate detection probability of PF method. The hops number between arbitrary two nodes is h. For simplification, we assume N nodes are randomly deployed within the area S and there are $h+1$ nodes on each detection path from node N_i. The area of circular is $S_r = \pi r^2$. The intersect area of two adjacent circulars is $S' = (4\pi - 3\sqrt{3})r^2/6$. The area formed by H hops path is $S_h = hS_r - (h-1)S'$. There are b witness nodes, so the number of request messages is b. Therefore, the total area formed by b paths can be calculated by

$$\begin{aligned} S_b &= bS_h - (b-1)S_r \\ &= \frac{6\pi r^2 + \left(2(h-1)\pi + 3\sqrt{3}(h-1)\right)br^2}{6}. \end{aligned} \tag{4}$$

Similarly, there are c nodes being captured, $c < N$, and the probability is $c(1-(1-b/N)^{a-1}) \approx (a-1)bc/N$. The remaining $b(a-1)(1-c/N)$ witness nodes are uncompromised. If none of them has received the request message, ath detection is failure and the probability is $(1-S_b/S)^{b(a-1)(1-c/N)}$. Consequently, we have

$$p = 1-\left(1-\frac{S_b}{S}\right)^{(a-1)b(1-c/N)}. \tag{5}$$

Similar to that of GM method, the communication cost of PF is $C = (b+\omega)h$, $a \geq 1$. If none of $(a-1)b$ witness nodes are captured, one passive message will always respond with the probability of S_b/S. That is, the number of passive messages is $\omega = (a-1)S_b b/S$. So, we have $C = (1+(a-1)S_b b/S)bh$. In addition, the storage cost is the same as that of GM, $M \approx ab$. Obviously, PF has higher detection probability and lower communication cost and storage cost by comparing to GM:

$$p = 1-\left(1-\frac{S_b}{S}\right)^{(a-1)b(1-c/N)}. \tag{6}$$

(3) Crossline. The third method is based on crossline theory, called CL method. GM and PF have a common characteristic of compromise among detection probability, communication cost, and storage cost. More witness nodes will improve detection probability but also cause large communication cost and storage cost and vice versa. However, it is different in CL method. CL method is based on crossline technology [15].

Data storage is along with one direction, called "copy path," but not in one node or several isolated nodes. User query towards another direction is called "query path." If two paths are crossed, user can query expected data.

In CL method, certificate is regarded as a unique data type and message to be copied or queried. If certificate is received, each node will send a detection request along with any fixed vertical path. If the request is intersected with uncompromised witness nodes which have certificate record, the witness nodes will respond with passive message to source node. Otherwise, the certificate will be regarded as new. The source node will select any horizontal path and copy the certificate to all nodes on the path for storage.

Node N_i randomly generates a position $H(m, x_1)$ after receiving certificate (m, m_w, φ, e, K). x_1 is arbitrary random number. A proxy query request message with m will be sent to the node at $H(m, x_1)$ by using GPSR. The node, which receives the proxy query request and is near to $H(m, x_1)$, is called proxy query node of N_i, denoted by U_1. If m is stored in node U_1, U_1 will send a passive message to node N_i. Otherwise, U_1 will send the query request messages, respectively, along the horizontal and vertical directions. If node N_i receives an abused passive message before the timer expired, the use of certificate (m, m_w, φ, e, K) is refused. Otherwise, the certificate (m, m_w, φ, e, K) is unused. Node N_i will generate a random number x_2 (different with x_1) and send a copied proxy query request message including m to nodes nearby $H(m, x_2)$. The node U_2, which is closest to $H(m, x_2)$, is regarded as the copied proxy node of N_i after receiving the request message. Then, U_2 stores and sends two copy paths towards horizontal direction. All nodes on copy path will store m.

Now, we analyze the detection probability of CL method. The certificate (m, m_w, φ, e, K) is used for $a - 1$ times. Therefore, there are $a - 1$ copy paths randomly generated in network. At least one node can receive request message for detection. We assume only one node receives the request message. There are $a - 1$ cross nodes. Since the query path of node N_i is unpredictable, user U attempts to use certificate (m, m_w, φ, e, K) at ath time by randomly capturing a number of nodes. If c nodes are compromised by U, the probability of each cross node being captured is c/N. If all of the cross nodes are compromised, ath certificate detection is failure. The probability is $(c/N)^{a-1}$. So, we have

$$p = 1 - \left(\frac{c}{N}\right)^{a-1}. \tag{7}$$

The communication cost evaluation should consider two cases: ath detection is successful or failure. For the first case, communication cost includes query cost C_1 and copy cost C_2. C_1 consists of the cost of transmitting proxy query request and the cost of sending two query requests from proxy query node. C_2 consists of the cost of transmitting proxy copy request and the cost of sending two copy requests from proxy query node. The hops at horizontal and vertical direction are, respectively, L and W. The average hops number between arbitrary two nodes is h. Consequently, we have

$$C = C_1 + C_2 = (h + W) + (h + L) = 2h + W + L. \tag{8}$$

If ath detection is failure, C is a sum of C_1 and the sent passive messages. If $a - 1$ cross nodes are uncompromised, $a - 1$ passive messages will respond to node N_i. In this case, $C = h + W + (a - 1)h$. So, we have

$$C = (1 - p)(2h + L) + W + p(ah + W). \tag{9}$$

In addition, the storage cost of CL method is

$$M = (a - 1)L + (1 - p)L = (a - p)L. \tag{10}$$

3.3. Security and Performance Evaluation. Data access control is necessary to ensure authorized access, since illegal access to sensitive data may cause disastrous consequences. From the view of protected object, security evaluation of data access control is classified into accessor security and access object security. The implementation of our method is analyzed as follows.

(1) Effective access control: the master key in each stage is realized by encryption of a set of characteristics. Since the key chain is one-way, attackers cannot obtain the key for data encryption without the master key. Encryption on the master key has provable security under the BDH hypothesis. It demonstrates that attackers cannot decrypt the master key except that they have expectant access structure. Therefore, the method makes the data only be accessed by authorized user.

(2) Constraining the collusion attack: the collusive users want to obtain the master key for data decryption. Actually, the method has provable security to select message attack under BDH hypothesis. The master key is encrypted as $Ke(g, g)^{ys}$. User can get K only by eliminating $e(g, g)^{ys}$. The only way to construct $e(g, g)^{ys}$ is $e(g^{(y-b)/\beta}, g^{\beta s}) = e(g, g)^{ys}/e(g, g)^{bs}$. Then, $e(g, g)^{bs}$ can be calculated. For each user, b is randomly selected from Z_p. The key of an unauthorized user is no use for other users to calculate $e(g, g)^{bs}$.

(3) Limit impact of node capture: each sensor node only stores the key for current data encryption. The key used before will be erased. Due to the one-way feature of key, attackers cannot deduce previous keys by using current key. Each node encrypts data independently, which is not useful to capture other nodes.

(4) Performance and functionality analysis: a sensor node is responsible for the following operations: (1) generate and encrypt the master key with the proposed method; (2) generate the key for data encryption by using the master key; (3) encrypt data of sensor nodes. These operations are deployed to various stages. Concretely, one node at one stage performs at most one dot product of scalar at elliptic curve, a one-way hash algorithm, and a symmetry data encryption.

In data request procedure, each node responds to data $\langle C_v, \{D\}_{K_t}\rangle$ at tth period of vth stage. C_v includes $f_i + 1$ group members in G_1 and a group element in G_T. $\{D\}_{K_t}$ is data

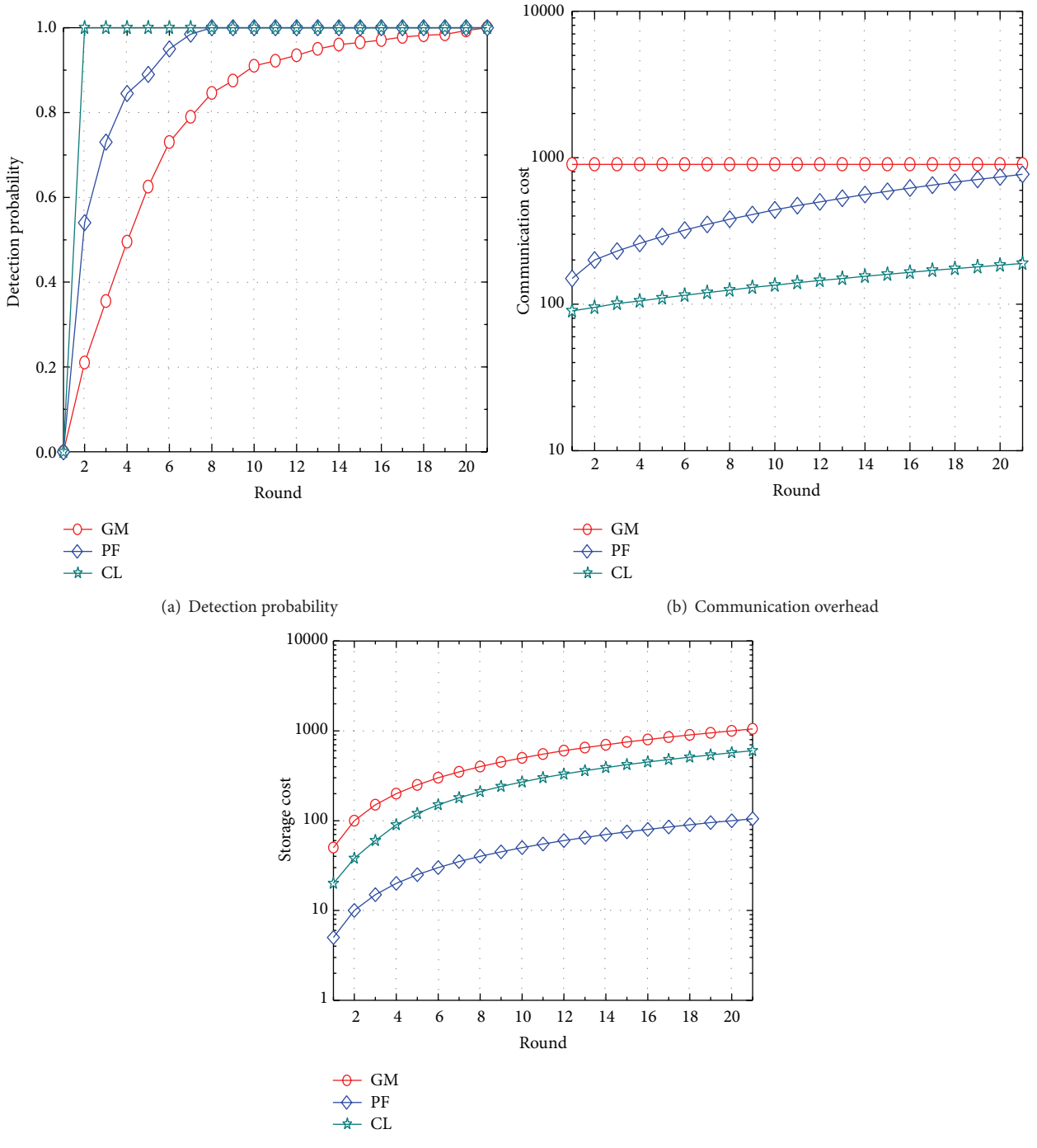


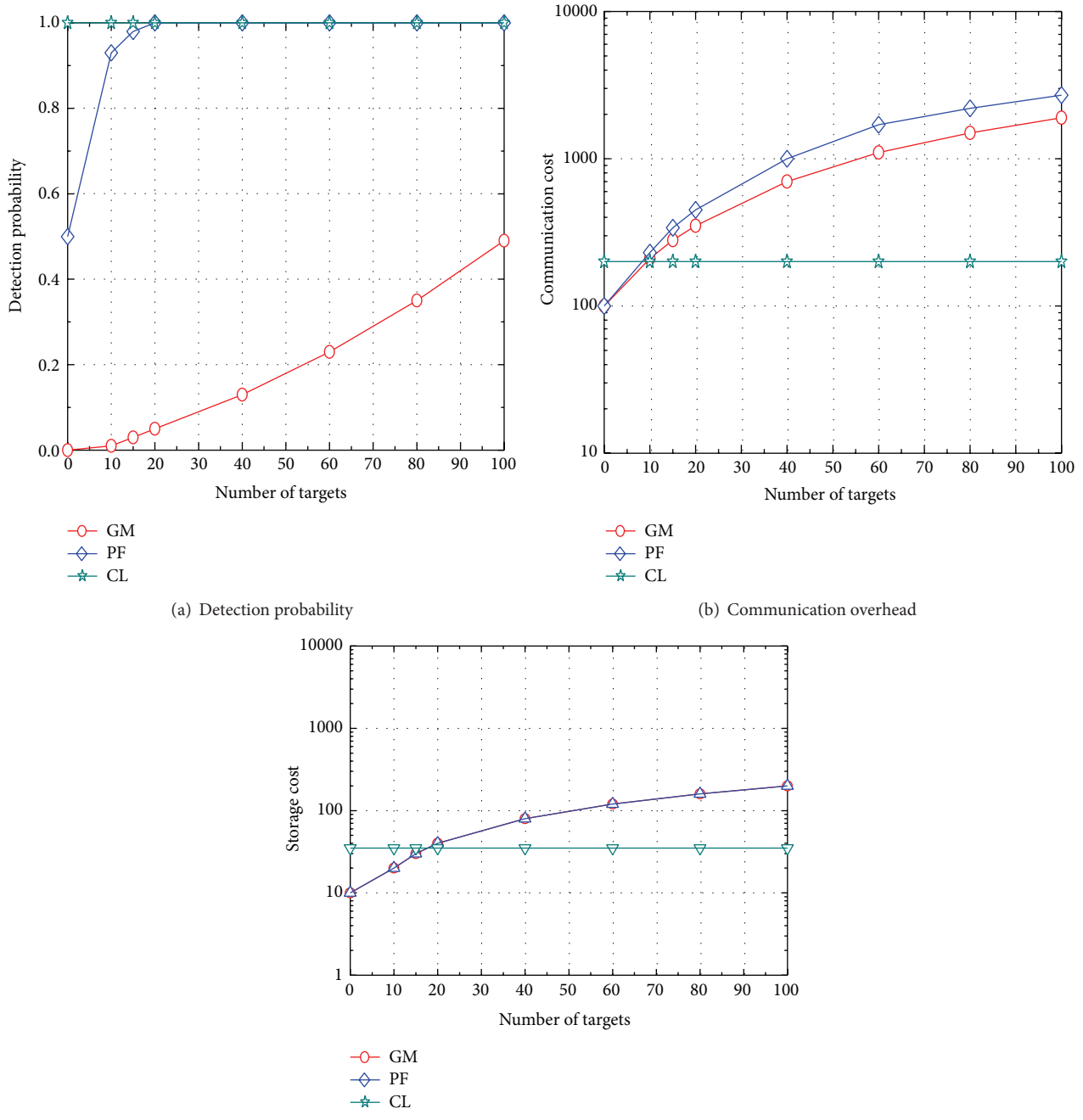
Figure 2: The relationship of detection rounds with detection probability, communication overhead, and storage overhead.

segment. In data cancel process, TP only needs to broadcast a group element in G_2 to all of sensor nodes.

Table 1 compares the functionalities of our method to those of BSW [8] and CN [10]. BSW has only designed threshold by simple combination of keys without network scalability and user revocation, and it can not withstand collusion attacks. CN is resilient to collusion attack and can resist some other attacks. The proposed method has scalability, ability against collusion attack, and user cancel. Meanwhile, the descriptiveness is better and functionality is more comprehensive.

4. Experiments and Analysis

Simulations have been performed in NS-2 (Network Simulator version 2), developed by UC Berkeley University, to



(a) Detection probability

(b) Communication overhead

(c) Storage overhead

Figure 3: The relationship of witness nodes with detection probability, communication overhead, and storage overhead.

Table 1: Functionality comparison of various methods.

Method	Scalability	Descriptiveness	Ability against collusion attacks	User cancel
Proposed	No	Normal	No	No
CN	No	Bad	Yes	No
CEB	Yes	Good	Yes	Yes

evaluate the efficiency of the proposed scheme. The settings for experiments are as follows. There are 1000 nodes in WSN deployed in the area with the size of 1000 × 1000. The communication radius of nodes is 50 m. The numbers of witness nodes (b) in GM and PF are, respectively, 50 and 5. The reason of choosing different b lies in their different detection probability. The number of compromised nodes is set to 100. Assume that no package loss or conflict occurs in data transmission. In Figure 2, every point represents the average usage of a certificate among 100 random nodes. For the use of each certificate, we randomly capture nodes for 100 times and calculate the average value. In addition, different network topology and random certificate are simulated. The evaluation indicators include detection probability, communication cost, and storage cost [15].

Figure 2(a) compares the detection probability of three methods as a function of the round of certificate used. As seen, the detection probability increases as a. When a is greater than 2, it can be completely detected. Since CL selects two cross curves to store and verify certificate, if the cross point is not captured, detection will be successful. But the detection probability is the minimum. On the contrary, the selection of target nodes in GM is totally random. It is not the optimized way for selection since a part of nodes may be captured, and certificate usage can be detected more than 8 times. By comparing to GM scheme, PF can realize feedback by using nodes on the path. Since b nodes will produce b paths, it is unable to capture nodes on all paths. Consequently, the detection accuracy is higher than that of GM scheme while requiring less witness nodes.

Figures 3(a), 3(b), and 3(c) compare the communication overhead and storage overhead of three detection schemes, separately. As we can see, the communication overhead in CL is lower than that of PF, but the storage overhead is opposite. In GM scheme, communication and storage overhead are larger than those of PF. This is because the witness nodes in GM are fixed and the number of witness nodes is more than that in PF. Since PF depends on other nodes and witness nodes on the path and requires less witness nodes, the communication and storage overhead are lower than those of GM.

Figure 3 demonstrates the effect of b on GM and PF. Due to the fact that we concern certificate use at the first time, $a = 2$ is set. Additionally, b has no impact on CL scheme. For comparison, it is also shown. As seen, the detection probabilities, respectively, in GM and PF are growing as b. The communication and storage overhead show the same tend. When $b = 10$, PF can detect the first abuse of certificate with the probability of 0.9. But in GM, the detection probability is less than 0.5, even $b = 100$. Since PF lets other nodes on the path responding to a passive message to the source node when detecting a message, it introduces higher communication overhead than GM. Moreover, when b is larger than 20, the detection probability of PF is close to 1. The communication and storage overhead are grown continuously as well. Consequently, a compromise should be chosen among detection probability, communication overhead, and storage overhead.

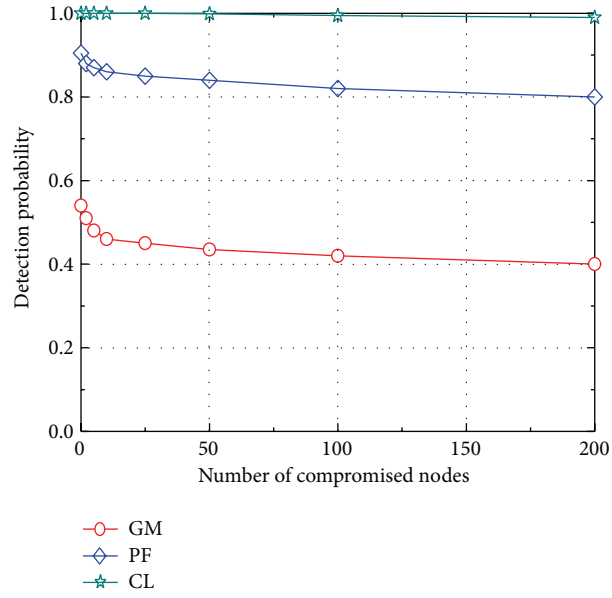


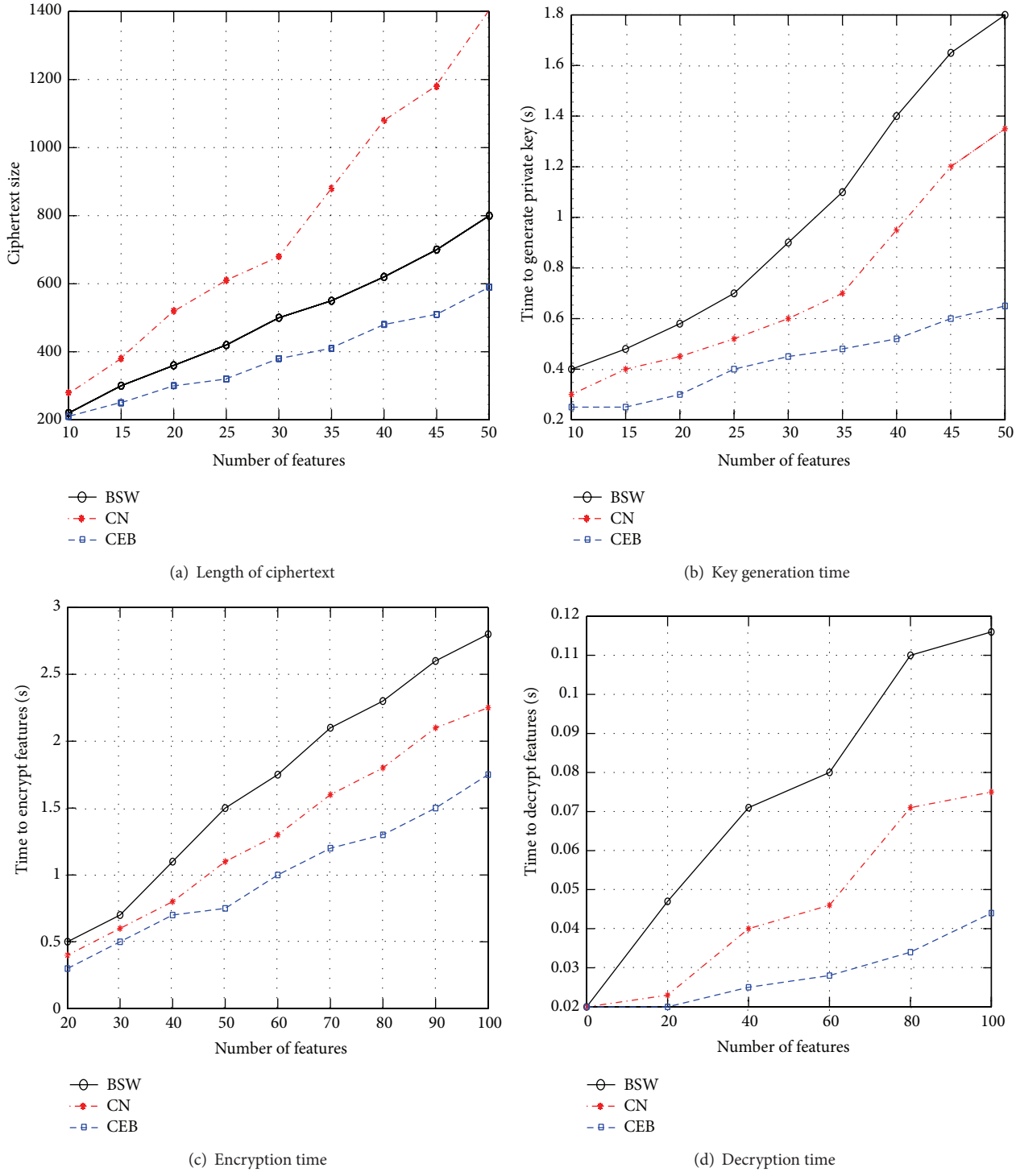
Figure 4: The relationship between detection probability and compromised nodes.

Figure 4 shows the detection probabilities in three schemes with increase of compromised nodes. We set $a = 2$ and $b = 50$ in GM and $b = 10$ in PF. In Figure 3, three schemes are affected by c since the number of witness nodes is random. For instance, CL can detect certificate being abused firstly with the probability of $p = 98\%$. Because many nodes on copy path may receive detection request message, it demonstrates that the scheme has good effect on capturing attacks.

In the following, we simulate various performance indicators after applying our scheme, including length of ciphertext, key generation time, and time overhead on encryption and decryption. These indicators are compared to BSW and CN. In finite field, a super singular ellipse curve $y^2 = x^3 + x$. The time to match with PCB library is 5.5 ms. The time of selection random elements from G_1 and G_2 are 16 ms and 1.6 ms, respectively.

Figures 5(a)–5(d) show the comparison with length of ciphertext, key generation time, encryption time, and decryption time. Ciphertext includes ID, head, and data block. The head consists of characteristic collection f, a group element in G_2, and $|f|$ group elements in G_1.

As we can see, the length of ciphertext, key generation time, and encryption time linearly increase as the number of characteristics in all three schemes. But the decryption time is not linear. Since the decryption time is related to the number of characteristics and access trees, different access tree may include different access structure. Moreover, the indicators in CEB are superior to that of other schemes. Because secret sharing is employed in encryption of BSW, serious access control is realized. Polynomial interpolation is required to construct key. Many complex matching and exponentiation operations are required in decryption. Although CN scheme replaces secret sharing with random elements in encryption, the length of ciphertext and key linearly increase as the



(a) Length of ciphertext

(b) Key generation time

(c) Encryption time

(d) Decryption time

Figure 5: The comparison of various schemes.

number of system characteristics. It causes low efficiency of CN scheme. However, our scheme encrypts and stores data periodically. The data of each node is encrypted by symmetric encryption algorithm. Meanwhile, the keys in encryption are linked as a one-way key chain. One key is used in a period.

The abilities against collusion attacks of three schemes are compared in Figure 6. Simply, we assume each node only generate one data unit at each phase of per round. The total number of users in current network is supposed to be 100. The collusion users vary from 10 to 50. Then we simulate data leaking rate of three schemes.

As a note, the purposes of collusion users are to obtain more data with the key. By comparing with directly capturing node and intercepting attacks, collusion can save overhead

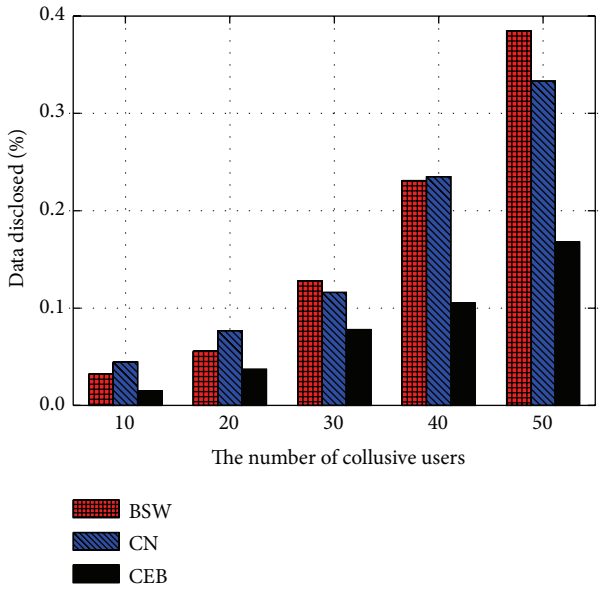


Figure 6: The comparison of abilities against collusion attacks for three schemes.

and is hard to be detected [16]. As shown in Figure 6, three schemes have almost the same abilities against attacks when there are few collusion users. With the growth of collusion users, data security of BSW and CN decreases rapidly, while that of our scheme shows a gentle decline. When the number of collusion users is greater than 40, data security of BSW scheme drops more dramatically than that of CN. As mentioned above, although CN generates key by utilizing the way of random number, actually, the number belongs to pseudorandom number. Attack can be realized with exhaustive method, easily with more collusion users. The proposed scheme has eliminated the above advantages. The master key is continuously updated. Once malicious users are found, we will cancel the operation. In this case, collusion users can only obtain their own data without obtaining data of other nodes. Therefore, the interference caused by attacks will be restricted to be the minimum.

5. Conclusion

To address the issue on security of access object and accessor, we proposed a digital certificate based remote data access control scheme. It is founded on access control scheme with characteristic expression. Our scheme has two features. On one hand, the network data is divided by characteristic and connected with key. When user requires query, the access control strategy, which is related to key, will judge the validity of the query. In this way, data access control is realized. On the other hand, anonymous authentication is realized for security of accessor. Moreover, three distributed certificate detection methods are designed for preventing certificate being abused by malicious anonymous users. The security analysis and experiments show that our scheme has the ability against collusion attacks and higher detection probability. The next work is to perfect our scheme and apply it on real sensor nodes. The experiments are summarized as follows. GM has lower detection probability, or higher communication and storage overhead are required to achieve some detection probability. PF has higher detection probability but grows as witness nodes and successful use times of certificate. Meanwhile, the communication and storage overhead of PF are within a reasonable range. The case of CL scheme is similar to that of PF.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the China Postdoctoral Science Foundation funded project (Grant no. 140778), the Natural Science Foundation of Fujian Province (Grant no. 2014J05079), the Young and Middle-Aged Teachers Education Scientific Research Project of Fujian province (Grant nos. JA13248 and JA14254), the special scientific research funding for colleges and universities from Fujian Provincial Education Department (Grant no. JK2013043), the Scientific Research Project of Minjiang University (Grant no. YKQ13003), and the Research Project supported by Xiamen University of Technology (YKJ13024R, XYK201437).

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] P. Levis, S. Madden, J. Polastre et al., "Tinyos: an operating system for sensor networks," in *Proceedings of the 6th International Conference on Mobile Data Management (MDM '05)*, pp. 115–148, IEEE, Nara, Japan, 2005.

[3] S. Bhatti, J. Carlson, H. Dai et al., "Mantis os: an embedded multithreaded operating system for wireless micro sensor platforms," *Mobile Networks and Applications*, vol. 10, no. 4, pp. 563–579, 2005.

[4] C. Han, R. Kumar, R. Shea et al., "A dynamic operating system for sensor networks," in *Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services (MobiSys '05)*, pp. 163–176, Seattle, Wash, USA, 2005.

[5] C. Karlof and D. Wangner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, IEEE, Anchorage, Alaska, USA, May 2003.

[6] B. Carbunar, Y. Yu, L. Shi, M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," in *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07)*, pp. 203–212, June 2007.

[7] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3472–3481, 2011.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, Calif, USA, May 2007.

[9] H. Wang and Q. Li, "Distribuled user access control in sensor networks," in *Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS '06)*, pp. 305–320, Berlin, German, 2006.

[10] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 456–465, Alexandria, Va, USA, November 2007.

[11] Z. Ruan, W. Liang, D. Sun, H. Luo, and F. Cheng, "An efficient and lightweight source privacy protecting scheme for sensor networks using group knowledge," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 601462, 14 pages, 2013.

[12] Z. Ruan, X. Sun, and W. Liang, "Securing sensor data storage and query based on *k*-out-of-*n* coding," *International Journal of Communication Systems*, vol. 26, no. 5, pp. 549–566, 2013.

[13] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 243–254, ACM, Boston, Mass, USA, August 2000.

[14] Z.-W. Tan, Z.-J. Liu, and C.-M. Tang, "A proxy blind signature scheme based on DLP," *Journal of Software*, vol. 14, no. 11, pp. 1931–1935, 2003.

[15] R. Sarkar, X. Zhu, and J. Gao, "Double rulings for information brokerage in sensor networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 6, pp. 1902–1915, 2009.

[16] N. Subramanian, K. Yang, W. Zhang et al., "Ellips: privacy preserving scheme for sensor data storage and query," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM '09)*, pp. 936–944, Rio de Janeiro, Brazil, 2009.