Hindawi
Mathematical Problems in Engineering
Volume 2018, Article ID 7379364, 19 pages
https://doi.org/10.1155/2018/7379364

Research Article

WPKI Certificate Verification Scheme Based on Certificate Digest Signature-Online Certificate Status Protocol

Ke Gu,[1,2,3] **Na Wu**,[1] **Yongzhi Liu**,[1] **Fei Yu**,[1] **and Bo Yin**[1]

[1]*School of Computer & Communication Engineering, Changsha University of Science & Technology, Changsha 410114, China*
[2]*Hunan Provincial Key Laboratory of Intelligent Processing of Big Data on Transportation, Changsha University of Science & Technology, Changsha 410114, China*
[3]*School of Information Science and Engineering, Central South University, Changsha 410083, China*

Correspondence should be addressed to Ke Gu; gk4572@163.com

Received 17 May 2017; Revised 26 September 2017; Accepted 1 November 2017; Published 11 February 2018

Academic Editor: Yakov Strelniker

Aiming at the problems of the WPKI certificate verification schemes based on online certificate status protocol (OCSP), this paper proposes a WPKI certificate verification scheme based on the certificate digest signature-online certificate status protocol (CDS_OCSP). Compared with the existing schemes, the proposed scheme optimizes the number of communication connections between the communication entities and the network, reduces the consumption of the wireless network bandwidth in the certificate verification process, and uses the elliptic curves cipher- (ECC-) based encrypting/decrypting functions to sign and verify the certificate digest, which ensures the consistency of the verified certificates among the communication entities. The proposed scheme makes the certificate verification process more efficient and secure. The experimental results show that the proposed scheme effectively reduces the communication consumption of the wireless network and saves the storage space of the wireless entities.

1. Introduction

With the rapid development of wireless network, mobile e-commerce has become an important commerce transaction method. WPKI (Wireless Public Key Infrastructure) is the main solution for the security of mobile e-commerce [1, 2]. In the entire mobile e-commerce transactions, the WPKI mechanism provides the issuance and verification of the certificates and ensures the validity and legitimacy of the certificates [3, 4]. The WPKI mechanism is designed as the public key infrastructure scheme for wireless network environment [1], which provides the digital certificate issuance and management, the user identity authentication, the digital certificate verification and authentication, the transmission content confidentiality and integrity protection, and so on. The WPKI mechanism is a set of key and certificate management system which conforms to the established standards, by introducing the PKI (Public Key Infrastructure) mechanism from the wired network into the wireless network. Thus, based on the characteristics of wireless network, the WPKI mechanism provides users with security services, such as identity authentication, access control and authorization, transmission confidentiality and integrity, and nonrepudiation.

1.1. WPKI Structure and Certificate Format

1.1.1. WPKI Structure. WPKI is a key management system [1, 3] composed of mobile terminal entity (MTE), PKI Portal, CA (Certificate Authority), PKI Directory Server, OCSP Server, and so on. In practical applications, WPKI also involves content server, WAP (Wireless Application Protocol) Gateway, and other service equipment. The basic structure and data flow are shown as Figure 1.

In Figure 1, mobile terminal entity stores the optimization software designed for the WAP device. Its functions include (a) generating, storing, and allowing access to the user's public/private key pair; (b) initializing certificate application; (c) certificate update request; (d) certificate revocation

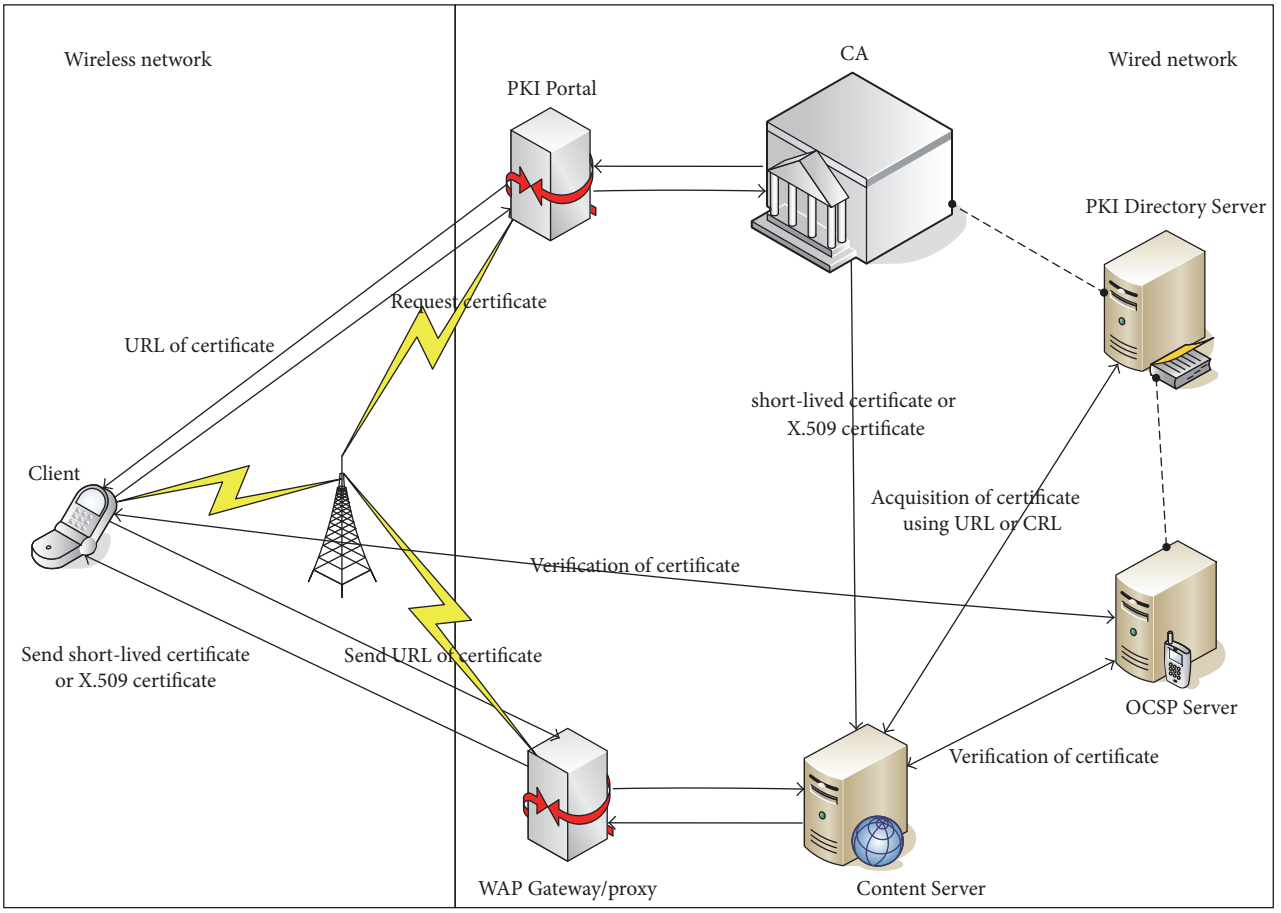

Figure 1: WPKI mechanism structure and data flow.

request; (e) querying, restoring, and revoking certificate; (f) verifying certificate and reading the contents of certificate; (g) generating and verifying digital signature. As a bridge between the mobile terminals and the current PKI, PKI Portal is responsible for the interoperating between the mobile terminals in the wireless network and the CA in the wired network. Certificate Authority (CA) is responsible for generating, issuing, and refreshing certificates. PKI Directory Server (PKI Catalog Server) stores the PKI Certificate catalog, which periodically updates the database. OCSP responder (OCSP Server) is responsible for verifying the validity of certificates and keeping their databases up-to-date with the CA or as a system with the CA. Content Server is responsible for providing content services to the users. WAP Gateway/Proxy is responsible for handling the protocol conversion between the mobile terminals and the content server.

1.1.2. Certificate Format. WPKI certificates have two kinds of certificates [1, 5, 6], respectively, wireless X.509 certificate and short-lived certificate, where wireless X.509 certificate omits some of the public key certificate fields and reduces the storage space of the certificate; compared with the wireless X.509 certificate, the short-lived certificate not only omits some of the certificate fields but also reduces the length of the key by using the elliptic curve cryptography (ECC) [7, 8] so as to reduce the overall length of the certificate. The format of the two certificates is shown in Tables 1 and 2.

1.2. WPKI's Certificate Verification Scheme. Currently wireless X.509 certificate and short-lived certificate are used in WPKI mechanism. Because the life cycle of the short-lived certificate is fixed, the verification of the short-lived certificate needs to check whether the certificate is legal, it does not need to verify whether the certificate expires [9, 10]. However, the wireless X.509 certificate not only needs to verify its legitimacy but also to check whether the certificate expires, so the verification of the wireless X.509 certificate needs a more complex certificate verification scheme. In the current WPKI mechanism, there are the certificate revocation list (CRL) scheme, the OCSP scheme and other extended schemes based on CRL or OCSP [9, 11], where the CRL scheme and the OCSP scheme are widely used.

(1) CRL scheme: the CRL scheme is a simple certificate verification scheme. In the CRL scheme, the CA periodically issues a certificate revocation list, and then all clients download the latest CRL from the verified CRL distribution points and check whether the certificates

Table 1: The format of wireless X.509 certificate.

	Generation	Process
Basic Field	m	m
Version	m	m
Serial number	m	m
Signature	m	m
Issuer	m	m
Validity	m	m
Subject	m	m
Subject public key info	m	m
Issuer unique identifier	x	x
Subject unique identifier	x	x
Extension field		
Authority key identifier	m	o
Subject public identifier	m	o
Key Usage	m	m
Private key usage period	x	x
Certificate policy	m	m
Policy mapping	-	-
Subject alternative names	m	m
Issuer alternative names	o	m
Subject directory attributes	x	x
Basic constraints	x	x
Name constrains	-	-
Policy constrains	-	-
Extended key usage	o	m
CRL distribution points	m	o
Domain information	o	o
Authority information access	m	o

m: mandatory; *o*: optional; x: not recommend; -: not defined.

Table 2: The format of short-lived certificate.

Filed	Value	Generation/process
Version	V1	m
Signature algorithm	ECDSA	m
Issuer	⟨Text⟩	m
Valid not before	Time	m
Valid not after	Time	m
Subject	⟨Text⟩	m
Public key type	ECDH	m
Parameter specifier	operation	m
Signature	ECDSA signature	m

have expired. Although the CRL scheme is simple and easy to be implemented, it also has many shortcomings, such as large amount of data transmission, long verification time, large computation cost, and inconsistent issued data (certificate revocation list).

(2) OCSP scheme: the OCSP scheme is a protocol proposed by the IETF's PKIX working group in RFC2560 [1, 2]. Compared with the certificate revocation information provided by CRL, it can meet the requirement of more timely operation, so the OCSP scheme can be used as a substituting or supplementary mechanism of CRL. OCSP is a typical client/server (CS) mode protocol in which the OCSP client sends a certificate status query to the OCSP server (OCSP responder) and waits for the response, where the query from the OCSP client may be signed. After receiving the certificate status query request from the OCSP client, the OCSP server queries the local database to obtain the certificate status information, then signs the status response information, and sends it to the OCSP client. The response information includes the certificate status, the time of the certificate update, and the next time of the certificate update [9], where the certificate status has three states, which, respectively, are "good," "revoked (hold)," or "unknown." In the WPKI mechanism, the OCSP scheme is shown in Figure 2: the mobile terminal applies for a transaction to the content server; after obtaining the transaction request, the content server requests the CA certificate and the ARL (Authority Revocation List) from the directory server, and then the directory server sends the CA certificate and the ARL to the mobile terminal and at the same time the content server sends its own certificate to the mobile terminal; after obtaining the CA certificate, the ARL, and the content server certificate, the mobile terminal sends a request to the OCSP server to verify the certificate status of the content server, and then the OCSP server sends the response result to the mobile terminal after querying the certificate status.

1.3. Our Contribution. With the improvement of computing performance and storage space of mobile terminals, we design the WPKI mechanism from the combination viewpoint of performance and security. Therefore, according to the works of [9, 10, 12–15], we improve the certificate verification scheme based on OCSP. In this paper, our contributions are as follows:

(1) Based on the related works [10, 13–15], we improve the interaction process between the communication entity and the network in the whole certificate verification: (a) we optimize the number of connections between the wireless communication entity and the wired network, and during the certificate verification process, the content server sends the OCSP query request directly so as to reduce the time and the consumption of wireless network bandwidth, compared with that the mobile terminal sends the query request; (b) we reduce the time and the consumption of network bandwidth when wireless communication entity needs to download the certificate; compared with the works [10, 13–15], the wireless communication entity does not need to download the CA certificate and the ARL in our the proposed scheme; thus the verification process of the CA certificate is committed to the OCSP server; although the directory server needs to send the mobile terminal certificate to the content

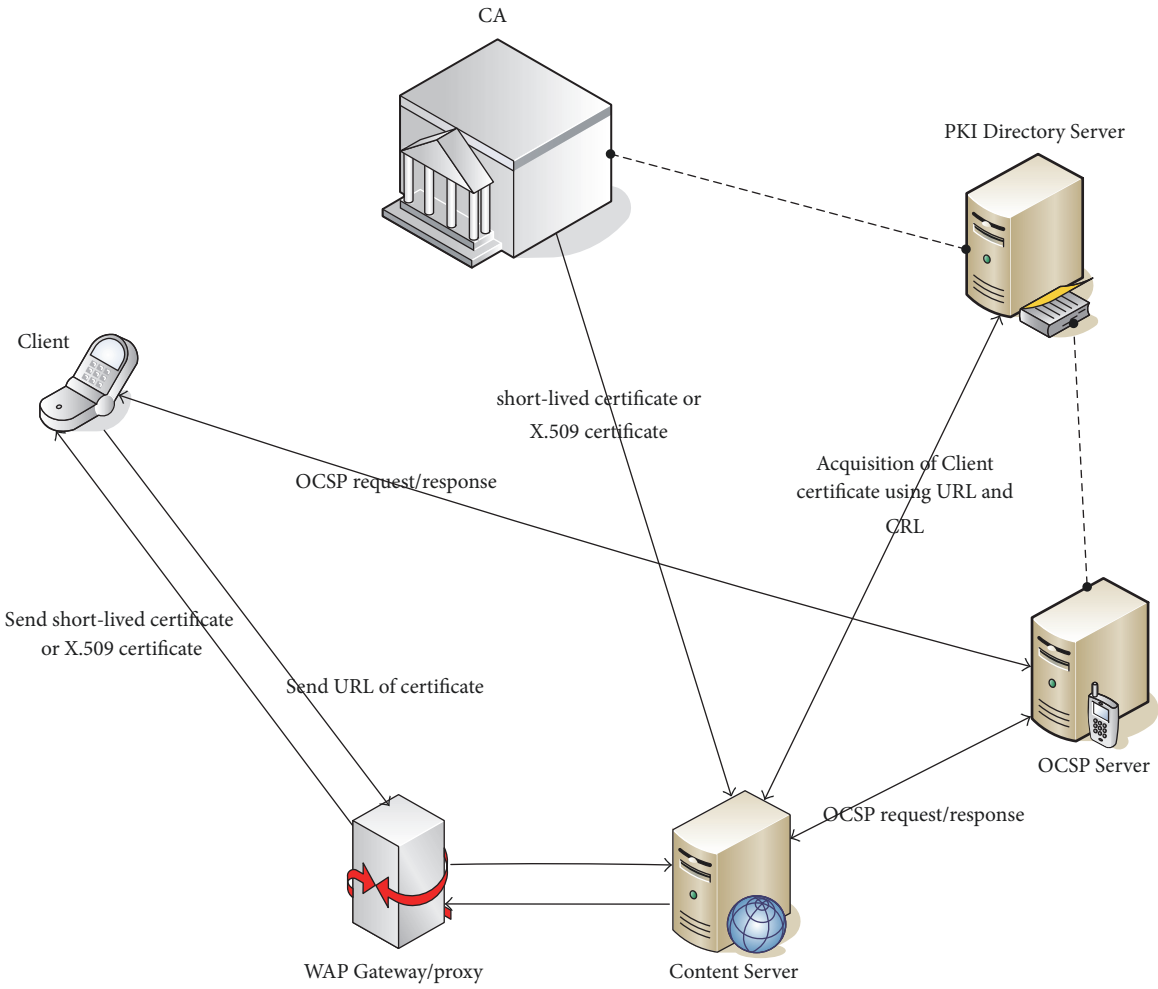

Figure 2: WPKI's certificate verification scheme.

server, the procedure is finished in the wired network, and thus the cost is beneficial; (c) if the OCSP server requires the signed OCSP query request, then in the original scheme the mobile terminal needs to send its own certificate to the OCSP server to be verified through the wireless network, and thus the occupied time and consumption of network bandwidth, however increase; in our proposed scheme, the content server sends its own certificate to the OCSP server through the wired network, such communication efficiency is much higher, and because the number of content servers is much smaller than the number of mobile terminals, the amount of data sent by the entire authentication process is reduced.

(2) We use the ECC-based encrypting/decrypting functions [16] to sign and verify the certificate digest, which ensures the consistency of the verified certificates among the communication entities to prevent the forgery of the certificate and the replay attack of verification data. Since the security of presignature technology for certificate status still needs to be discussed, our proposed scheme does not use the presignature technology, but it can be extended to use presignature technology.

(3) Based on the works [9, 12–15], the structure of the certificate verification mechanism is improved and designed, which is compatible with the existing OCSP schemes. In this paper, we evaluate and analyze the efficiency of our proposed scheme by simulation and implementation. The simulation results of the proposed scheme are evaluated according to the evaluation frameworks [9, 17], and the test system is designed with JAVA to evaluate the actual performance of the proposed scheme.

2. Related Work

WPKI is a PKI-based extension scheme. Due to the unique characteristics of wireless network, WPKI needs to be improved or redesigned in many ways [9–15, 17–20]. The evaluation framework of certificate verification scheme was given in [17]. Also, [9] evaluated the performance of the CRL scheme and the OCSP scheme according to the evaluation framework. It pointed out that the CRL scheme is not

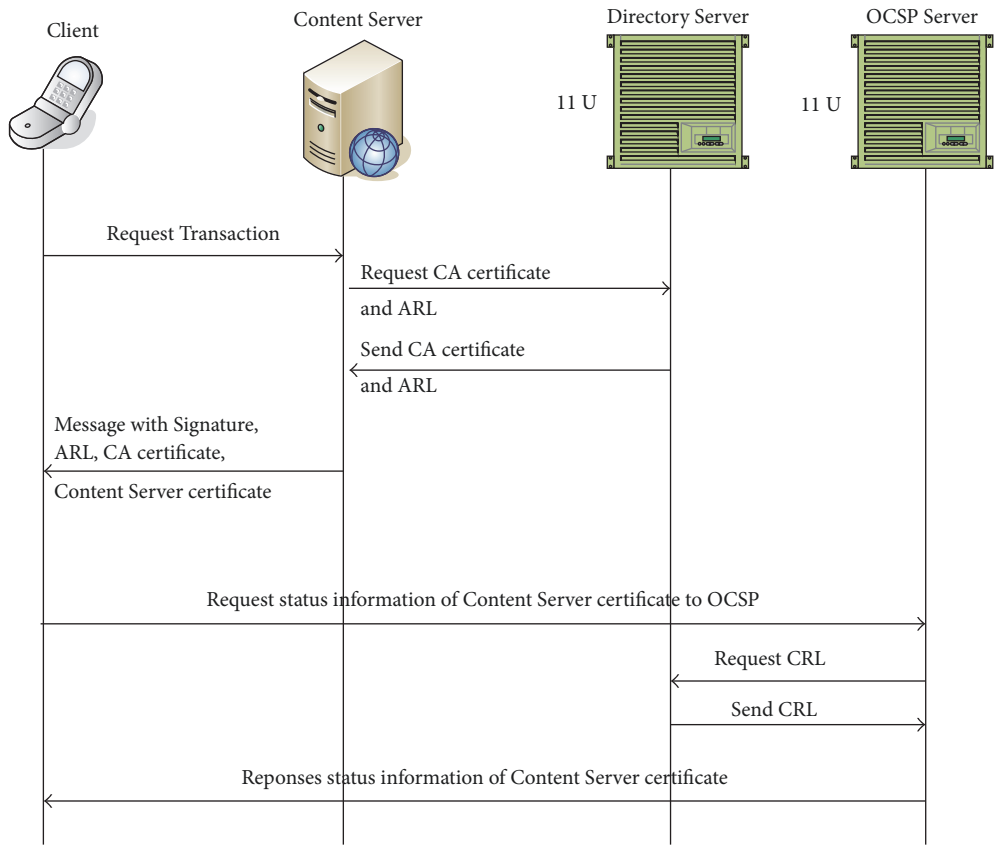

Figure 3: The certificate verification scheme based on OCSP.

effective, which requires high computing ability and high overhead for the mobile terminal entity. So, there are many improved schemes based on CRL, such as delta_CRL [9, 10] scheme, and partition_CRL [9, 10] scheme. However, because the additional models of the schemes require more computational overhead, and the security of the schemes is not ideal, the schemes are not effective to be introduced into the WPKI mechanism.

The work [9] pointed out that the OCSP scheme is an effective certificate authentication scheme, while the works [9–11, 18] pointed out some shortcomings of the OCSP scheme. The work [9] pointed out that the OCSP server and the CA maintain synchronization updates in the OCSP scheme, but because the directory server is based on the released contents of the CA to regularly update its database, there is a time gap so that some certificates have expired but the directory server and the OCSP server do not receive the latest CRL and ARL at the same time, which leads to the database inconsistency between the directory server and the OCSP server. Therefore, the attacker can exploit the data inconsistency in the time slot to carry out the spoofing attack on the communication entities.

In the other related works [10–15, 18–20], the original OCSP scheme has been improved. The work [10] proposed a certificate verification scheme for reducing the number of interactive connections between the mobile terminal and the wireless network, in which CA certificate and ARL are forwarded by content server to reduce the interaction number between entities and network. The scheme is shown in Figure 3: (1) a mobile terminal applies for a transaction to the content server, and after obtaining a transaction request, the content server applies to the directory server for the CA certificate and the ARL; (2) the content server forwards the CA certificate, the ARL, and its own certificate to the mobile terminal; (3) after obtaining the CA certificate, the ARL, and the content server certificate, the mobile terminal sends a request to the OCSP server to verify the status of the content server certificate; (4) after the OCSP server gets the certificate status, it sends the result of the certificate status to the mobile terminal. However, the proposed scheme [10] has security weakness in the authentication process. As shown in Figure 3, the content server can tamper with the CA certificate and the ARL; the process makes the transaction insecure to the mobile terminal. Also, if a mobile terminal verifies the certificates by the OCSP server, then the verification process of the content server certificate is completely transparent to the mobile terminal; therefore the steps for the mobile terminal to obtain the complete CA certificate and the ARL could be omitted, and the verification of the content server certificate could be completed by the OCSP server so as to reduce the time and storage space for the mobile terminal to download the ARL and CA certificates and the wireless network bandwidth consumption for the download process.

The work [20] proposed the concept of proxy OCSP by setting up a proxy OCSP server between the OCSP server (OCSP responder) and the mobile terminal. The proxy OCSP server is set as an intermediate site to forward the OCSP requests and responses between the mobile terminal and the OCSP server, which alleviates the workload of the OCSP server. However, there are no specific implementation details of the certificate verification procedure in this paper [20], and the scheme also has the problem of verified data inconsistency. The other works proposed an improved OCSP scheme which precomputes the signature of certificate status, but the work [9] pointed out that the security of the precomputed signature's OCSP scheme needs to be discussed and studied. The work [15] proposed a scalable OCSP-based certificate validation system exploiting the Fast-CGI interface. However, the security of this scheme still needs to be discussed. Additionally, the work [11] proposed a hash-table-based OCSP scheme, which uses hash-table to compute certificate status to replace the signature of certificate status. The hash-table-based OCSP scheme reduces the required time of frequent signature calculation and the data size of OCSP response, but there are still many problems in this scheme:

(1) Because this scheme is not designed for mobile networks, it is not entirely suitable for mobile networks. This scheme needs to calculate the hash function several times, the computation time is proportional to the length d of the hash chain, so the length of the hash chain has a great impact on the performance of this scheme. The value of d is too large to increase computing cost, especially for the mobile terminal, the value of d is too small to degradate to the original OCSP protocol. Additionally, in this scheme the OCSP server (OCSP responder) generates a set of random data based hash-table for each user query and saves them; thus these additional costs may increase the burden of the OCSP server.

(2) The security of this scheme is still worth discussing: (a) there is the time gap in storing cache data. For example, if the certificate status is changed so that the OCSP server needs to calculate the new hash chain value, at the same time one query is responded to the OCSP server, then the queried result is still the previous hash chain value. That is because that although the computation time of hash chain value is very short, too much hash chain computation will need much longer computing time; thus this time gap could be used by attackers to get the old hash chain value; (b) the cache of the client stores hash chain value; however, if the status of certificate does not change, the OCSP server will only return an unsigned query result [11]. So, in this case, the scheme cannot defend against the man-in-the-middle attack, because the attacker can intercept the query result and pretend OCSP server for spoofing the client to require to check certificate validation in the next time, such results in that the client cannot get the correct result so that the entire transaction cannot be completed in a period of time. In addition, if the query result is signed and sent to the client, then the scheme is not different from the original OCSP and increases the cost of computing hash chain; (c) the client stores hash chain value, and thus the scheme is not enough secure for the mobile terminals in the wireless mobile network. When the caching data is leaked out and lost, the data easily threatens the authentication of other mobile terminals.

Presently most of the related schemes only change the CRL structure or the OCSP procedure so that the variant schemes can be applied to some specific applications [13, 14], such as P2P networks and Adhoc. However, these schemes are difficult to be applied to the common scenes; thus the whole certificate verification process still needs to be improved, such that it is necessary to optimize the number of interactions between wireless communication entities and wired network.

3. WPKI Certificate Verification Scheme Based on CDS_OCSP

In this paper, we propose a WPKI certificate verification scheme based on the certificate digest signature-online certificate status protocol (CDS_OCSP) with the basis of [10]. The proposed scheme optimizes the number of communication connections between the communication entity and the network, reduces the consumption of the wireless network bandwidth in the certificate verification process, and uses the ECC-based encrypting/decrypting functions [8, 16] to sign and verify the certificate digest, which ensures the consistency of the verified certificates among the communication entities.

According to the IETF's function definition of entities in the WPKI mechanism [21], mobile terminal and content server are untrusted entities, and directory server and OCSP server are trusted entities. Therefore, from the perspective of security, the logic relationship among the four entities (as Figure 3) may be simplified as a trusted tripartite agreement, shown as Figure 4.

At the same time, because content server, directory server, and OCSP server are on wired network but mobile terminal is on wireless network, we may aim to optimize the number of connections between communication entities and network, which can effectively reduce the number of interactive connections between mobile terminals and wired network and the size of content downloaded from wired network.

In this paper, our proposed CDS_OCSP-based scheme aims to improve the existing OCSP-based WPKI certificate verification scheme [10] according to the principle of optimizing the number of connections and reducing the consumption of wireless network bandwidth and to adopt the method of verifying the certificate digests to ensure that all related entities obtain the consistency of certificate. Because the security of using the presignature technology in the OCSP request and reply is still doubtful, our CDS_OCSP-based scheme does not use the presignature method, but the OCSP request and response in our proposed scheme are modified from the traditional format of the OCSP request and response [21]; thus our scheme may also use presignature method.

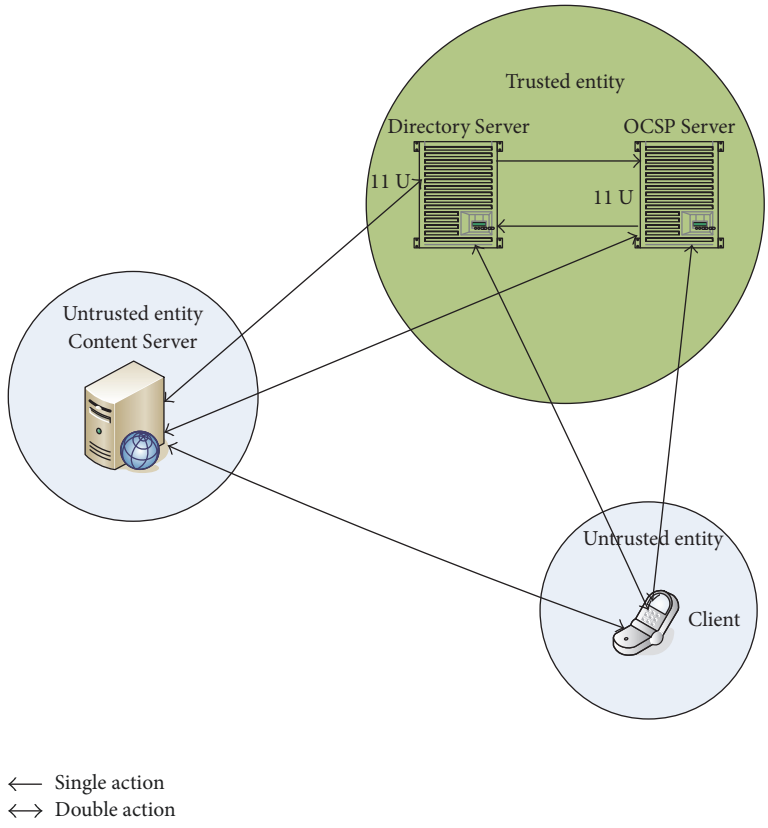

Figure 4: The logic relationship division of the four entities based on security viewpoint.

3.1. Certificate Digest. Currently wireless X.509 certificate and short-lived certificate are used in WPKI mechanism. The format of the two certificates is different as shown in Tables 1 and 2. However, since the short-lived certificate has a fixed life cycle, the certificate verification scheme is primarily for wireless X.509 certificate verification. In our proposed scheme, according to the function definition of each field of wireless X.509 certificate proposed by the IETF group [1, 5, 6], we select two fields "Serial number" and "Issuer" as the components of certificate digest, where the field "Serial number" represents the serial number of certificate which is unique, and the field "Issuer" indicates the issuer name of certificate; thus the certificate digest is represented as $Ce\_Digest = Serial\ number \oplus Issuer$.

3.2. Certificate Status Mapping Table. Our proposed certificate verification scheme is based on the online authentication mode: the OCSP server needs to query local database to obtain certificate status. So, in order to speed up the response time of the OCSP server, a temporary certificate status mapping table is established in the OCSP server's database, each time the OCSP server responding to request only needs to query the mapping table, whose structure is shown as Figure 5.

In the mapping table, the field "Certificate_ID" represents the field "Serial number" of the certificate, the field "Issuer" is the same as the field "Issuer" of the certificate; the field "Ce_Digest" is the certificate digest, which is the conjunction computed by the field "Issuer" and the field "Serial number", namely, Ce_Digest = Serial number ⊕ Issuer; the field "Certificate_Status" indicates the certificate status, whose value is "good," or "revoked (hold)," or "unknown"; the field "ExpirationDate/ValidityPeriod" indicates the valid time of the certificate status. The record data in the mapping table is divided into two parts: CRL zone and non-CRL zone, where the CRL zone saves the records generated by the CRL [21] and the non-CRL zone saves the records generated by the real-time queries or the certificate status data published by CA. The update of the mapping table is also divided into two cases, in which the records from the CRL zone are updated synchronously with the CRL and another records from the non-CRL zone are updated in real time.

The OCSP server uses the mechanism of querying the mapping table to complete the response to the OCSP request. For each request, the OCSP server only needs to query the mapping table and then obtains the corresponding certificate status and generates a new OCSP response (the same method may be used for querying the CA certificate status). Also, although our proposed scheme does not use the presignature method of certificate status, it can be easily extended to use the method. For example, if our proposed scheme adopts the presignature method of hash chain proposed by [11], then our proposed scheme can add the corresponding field [11] to the mapping table.

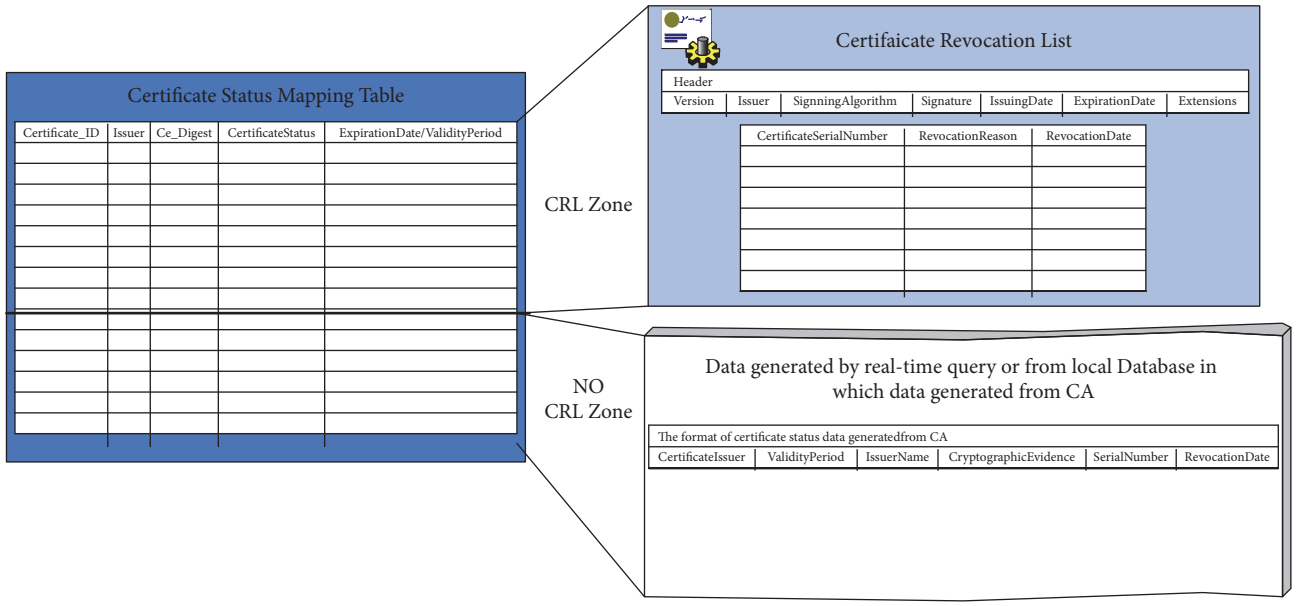

Figure 5: Certificate status mapping table.

3.3. Related Cryptographic Functions. Because our proposed CDS_OCSP-based scheme needs to verify certificate digest in interaction process, the proposed protocol defines two types of functions: (a) encryption function $E_{R_2}^{r_1}(k, M)$ and decryption function $D_{R_1}^{r_2}(k, Q)$, both of which are based on ECC from [16], where k is the random number, M is the plaintext (message), Q is the ciphertext, r_1 and r_2 are the private keys, R_1 and R_2 are the corresponding public keys, and all ECC parameters are set by the CA, which are comprised in the issued certificates from the CA; (b) two one-way collision free hash functions: $F : \{0,1\}^* \to z_q^*$ and $H : \{0,1\}^* \times \{0,1\}^* \to z_q^*$, where the hashing results from hash functions are 160 bits. In this paper, we set the private key of mobile terminal as sk_c, the corresponding public key as pk_c, the private key of the content server certificate as sk_s, and the corresponding public key as pk_s.

3.4. The Procedure of CDS_OCSP-Based Scheme. The CDS_OCSP-based scheme performs cross-validation among four entities. So, assuming that the deployment of all certificates has been completed, which includes the OCSP server certificate [9], and that the request and response format is appropriately modified in OCSP [2, 21, 22], the interactive procedure among the mobile terminal, the content server, the directory server, and the OCSP server is described as shown in Figure 6.

(1) When the mobile terminal applies for a transaction to the content server, if the transaction request includes a certificate verification request, then that means the mobile terminal requires checking the validity of the content server certificate and requires the content server to directly send the OCSP request to the OCSP server; additionally the mobile terminal generates the transaction ID and the transaction password and then sends them to the content server.

(2) After receiving the transaction request, the content server sends the transaction ID and the request of querying the content server certificate and the corresponding mobile terminal certificate to the directory server, and then the directory server sends the mobile terminal certificate to the content server. The content server computes $M_1 = F(\text{CServer.Ce\_Digest})$ by its own certificate digest and the signature $Z = E_{\mathrm{pk}_c}^{\mathrm{sk}_s}(\mathrm{PW}, M_1)$ according to the private key sk_s of the certificate, the public key pk_c of the mobile terminal certificate, and the transaction Password (abbreviated as PW) and finally sends Z to the mobile terminal and simultaneously sends the transaction ID and the transaction Password and the request (the CDS_OCSP request) of inquiring the status of the self certificate to the OCSP server; since the sender of the CDS_OCSP request is not the mobile terminal, if the OCSP server requires, the CDS_OCSP request has a signature information to prevent the DoS (denial of server) attack; then the content server signs the CDS_OCSP request with the private key sk_s of its own certificate and sends the certificate to the OCSP server, and then the OCSP server verifies the certificate (which may also be performed in step (5) and checks the CDS_OCSP request by using the public key pk_s of the corresponding certificate.

(3) The directory server sends the content server certificate to the mobile terminal according to the transaction ID after receiving the request for querying the content server certificate.

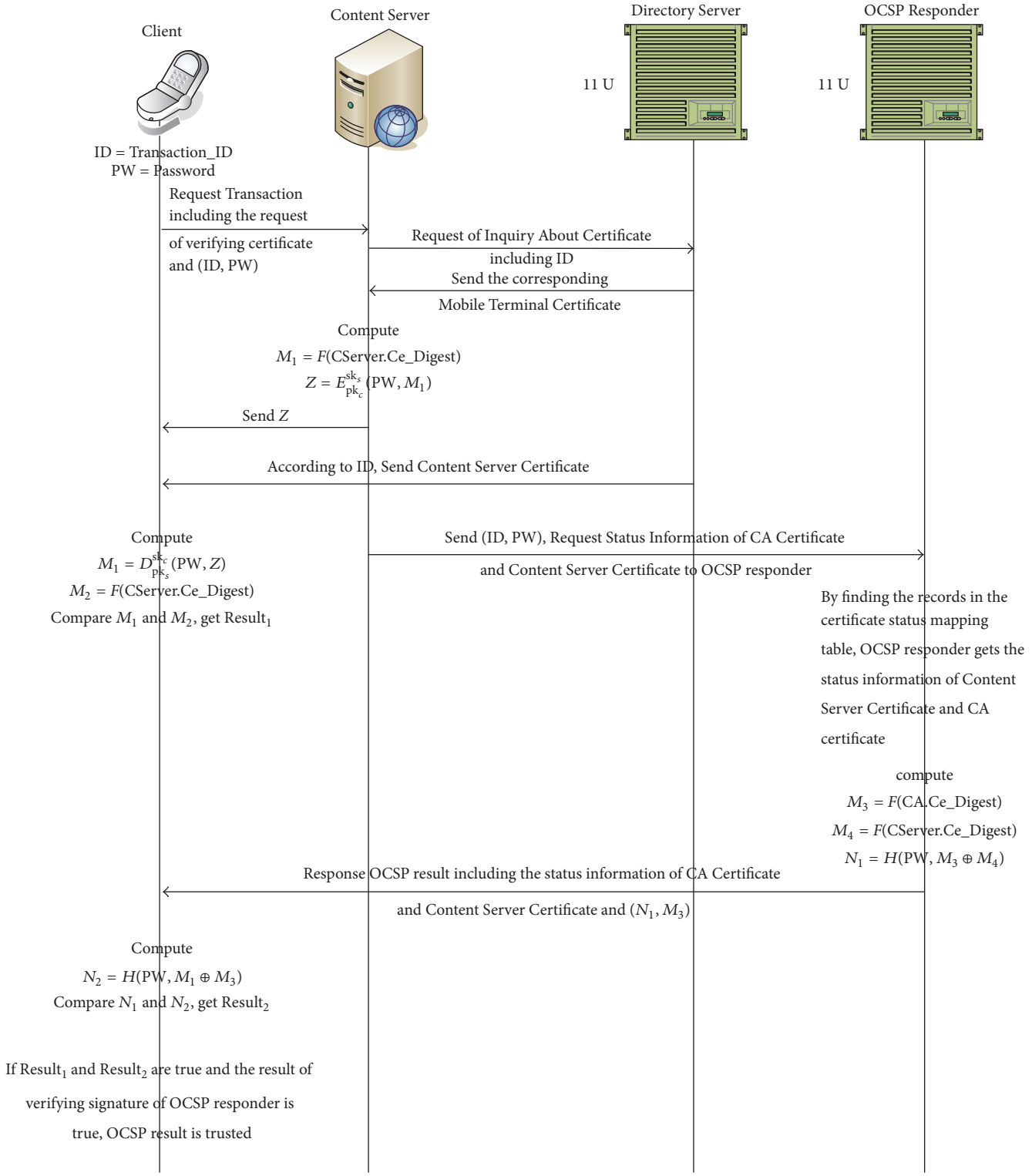

Figure 6: The procedure of the CDS_OCSP-based scheme. CA.Ce_Digest denotes the digest of the CA certificate, CServer.Ce_Digest denotes the digest of the content server's certificate, the private key of mobile terminal is sk_c, the corresponding public key is pk_c, the private key of content server certificate is sk_s, and the corresponding public key is pk_s.

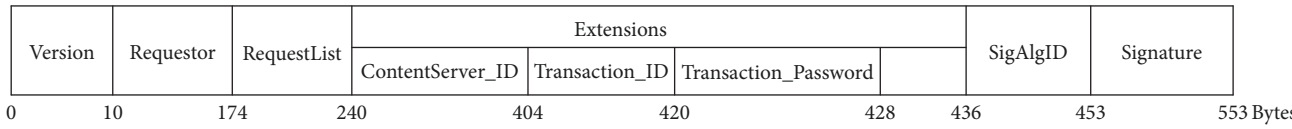

Figure 7: CDS_OCSP request.

(4) After the mobile terminal receives Z, it computes $M_1 = D^{sk_c}_{pk_s}(PW, Z)$ according to the private key sk_c of the own certificate, the public key pk_s of the content server certificate, and the transaction Password and then computes $M_2 = F$(CServer.Ce_Digest) according to the received content server certificate and compares M_1 and M_2 (checks whether M_1 is equal to M_2) and then gets the result $Result_1$. If $Result_1$ is true, then the transaction continues; otherwise the transaction verification process has an exception, and the transaction is aborted;

(5) After receiving the transaction ID, the password PW, and the CDS_OCSP request (the format detail of the request is given in Section 3.5), the OCSP server looks up the record in the certificate status mapping table according to the serial number of the CA certificate from the CDS_OCSP request and and then obtains the CA certificate status; then the value of the Ce_Digest field of the record is calculated as $M_3 = F$(CA.Ce_Digest); and then, in the CDS_OCSP request, the OCSP server looks up the corresponding record in the certificate status mapping table according to the serial number of the inquired content server certificates and obtains the content server certificate status; then the value of the Ce_Digest field of the record is calculated as $M_4 = F$(CServer.Ce_Digest); and then the OCSP server computes $N_1 = H(PW, M_3 \oplus M_4)$; finally the CDS_OCSP request result with signature information is returned to the mobile terminal according to the transaction ID, which includes (N_1, M_3).

(6) After receiving the result of the CDS_OCSP request, the mobile terminal computes $N_2 = H(PW, M_1 \oplus M_3)$ and then compares N_1 and N_2 to obtain the result $Result_2$ (checks whether N_1 is equal to N_2). If both of $Result_1$ and $Result_2$ are true and the signature of the OCSP server can also be verified as validity, the result of the CDS_OCSP request is true. The entire procedure of CDS_OCSP is completed.

3.5. The Format of CDS_OCSP Request and Response. According to the format of OCSP request and response [9, 21, 22], our proposed scheme appropriately modifies the format and makes the modified OCSP request and response compatible with the original OCSP.

(1) CDS_OCSP request: in our CDS_OCSP based scheme, because the sender of the CDS_OCSP request is not the mobile terminal but the content server and the CDS_OCSP request adds the transaction ID field and the transaction Password field, it is necessary to modify the OCSP request format shown as Figure 7, where the "Requestor" field corresponds to the mobile terminal ID of the transaction, and the proposed scheme extends the "Extensions" field (which is optional in the original OCSP request format): the first 164 bytes correspond to the content server ID of the transaction, 16 bytes correspond to the transaction ID, 8 bytes correspond to the transaction Password, and the other fields' definitions are invariant; additionally, in order to be compatible with the original OCSP, if the value of the "Extensions" field is zero, the request is a standard (original) OCSP request, the sender of OCSP request is mobile terminal.

It should be noted that, in the original OCSP request, an OCSP request sender generally requires the status of one or more certificates to be queried; therefore a request list [9] containing one or more queried certificates is included in an OCSP request. For example, in the wired P2P network, the client can simultaneously require the OCSP server to query multiple certificate status; however, in the WPKI mechanism, the OCSP requests sent by the mobile terminal generally require querying only the CA certificate status and the content server certificate status, shown as Figure 3; thus the modified OCSP request (CDS_OCSP request) will not bring the data increase in the WPKI certificate verification scheme, compared with the original OCSP request. In the original OCSP, if the OCSP server requires that the OCSP request has the signature information, then the mobile terminal needs to send its own certificate to the OCSP server for the authentication through the wireless network, which increases the time and bandwidth of the OCSP request. In the CDS_OCSP scheme, the content server sends its own certificate and the CDS_OCSP request to the OCSP server through the wired network; thus its communication efficiency is much higher than that of the transmission on the wireless network, and because the number of the content servers is much smaller than the number of the mobile terminals, the amount of data sent in the entire authentication procedure is reduced in the CDS_OCSP scheme.

(2) CDS_OCSP response: compared with the original O CSP response, the modified OCSP response (CDS_ OCSP response) only adds the authenticating data N_1 and M_3, and the other contents are not modified.

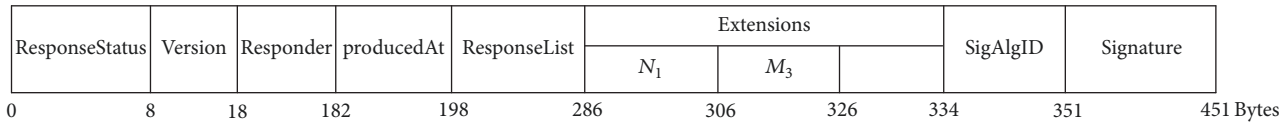

Figure 8: CDS_OCSP response.

As N_1 and M_3 are the result of one-way collision-resistance hash function, the modified OCSP response format is shown as Figure 8, in which the "Extensions" field needs to be extended, the first 20 bytes correspond to the authenticating data N_1, and the other 20 bytes correspond to the authenticating data M_3 (in this paper, the result of hashing function is 160 bits).

4. The Analysis of the CDS_OCSP Based Scheme

4.1. Security Analysis. According to the function definition of the interactive entities proposed by the IETF working group in WPKI, the directory server and the OCSP server are the trusted entities and the mobile terminals and the content servers are the untrusted entities. Therefore, from the perspective of security, the logic relationship among the four entities may be simplified as a trusted tripartite protocol; thus the security of the proposed scheme is analyzed as follows:

(1) Because the directory server is a trusted entity, the content server certificate provided by it directly to the mobile terminal is trusted, namely, not tampered with or forged.

(2) The CDS_OCSP based scheme uses the ECC-based encrypting/decrypting functions to sign and verify the certificate digest [16]. So, the verification procedure can be trusted for the mobile terminal and the content server.

(3) In the CDS_OCSP based scheme, the content server only signs the certificate digest with the private key sk_s of the own certificate, the public key pk_c of the mobile terminal certificate, and the transaction Password. Then, the mobile terminal can use the private key sk_c of the own certificate, the public key pk_s of the content server certificate, and the transaction Password to decrypt and verify the certificate digest and compute $M_2 = F(\text{CServer.Ce\_Digest})$ from the received content server certificate and then compare M_1 and M_2. Because the content server certificate provided by the directory server to the mobile terminal is trusted, the comparison of M_1 and M_2 can guarantee that the mobile terminal obtains that the received content server certificate is consistent with the content server certificate on the content server, so as to prevent that the third party forges the identity to participate in the transaction.

(4) The OCSP server checks the content server certificate status and the CA certificate status and computes $M_3 = F(\text{CA.Ce\_Digest})$ by the CA certificate digest, $M_4 = F(\text{CServer.Ce\_Digest})$ by the content server certificate digest and $N_1 = H(\text{PW}, M_3 \oplus M_4)$ and then sends N_1 to the mobile terminal; then the mobile terminal compares N_1 with N_2 so as to guarantee that the content server certificate verified by the current OCSP server and the content server certificate obtained by the mobile terminal are identical and to resist the attack of replaying verification data.

(5) The CDS_OCSP based scheme can require that all processes of sending and receiving certificates and the message requests and responses contain signature information, that can effectively prevent the man-in-the-middle attack and resist the denial-of-service attack caused by the malicious request.

(6) For each transaction, the mobile terminal generates the different transaction ID and the transaction Password to ensure the randomness of the whole verification. Therefore, the CDS_OCSP based scheme can prevent the untrusted entity from replaying the authentication data. For example, an attacker can replay an OCSP response with the same certificate status to attack the mobile terminals or the servers. However, as the CDS_OCSP response in our proposed scheme contains $N_1 = H(\text{PW}, M_3 \oplus M_4)$, the CDS_OCSP response is different each time, so that an attacker cannot replay the CDS_OCSP response.

(7) The CDS_OCSP based scheme uses the ECC-based encrypting/decrypting functions to sign and verify the certificate digest, which can prevent the content server from forging the CA certificate, the ARL, and the content server certificate to attack the mobile terminal, compared with the scheme proposed by [10].

4.2. Efficiency Analysis. In the CDS_OCSP based scheme, the number of interactions among communication entities is seven times (see Figure 6), in which the number of interactions between the mobile terminal entity and the communication entity of the wired network is four times. In [10], the number of interactions among communication entities is eight times (see Figure 3), where the number of interactions between the mobile terminal entity and the communication entity of the wired network is four times. Although the CDS_OCSP based scheme does not reduce the number of interactions in the wireless network, the whole verification reduces the time of downloading the CA certificate and the

Table 3: Model of WPKI for performance evaluation.

Parameter	Description	Value	Unit
K	Size of ECC's key	163	bits
H	Size of hash function's result	160	bits
C	Number of CA	2	
N	Number of users of the WPKI	10000	
T	Validity period of a certificate	90	day
F	Number of content providers	50	
U	Percentage of users requesting transaction	10, 20	%N
Q	Status request per day per user	5, 10, 20	1/day·user
P	Percentage of certificates revoked	10	%N
R	Number of CRLs issued per day	1	day
l_i	Size of the date structure i		bytes
V_i	Data size of transaction i		bytes

ARL by the mobile terminal and the bandwidth consumption of the wireless network, and since the mobile terminal does not send the OCSP request to the OCSP server through the wireless network, but the content server sends the OCSP request directly to the OCSP server through the wired network, the CDS_OCSP based scheme is more efficient than that of [10]. Also, although the directory server needs to send the mobile terminal certificate to the content server, the procedure is finished in the wired network; thus the cost is beneficial. Additionally, if the OCSP server requires the OCSP request to have signature information, then the content server sends its own certificate through the wired network to the OCSP server. So, its communication efficiency is much higher than that of the wireless network. Because the number of content servers is much smaller than the number of mobile terminals, the amount of sent data is also reduced.

5. Simulation and Experiment

In this paper, we simulate the verification procedure on the CDS_OCSP based scheme and the original scheme [10] and then analyze the experimental results. In the experiment, we are mainly concerned about the following two performance factors:

(1) The sent data size through the wireless network in the verification procedure: because the bandwidth and communication efficiency of the wired network are much higher than that of the wireless network, the data traffic on the wireless network is concerned. Compared with the scheme proposed by [10], the CDS_OCSP based scheme reduces the CA certificate and the ARL (downloaded by the mobile terminal) and the OCSP request in the wireless network. Therefore, it needs to be measured that this reduced data size can bring benefit.

(2) The time of the whole certificate verification process: although the CDS_OCSP scheme reduces the time of downloading the CA certificate and the ARL and committing the OCSP request by the mobile terminal, it adds the extra computing function cost, where the OCSP server adds the hash function calculation three times, the content server adds the signature calculation and a hash function calculation, and the mobile terminal adds the verification computation and two hash function calculations; thus we need to consider the comparison of computing cost of additional functions and reducing the time; also, the computing time of each function is also considered, because too much of computational overhead increases the burden of the content server and the OCSP server.

In our experiments, the above-mentioned performance factors are divided to two parts: (a) the sent data size in the wireless network, where we use the simulation method to assess the amount of data [9]; (b) the whole time of the certificate verification procedure, where we make the prototype system to test the time.

5.1. Simulation Analysis. According to the evaluation model proposed by [9], we, respectively, evaluate and analyze our proposed CDS_OCSP based scheme and the other scheme proposed by [10]. The evaluated data structure and data size are described as shown in Tables 3 and 4.

Table 3 shows all the used parameters, including parameter descriptions, value sizes, and numerical units in the evaluation model.

Table 4 shows all the used data structure names, including data structure descriptions and data structure sizes in the certificate verification procedure.

According to the above-mentioned parameters, we can compute the average data size V_i daily made by our proposed CDS_OCSP based scheme and the scheme proposed by [10] in the transaction verification procedure. So, we divide the computation of the data V_i to four cases: (a) the entire verification data $V_{\text{entire\_signature}}$ required with certificate verification signature; (b) the wireless network data $V_{\text{wireless\_signature}}$ required with certificate verification signature; (c) the entire

Table 4: Sizes of different data structures in the performance evaluation.

Parameter	Description	Value (bytes)
l_{cert_ca}	Size of X.509 certificate (CA)	804
l_{cert}	Size of X.509 certificate	983
l_{CRL}	Size of X.509 CRL (number of users = 10000)	39500
l_{ARL}	Size of ARL (number of CA = 2)	3000
l_{Tst_ID}	Size of Transaction_ID	16
l_{Tst_PW}	Size of Transaction_Password	8
l_{Tst_Req}	Size of Transaction_Request in OCSP [10]	168
$l_{Req\_CA\_ARL}$	Size of Request for CA and ARL in OCSP [10]	184
$l_{imp\_Tst\_Req}$	Size of Improved Transaction_Request including Transaction_ID and Transaction_Password	200
l_{Req_Cert}	Size of Request of inquiry about certificate	344
l_z	Size of Z sent by content server	364
$l_{Ocsp\_Req\_sign}$	Size of OCSP request (signed) [10]	403
$l_{Ocsp\_Req\_unsign}$	Size of OCSP request (unsigned) [10]	303
l_{Ocsp_Resp}	Size of OCSP response [10]	429
$l_{Cds\_Ocsp\_Req\_sign}$	Size of CDS_OCSP request (signed)	553
$l_{Cds\_Ocsp\_Req\_unsign}$	Size of CDS_OCSP request (unsigned)	453
$l_{Cds\_Ocsp\_Resp}$	Size of CDS_OCSP response	451

verification data V_{entire} without certificate verification signature; (d) the wireless network data $V_{wireless}$ without certificate verification signature. Also, to compare the scheme proposed by [10], we divide the data results into two groups:

(1) The OCSP-based scheme (the scheme proposed by [10])

According to the verification process of Figure 3, we compute the average data size V_i based on the OCSP-based scheme in a day:

(a) $V_{entire\_signature} = (l_{Tst\_Req} + l_{Req\_CA\_ARL} + l_{ARL} + l_{cert\_ca} + 2 \cdot l_{cert} + l_{Ocsp\_Req\_sign} + l_{Ocsp\_Resp}) \cdot N \cdot U \cdot Q.$

(b) $V_{wireless\_signature} = (l_{Tst\_Req} + l_{ARL} + l_{cert\_ca} + 2 \cdot l_{cert} + l_{Ocsp\_Req\_sign} + l_{Ocsp\_Resp}) \cdot N \cdot U \cdot Q.$

(c) $V_{entire} = (l_{Tst\_Req} + l_{Req\_CA\_ARL} + l_{ARL} + l_{cert\_ca} + l_{cert} + l_{Ocsp\_Req\_unsign} + l_{Ocsp\_Resp}) \cdot N \cdot U \cdot Q.$

(d) $V_{wireless} = (l_{Tst\_Req} + l_{ARL} + l_{cert\_ca} + l_{cert} + l_{Ocsp\_Req\_unsign} + l_{Ocsp\_Resp}) \cdot N \cdot U \cdot Q.$

(2) The CDS_OCSP scheme (assuming that all content servers are required to provide content services within a day's time)

Similarly, according to the verification process of Figure 6, we compute the average data size V_i based on the CDS_OCSP scheme in a day:

(a) $V_{entire\_signature} = (l_{imp\_Tst\_Req} + l_{Req\_Cert} + l_z + 2 \cdot l_{cert} + l_{Cds\_Ocsp\_Req\_sign} + l_{Cds\_Ocsp\_Resp}) \cdot N \cdot U \cdot Q + l_{cert} \cdot F.$ Compared with $V_{entire\_signature}$ from the OCSP-based scheme, although the CDS_OCSP scheme requires that the directory server sends the mobile terminal certificate to the content server so as to add one l_{cert} to the formula, the procedure is finished in the wired network; thus the cost is beneficial. Because our proposed OCSP-based scheme optimizes the authentication process, in which the content server sends the request of verifying the certificate directly, our proposed $V_{entire\_signature}$ should be less. Additionally, as the number of the sent content server certificates (the OCSP responder requires a certificate signature for verification) is determined by the number F of the content servers, and the number of the content servers on the wired network is much smaller than the average number of the transaction users, which leads to a significant reduction in the number of the sent l_{cert}; thus our proposed $V_{entire\_signature}$ should be less.

(b) $V_{wireless\_signature} = (l_{imp\_Tst\_Req} + l_z + l_{cert} + l_{Cds\_Ocsp\_Resp}) \cdot N \cdot U \cdot Q.$

Also, since the content server directly sends its own certificate and the request of verifying the certificate, the size of data is reduced on the wireless network. Compared with $V_{wireless\_signature}$ from the OCSP-based scheme and our proposed $V_{entire\_signature}$, the proposed formula $V_{wireless\_signature}$ reduces one l_{cert}, l_{Req_Cert}, $l_{Cds\_Ocsp\_Req\_sign}$, and $l_{cert} \cdot F$.

(c) $V_{entire} = (l_{imp\_Tst\_Req} + l_{Req\_Cert} + l_z + 2 \cdot l_{cert} + l_{Cds\_Ocsp\_Req\_unsign} + l_{Cds\_Ocsp\_Resp}) \cdot N \cdot U \cdot Q$

(d) $V_{wireless} = (l_{imp\_Tst\_Req} + l_z + l_{cert} + l_{Cds\_Ocsp\_Resp}) \cdot N \cdot U \cdot Q.$

Also, compared with V_{wireless} from the OCSP-based scheme and our proposed V_{entire}, the proposed formula V_{wireless} reduces one l_{cert}, $l_{\text{Req\_Cert}}$, and $l_{\text{Cds\_Ocsp\_Req\_unsign}}$.

Through the computing simulation of the above data structure, we can get the performance comparisons of the CDS_OCSP scheme (new OCSP) and the OCSP-based scheme (old OCSP), shown as Figures 9–14.

Figures 9–11 show the comparisons of the data V_i from the CDS_OCSP scheme and the OCSP-based scheme when the number N of users is 10000, the average percentage U of the request's users is 10%, and the numbers Q of the requests per user are 5, 10, and 20, respectively. In Figures 9–11, the sizes of the data V_i from the CDS_OCSP scheme are less than 2/3 of those of the original OCSP-based scheme according to $V_{\text{entire\_signature}}$ and V_{entire}, and the sizes of the data V_i from the CDS_OCSP scheme are less than 1/2 of those of the original OCSP-based scheme according to $V_{\text{wireless\_signature}}$ and V_{wireless}. When Q increases, this situation becomes more obvious. There are two main reasons: (a) the CDS_OCSP scheme eliminates the request and transmission of ARL (the size of l_{ARL} is 3000 bytes), and the CA certificate is verified by the OCSP responder; (b) the CDS_OCSP scheme uses the method that the content server directly sends the request of certificate verification and the content server certificate; thus the work is implemented by the wired network. In particular, when the OCSP request requires a signature, the certificate transmission for signing and verification is not implemented by the wireless network; thus the sizes of the data $V_{\text{wireless\_signature}}$ from the CDS_OCSP scheme are almost 1/3 of those of the original OCSP-based scheme.

Figures 12–14 show the comparisons of the data V_i from the CDS_OCSP scheme and the OCSP-based scheme when the number N of users is 10000, the average percentage U of the request's users is 20%, and the numbers Q of the requests per user are 5, 10, and 20, respectively. In Figure 14, with the rapid increase of user's requests, the sizes of the data V_i from the CDS_OCSP scheme are more less than those of the original OCSP-based scheme. Thus, our proposed CDS_OCSP scheme should be efficient. Additionally, the length of our modified OCSP request and response is not increased, compared with the original OCSP request and response.

5.2. Testing Analysis. The prototype system is composed of three computers and a mobile phone. The equipment configuration is shown in Table 5, where the three computers are used as the directory server, the OCSP server, and the content server, and the mobile phone is used as the mobile terminal. The prototype system eliminates the WAP Gateway, and the CA and the OCSP server are separated as two systems [2, 9, 21]. In the test, we assume that all the certificates have been initialized and deployed; thus the CA is omitted from our test. The prototype system is written in JAVA, and the HTTP protocol is used to implement the communication among all the entities. The prototype system is shown as Figure 15.

Table 5: Device configuration.

Item	Server	Mobile phone
CPU	3 GHZ	1.5 GHZ
Memory	8 GB	2 GB

The functional design of the OCSP server (responder) is shown as Figure 16, where each function is modularized [11].

In the prototype system, the wireless X.509 certificate's length is 983 bytes, the key length of all certificates is 163 bits (used by the ECC encryption/decryption mode), the value of hash function is 160 bits, and the size of the ARL is 10 K. For the whole verification process, the time comparison of the CDS_OCSP scheme and the original OCSP-based scheme is shown as Figure 17. Additionally, the computation time of all the encrypting functions is shown as Table 6.

In Figure 17, the CDS_OCSP scheme is finished between [12 s, 14 s]; the original OCSP-based scheme is finished between [15 s, 17 s]. As the CDS_OCSP scheme reduces the time and bandwidth consumption of downloading the CA certificate and the ARL and committing the OCSP request by the mobile terminal in the wireless network, the whole process time of the CDS_OCSP scheme is reduced about 18%, compared with the OCSP-based scheme. Also Table 6 shows that the computation time of all the encrypting functions is very short; the total time is less than 200 ms. Therefore, although the CDS_OCSP scheme adds the time cost of the encrypting functions' computation, the cost is beneficial.

6. Conclusions

This paper proposes a WPKI certificate verification scheme based on certificate digest signature-online certificate status protocol (CDS_OCSP). The proposed scheme optimizes the number of communication connections between the communication entity and the network, reduces the time and bandwidth consumption of downloading the CA certificate, the ARL, and committing the OCSP request by the mobile terminal in the wireless network, and uses the ECC-based encrypting/decrypting functions to sign and verify the certificate digest, which ensures the consistency of the verified certificates among the communication entities. The proposed scheme makes the certificate verification process more efficient and secure. Simulated and experimental results show that the proposed scheme effectively reduces the communication consumption of the wireless network and saves the storage space of the wireless entities.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Table 6: The average computing time of the encrypting functions.

Function	Computing entity		
	Content server	OCSP server	Client
$M_1 = F(\text{CServer.Ce\_Digest})$	13 μs		
$Z = E_{\text{pk}_c}^{\text{sk}_s}(\text{PW}, M_1)$	1.3 ms		
$M_1 = D_{\text{pk}_s}^{\text{sk}_c}(\text{PW}, Z)$			189 ms
$M_2 = F(\text{CServer.Ce\_Digest})$			157 μs
$M_3 = F(\text{CA.Ce\_Digest})$		13 μs	
$M_4 = F(\text{CServer.Ce\_Digest})$		12 μs	
$N_1 = H(\text{PW}, M_3 \oplus M_4)$		15 μs	
$N_2 = H(\text{PW}, M_1 \oplus M_3)$			270 μs

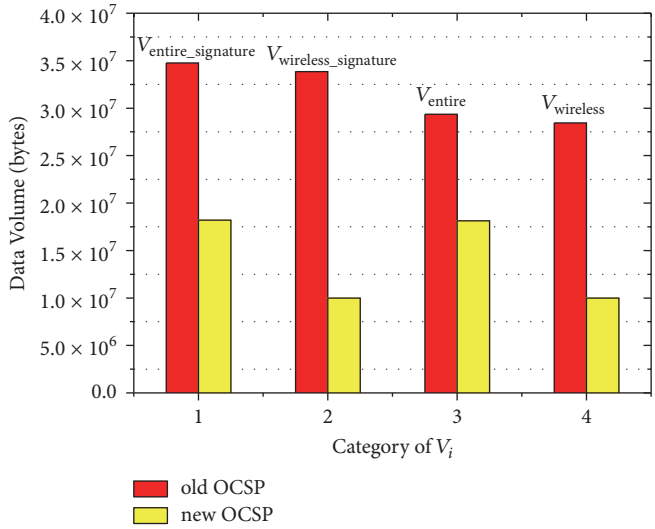

Figure 9: Data volume V_i for $N = 10000$, $U = 0.1$, and $Q = 5$.

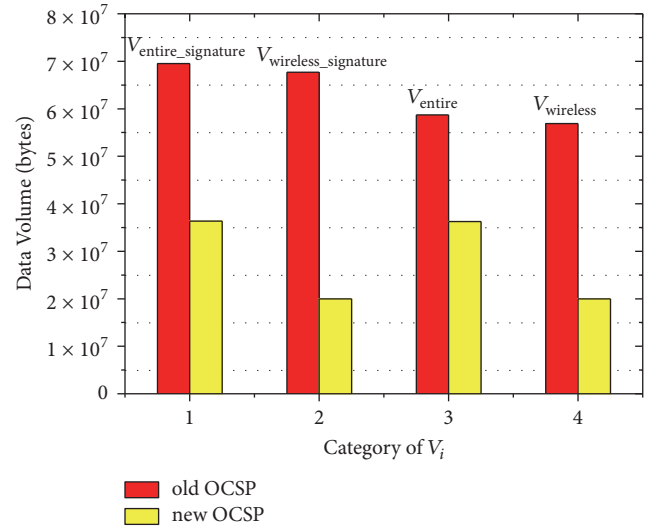

Figure 10: Data volume V_i for $N = 10000$, $U = 0.1$, and $Q = 10$.

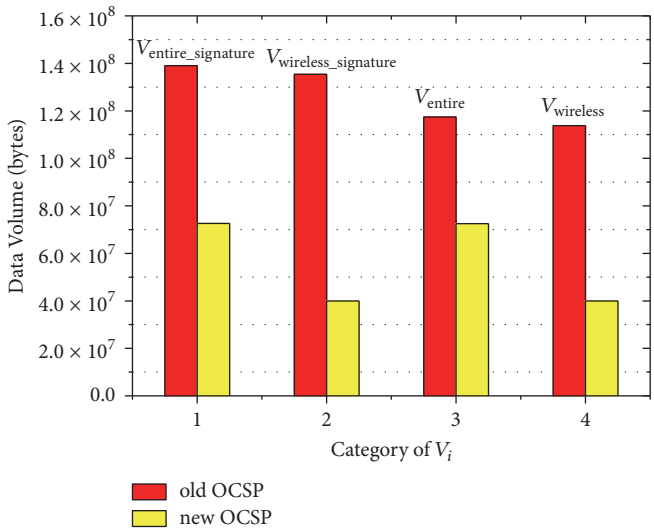

Figure 11: Data volume V_i for $N = 10000$, $U = 0.1$, and $Q = 20$.

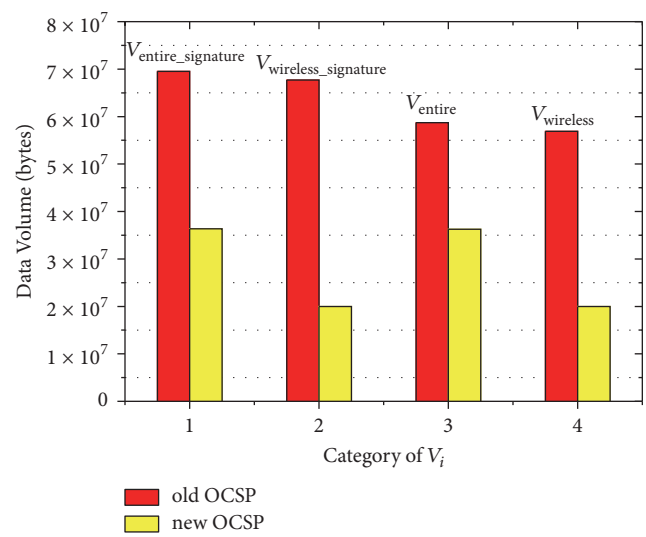

Figure 12: Data volume V_i for $N = 10000$, $U = 0.2$, and $Q = 5$.

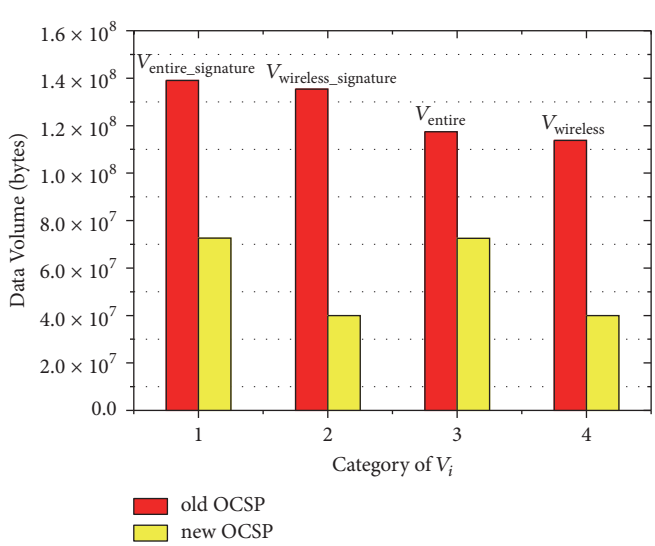

Figure 13: Data volume V_i for $N = 10000$, $U = 0.2$, and $Q = 10$.

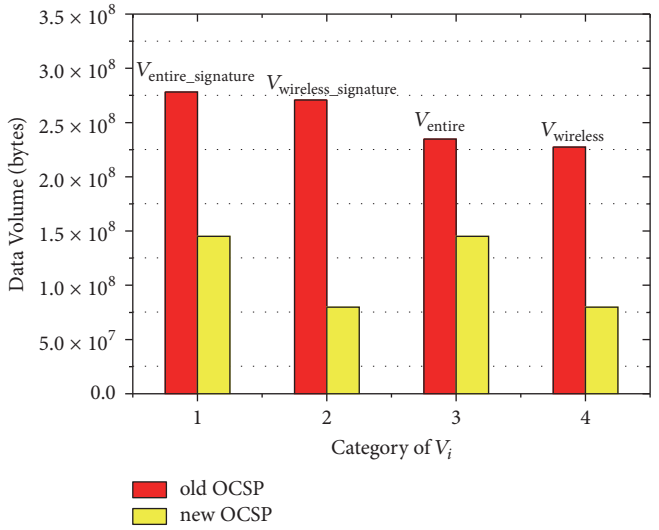

Figure 14: Data volume V_i for $N = 10000$, $U = 0.2$, and $Q = 20$.

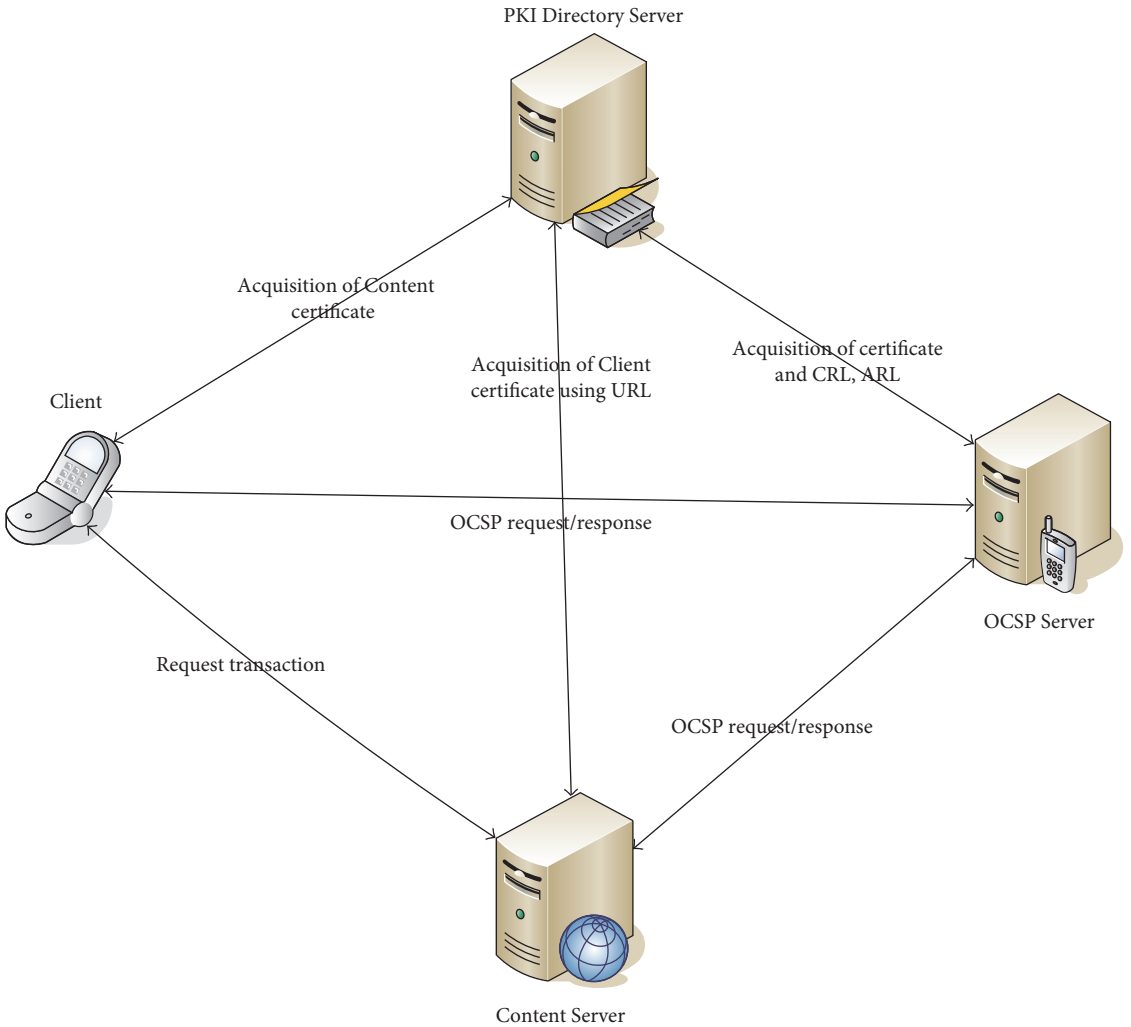

Figure 15: The structure of the prototype system.

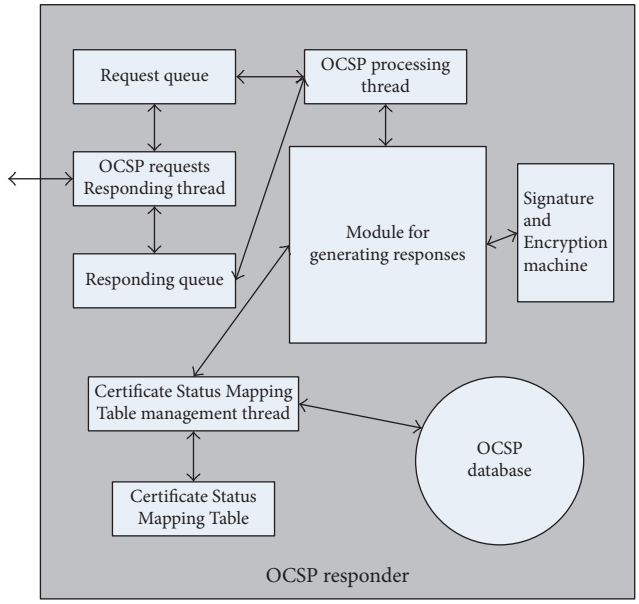

Figure 16: The function structure of OCSP server.

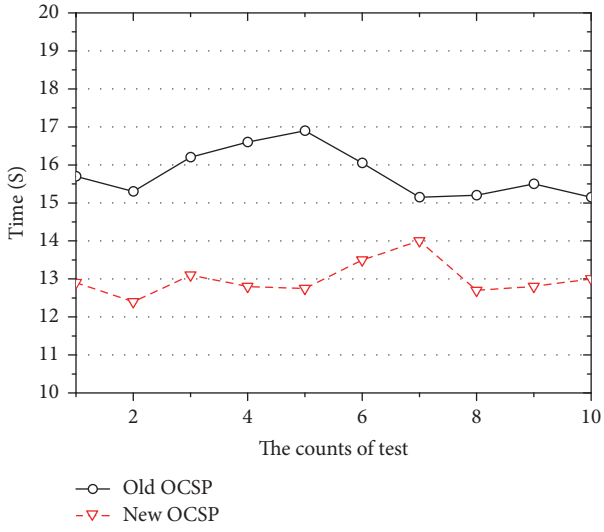

Figure 17: The whole time comparison of the two schemes.

Acknowledgments

This study was funded by the National Natural Science Foundation of China (no. 61402055 and no. 61504013), the Natural Science Foundation of Hunan Province (no. 2016JJ3012), and the Scientific Research Project of Hunan Provincial Education Department (no. 15C0041).

References

[1] OMA, Wireless Application ProtocolCWireless Public Key Infrastructure, WAP-217-WPKI, April 2001.

[2] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "RFC2560," Tech. Rep., 2013, https://www.rfc-editor.org/rfc/rfc6960.txt.

[3] C. Schwingenschlögl, S. Eichler, and B. Müller-Rathgeber, "Performance of PKI-based security mechanisms in mobile ad hoc networks," *AEÜ - International Journal of Electronics and Communications*, vol. 60, no. 1, pp. 20–24, 2006.

[4] D. Critchlow and N. Zhang, "Security enhanced accountable anonymous PKI certificates for mobile e-commerce," *Computer Networks*, vol. 45, no. 4, pp. 483–503, 2004.

[5] TU-T Recommendation X.509(1997)-ISO/IEC 9594-8:1998,Information technology-Open Systems Inter-connectionCThe Directory: Authentication Frame work.

[6] OMA, WAP Certificate and CRL, WAP-211-X.509, March 2000.

[7] L. C. Washington, *Elliptic Curves Number Theory and Cryptography, Discrete Mathematics and its Applications*, Discrete Mathematics and its Applications, Chapman & Hall/CRC, University of Maryland College Park, College Park, MD, USA, 2nd edition, 2008.

[8] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes and Cryptography. An International Journal*, vol. 19, no. 2-3, pp. 173–193, 2000.

[9] T. Perlines Hormann, K. Wrona, and S. Holtmanns, "Evaluation of certificate validation mechanisms," *Computer Communications*, vol. 29, no. 3, pp. 291–305, 2006.

[10] Y. Lee, J. Lee, and J. Song, "Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce," *Computer Communications*, vol. 30, no. 4, pp. 893–903, 2007.

[11] Y. Park and K. Rhee, "A Framework for Distributed OCSP without Responders Certificate," in *Proceedings of the Workshop on Information Security Applications (WISA 2004)*, 2004.

[12] J. L. Muñoz, O. Esparza, J. Forné, and E. Pallares, "H-OCSP: A protocol to reduce the processing burden in online certificate status validation," *Electronic Commerce Research*, vol. 8, no. 4, pp. 255–273, 2008.

[13] J. Lee, B.-J. Choi, S.-H. Seon, and E.-G. Kim, "Ocsp modification for supporting anonymity and high-speed processing in vehicle communication system," *Lecture Notes in Electrical Engineering*, vol. 373, pp. 607–612, 2015.

[14] M. Masdari, S. Jabbehdari, and J. Bagherzadeh, "Improving OCSP-Based Certificate Validations in Wireless Ad Hoc Networks," *Wireless Personal Communications*, vol. 82, no. 1, pp. 377–400, 2015.

[15] D. Berbecaru, M. M. Casalino, and A. Lioy, "FcgiOCSP: A scalable OCSP-based certificate validation system exploiting the FastCGI interface," *Software: Practice and Experience*, vol. 43, no. 12, pp. 1489–1518, 2013.

[16] F. Amounas, "Security Enhancement in Elliptic Curve Encryption of Amazigh alphabet using Genetic Algorithm," *International journal of Computer Science and Network Solutions*, vol. 3, no. 10, pp. 18–27, 2015.

[17] J. Iliadis, S. Gritzalis, D. Spinellis, D. De Cock, B. Preneel, and D. Gritzalis, "Towards a framework for evaluating certificate status information mechanisms," *Computer Communications*, vol. 26, no. 16, pp. 1839–1850, 2003.

[18] G. F. Marias, K. Papapanagiotou, V. Tsetsos, O. Sekkas, and P. Georgiadis, "Integrating a trust framework with a distributed certificate validation scheme for MANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, Article ID 78259, 2006.

[19] K. Papapanagiotou, G. F. Marias, and P. Georgiadis, "Revising centralized certificate validation standards for mobile and wireless communications," *Computer Standards & Interfaces*, vol. 32, no. 5-6, pp. 281–287, 2010.

[20] D. Kouřil, L. Matyska, and M. Procházka, "A robust and efficient mechanism to distribute certificate revocation information using the Grid Monitoring Architecture," in *Proceedings of the 21st International Conference on Advanced Information Networking and ApplicationsWorkshops/Symposia, AINAW'07*, pp. 614–619, Canada, May 2007.

[21] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP): IETF RFC2560, IETF NetworkWorking Group," Tech. Rep., 1999.

[22] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile[S]. RFC2459.PKIX Working Group," Tech. Rep., 1999.