This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

Investigating Public-Key Certificate Revocation in Smart Grid

Mohamed M. E. A. Mahmoud, *Member, IEEE,* Jelena Misic, *Senior member, IEEE,* Kemal Akkaya, *Member, IEEE* and Xuemin (Sherman) Shen, *Fellow, IEEE*

Abstract—The public key cryptography is essential for securing many applications in smart grid. For the secure use of the public key cryptography, certificate revocation schemes tailored to smart grid applications should be adopted. However, little work has been done to study certificate revocation in smart grid. In this paper, we first explain different motivations that necessitate revoking certificates in smart grid. We also identify the applications that can be secured by public key cryptography and thus need certificate revocation. Then, we explain existing certificate revocation schemes and define several metrics to assess them. Based on this assessment, we identify the applications that are proper for each scheme and discuss how the schemes can be modified to fully satisfy the requirements of its potential applications. Finally, we study certificate revocation in pseudonymous public key infrastructure where a large number of certified public/private keys are assigned for each node to preserve privacy. We target vehicles-to-grid communications as a potential application. Certificate revocation in this application is a challenge because of the large number of certificates. We discuss an efficient certificate revocation scheme for pseudonymous public key infrastructure, named compressed certificate revocation lists. Our analytical results demonstrate that one revocation scheme cannot satisfy the overhead/security requirements of all smart grid applications. Rather, different schemes should be employed for different applications. Moreover, we used simulations to measure the overhead of the schemes.

Index Terms—Certificate revocation schemes, public key cryptography, and smart grid communication security.

1 Introduction

The Smart grid has been envisioned as a promising evolution to the existing power grid [1]–[3]. It integrates communications into the electric transmission and distribution systems to enable two-way transmission of power and flow of information. It aims to improve reliability via self-healing and generate and distribute power efficiently, which can contribute to reducing the electricity prices. However, according to the Electric Power Research Institute (EPRI), one of the main challenges facing the smart grid is cybersecurity [4]. No responsible government will allow the deployment of the smart grid if there is a chance of launching cyberattacks, probably, by an opponent country to halt the nation's electricity supply.

Public key cryptography (PKC) is essential to secure many applications in smart grid such as firmware updates [5]. These applications will be discussed in Section 3.2. PKC can ensure message authenticity and integrity [6]–[8]. It can also ensure the non-repudiation of sending a message and its content, which is essential to enforce accountability. PKC can be used to enforce access control to protect the proper operation of the grid. In PKC, nodes should hold public key certificates to bind the certificate holder's identity to its public key. For more information on the certificates' format, we refer to reference [5]. When a certificate is issued, its validity is limited by an expiration date. However, there are motivations that necessitate revoking certificates before the expiration date, e.g., in case of compromised node. The motivations of revoking certificates in smart grid will be discussed in Section 4.1. Accordingly, to verify a certificate, two checks are needed to ensure that the certificate is neither expired nor revoked. Using a secure certificate revocation scheme is essential for the secure use of the public key cryptography.

A good certificate revocation scheme should take into account the characteristics and requirements of the smart grid applications. These characteristics include complexity, scalability, mobile and stationary nodes, and the large geographical spread of the communication networks. Comparing to other networks, the availability of the revocation information is a priority in the smart grid. Existing works on smart grid security such as [9], [10] use PKC, but they do not provide any schemes for certificate revocation, even though it is a required component. In [11]–[13], we have made the first attempt to study certificate revocation in Automatic Metering Infrastructure (AMI) networks. In this paper, we broaden our investigation to include certificate revocation in different smart grid applications. The security/privacy requirements of the smart grid are first discussed and then we discuss how PKC can satisfy these require-

- *M. Mahmoud is with the Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, Tennessee, 38505, USA. E-mail: mmahmoud@tntech.edu*
- *J. Misic is with Department of Computer Science, Ryerson University, Toronto, Ontario, M5B 2K3, Canada.*
- *X. Shen is with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada.*
- *K. Akkaya is with Department of Electrical and Computer Engineering at Florida International University (FIU).*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

ments in different applications. We then point out the motivations of certificate revocation and the metrics to evaluate certificate revocation schemes. We classify and discuss the existing certificate revocation schemes, and study certificate revocation in pseudonymous public key infrastructure ($PPKI$). Finally, we evaluate the schemes under the metrics and discuss how they can be used in potential smart grid applications.

In $PPKI$, each node should hold a large number of certificates with different public keys and pseudonyms to preserve its privacy. We target vehicle-to-grid communications as a potential application for $PPKI$. In this application, pseudonyms can be used to preserve the location privacy of the electric vehicles when they communicate with the grid to charge/discharge. The attackers may try to learn the location of a vehicle and the amount of power it charges to figure out the driving distance. The non-repudiation property of the $PPKI$ can help secure the communications and the payment of the power charging/discharging. Efficient certificate revocation in $PPKI$-based vehicle-to-grid communication is not easy because of the large number of certificates. A widely used approach to revoke certificates is by disseminating Certificate Revocation Lists (CRLs) that have the identifiers of the revoked certificates. To verify the status of a certificate, each node has to check whether the certificate's identifier is in the list. However, due to the large number of certificates, using the traditional CRLs for $PPKI$ is not efficient because they will grow very long. We discuss an efficient certificate revocation scheme for pseudonymous public key infrastructure, named compressed certificate revocation lists.

Our analytical results demonstrate that using certificate revocation schemes is essential for securing the smart grid, and one scheme cannot satisfy the overhead/security requirements of the different applications of the smart grid. Rather, different schemes should be employed for different applications. For example, physically protected nodes may not need as security strength as unattended nodes deployed in streets. Also, revoking important nodes such as a central unit should be done in a short time, but revoking less important nodes can tolerate some delay. Moreover, simulations have been used to measure the overhead of the schemes.

The remainder of this paper is organized as follows. Section 2 presents the system models. Section 3 discusses the security/privacy requirements of the smart grid and the applications that can be secured by PKC. The certificate revocation motivations and the metrics that can be used to evaluate the certificate revocation schemes are explained in Section 4. Section 5 discusses the certificate revocation schemes. Performance and security evaluations are given in Section 6. The related works are discussed in section 7, followed by conclusions and future work in Section 8.

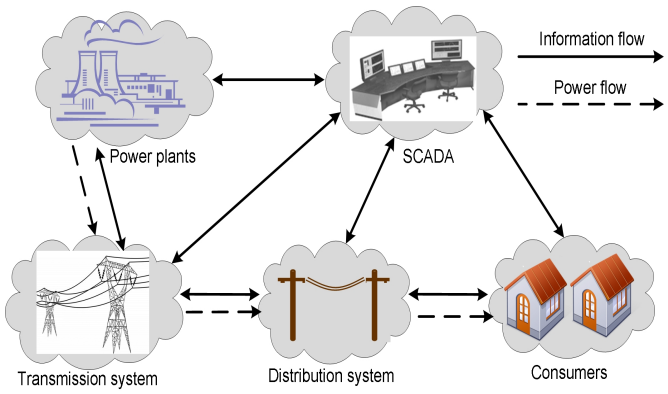


Fig. 1: The architecture of the smart grid.

2 System Models

Fig. 1 shows the considered smart grid architecture. The electric power is generated at the power plants and supplied to consumers via transmission and distribution substations. The transmission substations deliver power from the plants over high voltage transmission lines to the distribution substations. The distribution substations convert the electrical voltage to medium level and then distribute the power to the buildings' feeders to convert the voltage level into a lower level usable by consumer appliances. Supervisory control and data acquisition ($SCADA$) can communicate with all the grid systems. It monitors the distribution system to determine whether any actions should be taken to boost the reliability and efficiency or to respond to emergencies. $SCADA$ also monitors the power transmission substations and takes corrective actions within a few milliseconds (such as tripping circuit breakers) if anomalies are detected.

Consumers are the parties that use and pay for electrical power. Smart meters are two-way communication devices that are deployed at the consumers' premises. The utility companies will periodically receive measurements from the smart meters for billing and estimating the grid state. The grid provides consumers with real-time pricing information to help them to manage their power consumption to pay less and help the utility do necessary load reductions, e.g., shift power use from peak hours to non-peak hours. Distribution/transmission automation within substations involves monitoring and controlling devices in the substations to enhance the power system reliability and efficiency.

Some devices in the smart grid such as meters, sensors, and pole-top devices are unattended and have very weak physical protection to reduce their cost. The level of trust in these devices must be limited accordingly. An attacker tries to replace the legitimate firmware with his program, compromise the nodes and re-program them, or replace them with his own devices. However, other devices in the grid are physically protected well such as the devices of $SCADA$ and substations. It is not easy to compromise these devices by external attackers, but disgruntled employees can use their own credentials to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

attack the system.

3 Security/privacy requirements and PKC applications

3.1 Security/privacy requirements

The US National Institute of Standards and Technology (NIST) propose three main cyber-security requirements for the smart grid in [4]: availability, integrity and confidentiality. In this section, we extend these requirements and add privacy requirements.

Authentication: The receiver of a message should be able to ensure that the message is sent from the intended node. This can prevent impersonation attacks. This requirement is specifically important when the recipient takes actions based on the message. For instance, when a central unit sends a message to a circuit breaker to trip, it should be able to verify the identity of the sender.

Message integrity: The recipient of a message should be able to verify that the message has not been altered, replayed, or delayed. Message integrity is important for most smart grid applications. For instance, a home controller should periodically receive real-time electricity price and the integrity of these messages is important to enable the consumers to mange their power consumption. Message integrity requirement is also important to the measurements sent by sensors/meters because control centers take decisions based on this data.

Confidentiality: The loss of confidentiality is the unauthorized disclosure of information, i.e., unauthorized nodes should not be able to tell the content of messages. Confidentiality should be ensured in several applications in the smart grid, such as consumers' electricity consumption data, failure and grid state messages, etc.

Accountability and non-repudiation: For non-repudiation property, the sender of a message should not be able to deny either sending the message or its content. This property is important to enforce accountability in the smart grid to hold individuals accountable, assign liability, and provide information to investigators in case of a security breach. For example, damage may be caused if forged commands are sent to order devices to take wrong actions, and thus forensic investigations are required for understanding what happened to the system and identifying the attackers. This requirement is also important for securing the payment of power charging/discharging of electric vehicles.

Access control/authorization: This requirement aims to restrict the access of the network resources to the authorized nodes. Access control is necessary to ensure reliable and secure operation of the system. It enables the nodes to corroborate that a message sender has the privilege to issue some type of messages.

Availability: The network services should be available to the authorized nodes without excessive delay. This delay can be less than 4 ms for protective relays, subseconds for transmission wide-area situational awareness monitoring, seconds for substations and $SCADA$ data, minutes for monitoring non-critical equipment and market pricing information, and days for collecting long-term data such as power quality information. Availability is the most significant security requirement in the smart grid. The loss of availability can lead to serious problems, such as blackouts, due to the inability to properly monitor and control the grid. Availability is specifically important for systems such as $SCADA$, substation control system, and AMI that require real-time interaction.

Credential and identity revocation: The system should have the ability to exclude devices from the communication network by invalidating their keys when they show malicious behavior. This is *a fundamental requirement to defend against internal attackers and restore the safe operation of the grid if some devices are compromised*.

Privacy and anonymity: Privacy preservation is an important requirement for some applications in smart grid such as vehicle-to-grid communications. The common technique for ensuring privacy is by using pseudonyms instead of one permanent identity [14]. Each vehicle should be loaded with a set of pseudonyms, public/private keys, and certificates. Each pseudonym is used for a short time. For the secure use of pseudonyms, an adversary should not be able to link pseudonyms [15]. However, full anonymity is not desirable because it encourages attackers to launch attacks without being detected. It is also not desirable for payment system. A trusted party should be able to map pseudonyms to the real identity to enforce accountability and process the payment.

Not all these requirements are important for all smart grid applications. For instance, in some applications, a message recipient needs to make decisions such as whether consume more/less power, generate more/less power, turn a switch on/off, etc. In these cases, the message recipient needs to ensure that the message is sent from the intended sender and it has not been tampered with during transmission, but preserving the privacy of the sender or recipient may not be essential.

3.2 PKC for smart grid

PKC can satisfy the requirements discussed in Section 3.1 and offer several benefits compared to symmetric-key cryptosystems. Some of these benefits are summarized as follow:-

Flexibility, scalability, and efficiency: Any two nodes can communicate securely without the need for distributing/storing a large number of symmetric keys shared between each two nodes.

Non-repudiation: Unlike the symmetric-key cryptosystems, public key cryptography can achieve the non-repudiation property. As explained in Section 3.1, this property is important to enforce accountability, secure the payment, and provide information to investigators in case of a security breach.

Availability: Using PKC, communications can be secured without the direct involvement of a central unit.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

The reliance on a central unit may not be robust or scalable for many applications in the smart grid because the nodes cannot communicate when the unit is not available.

PKC can be used to secure several applications in the smart grid, as follow:-

Firmware updates: The ability to perform firmware updates allows the evolution of the applications without expensive physical visits to the devices. However, it is important to ensure that firmware updates are not used to install malwares. PKC can be used to ensure that the firmware update is sent from the authorized party and it is not modified during transit.

Operation and control: Remotely controllable intelligent electronic devices (IEDs) will be widely deployed to allow fast isolation of faults and restoration of electricity. These devices will receive control commands, e.g., to trip a switch, from control centers. Without protecting these messages, the attackers can send fake control commands, modify valid commands, and replay commands to cause chaos in the grid. The attackers can also reset the smart meters, order the meters to cut off electricity supply from houses, command the distribution feeders that supply a large number of consumers to disconnect to trigger a blackout, etc. PKC can operate in such massively distributed and locally autonomous setting.

$SCADA$/substations communications: $SCADA$ and substations monitor and control IEDs deployed in unattended locations (like pole tops) for automatic fault detection, isolation, and service restoration. They should receive information such as device states (on/off), alarms (overheat, overload, battery level, etc), and measurements (current, voltage, frequency, etc), and take corrective actions such as turn on/off automated switches, switch capacitor banks in and out, raise or lower voltage regulators, etc., to boost reliability and efficiency and respond to emergencies. In addition to ensuring the integrity of the messages, $SCADA$/substations need to verify that data is sent by the intended devices. They also need access control mechanisms that allow only authorized devices/users to configure or operate them.

Demand/response: From [16], the purpose of demand/response application is stated as "changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized". A house controller should frequently receive real-time electricity pricing information to manage the power consumption, e.g., to minimize the electric bill by reducing the power consumption during high-price periods (peak hours). Without securing demand/response messages, coordinated falsification of pricing information across many houses could cause grid instability. The integrity, availability and non-repudiation of pricing information are essential requirements since there could be financial losses and possibly legal implications.

Direct load control (DLC): In DLC application, smart appliances are configured by the end-user to communicate directly with the utilities for the efficient use of electricity [17]–[20]. For example, the utility may control lighting, thermal equipment (i.e., heating, ventilating, and air conditioning), refrigerators, and pumps. Usually, the on/off patterns are applied to some groups of loads during a time interval. The on/off periods of all groups under control should not be coincident in order to avoid some undesirable effects, such as the so-called payback effect (increase in peak power demand when compared with the situation without load control actions), that may cause strong reduction in revenues. The communications between the appliances and the utilities can be secured using PKC.

Advanced metering infrastructure network (AMI): Millions of smart meters are being deployed to enable the utility to interact with consumers. Each smart meter should send fine-grained electricity consumptions to the utility to be used for state estimation. Without securing the communications, external attackers can impersonate the meters and inject false data. The public key cryptography will enable the smart meters and the utility to secure the communications by verifying the origin and integrity of the data as proposed in [9].

Plug-in electric vehicles ($PEVs$): $PEVs$ are driven primarily by electric motor powered by a rechargeable battery that can be recharged by plugging into the grid. They can inject the energy stored in their batteries back to the grid at the times of high electricity load in a return of a financial incentive [21]. PKC can secure the communications between the vehicles and the grid and secure the payment of the power charging/discharging.

4 CERTIFICATE REVOCATION MOTIVATIONS AND METRICS

4.1 Motivations

Verifying the expiration of a certificate is necessary but insufficient. Another check is required to determine whether the certificate is revoked [22], [23]. The messages that are signed using revoked certificate should be discarded. This means that without holding a valid certificate, the nodes can be excluded from the grid's communication network. Strong motivations that necessitate revoking certificates to secure the smart grid are discussed as follows.

Key compromise: The private key of the certificate holder or the certificate authority (CA) that issued the certificate has been compromised or suspected to be compromised. Compromising (or revoking) a CA triggers revoking all the certificates issued by the CA. If the certificate is not revoked, the attacher who knows the private key can impersonate the certificate holder without any suspicion. If the compromised key is for a CA, the attacker can issue new certificates and revoke valid ones.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

Loss of security token: The private key might be stored in a smart card or USB device and the certificate holder (e.g., an employee) has lost it. Without revoking the certificate, the attacker can retrieve the private key and sends messages under the name of the employee.

End of certificate's purpose: The purpose of the certificate for which it was issued does not exist anymore. We discuss three cases named: *temporary certificates*, *change of affiliation*, and *defective devices*. For *temporary certificates*, a certificate may be issued for a temporary purpose, e.g., the hydro company may need to set up makeshift devices when it extends the power grid or repairs a damage. For *change of affiliation*, certificates are required for employees to use the grid's communication network. An employee's certificate is not only associated to his identity, but also to his privileges and permissions as proposed in [5]. Thus, if an employee is promoted or transferred to a different department/site or his contract has been terminated early, his certificate must be revoked. New certificates should be issued with the updated data such as the certificate holder's affiliation and privilege. For *defective devices*, the certificates of defective devices that are removed from service should be revoked. Otherwise, attackers can use their keys to launch attacks.

Malicious behavior: If the system loses trust in a device or an employee, e.g., due to evident malicious behavior, the system must promptly revoke their certificates to protect the network's proper operation. A member of the maintenance staff and a disgruntled employee who has physical access to the system and might also have extensive technical knowledge may act maliciously.

Change of security policy: Certificate revocation is necessary when the CA does not work under its defined policy anymore, e.g., when the certificate authority hierarchy changes.

Insecure key length: Certificate revocation is necessary when the secure key length becomes more than the used one. This might be due to advances in cryptanalysis and computing capabilities.

4.2 Metrics

We will use the following metrics to evaluate the certificate revocation schemes.

1) *Overhead*: The overhead of revoking a certificate and checking a certificate status should be minimal. Several metrics can be used to measure this overhead such as the communication overhead (or bandwidth requirement), storage area, and the computation cost on the CA and the nodes. The smart grid will involve communication over a variety of channels with varying bandwidths. Low bandwidth channels will be too slow to disseminate large certificate revocation information. Some devices such as residential meters may be limited in their computational power and/or storage space.
2) *Check latency*: When a signed message is received, the verifier has to check whether the certificate is revoked. The latency of this check should be minimized to expedite message authentication.
3) *Scalability*: This metric depicts how a revocation scheme scales up in large networks. A scheme with a large number of potentially revocable certificates is expected to require more resources comparing to small-scale schemes.
4) *Robustness*: This metric measures the scheme's ability to resist potential threats [24]. Availability is one way to measure robustness. For example, if the scheme requires an online and interactive server, the availability of the certificate revocation information relies on the availability of the server.
5) *Vulnerability period (or revocation latency)*: This is the latency between deciding revoking a certificate and the distribution of revocation information to all devices, i.e., when revocation is indeed implemented [25]. A good certificate revocation scheme should minimize this period because the messages sent by revoked certificates will be accepted during this period. The vulnerability period should particularly be minimized for the certificates of important nodes such as control centers because these nodes have enough privileges to launch serious attacks that can cause substantial damage.

5 CERTIFICATE REVOCATION SCHEMES

In this section, we explain five certificate revocation schemes called short-lived-certificate, tamper-proof-device, online certificate status server, certificate revocation list (CRL), and compressed CRL.

5.1 Short-lived certificates

This scheme makes use of the fact that *certificates are automatically revoked when they expire*. Short-lived certificates are self-revoked after short time [26]. If the CAs issue short-lived certificates, the nodes need to frequently contact them to renew their certificates. The CAs can revoke certificates by denying renewing them.

5.2 Tamper-proof-device based scheme

The main idea behind this scheme is that certificates can be revoked by deleting the associated private keys [27]. Without the private keys, the certificates' holders cannot compute valid signatures despite of having unexpired certificates. Tamper proof device (TPD) should be installed in each node and the device should be secure enough to resist manipulation. TPD stores the node's private key, and performs security functions such as signature and verification operations.

To revoke a certificate, the CA sends *Certificate Revoke Command* (CRC) message to the TPD of interest to delete the private key. The message should be encrypted either by a symmetric key or the device's public key to prevent the attackers from knowing

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

the purpose of the message and dropping it before it reaches the TPD. Only the TPD can decrypt the message. The CRC message has the identities of the CA and the device, a timestamp, the identifiers of the certificates to be revoked, and the CA's signature on the message. The CA's signature enables the TPD to verify the authenticity and integrity of the message. The message's format is as follows:

$$CA \rightarrow TPD_U : ID_{CA}, E_K(REVOKE, Ts, Cert\_IDs), Sig_{CA}(E_K(REVOKE, Ts, Cert\_IDs))$$

Where ID_{CA} is the identity of the CA and $E_K(X, Y, Z)$ denotes the encryption of "X, Y, Z" with the key K. $REVOKE$ indicates the message's type, Ts is a timestamp, and $Cert\_IDs$ is the identifiers of the certificates to be revoked. $Sig_{CA}(Y)$ is CA's signature on Y.

When TPD_U receives the message, it first verifies the CA's signature and decrypts the message. Then, it sends back a *Certificate Revocation Acknowledgment* (CRA) message to confirm revoking the certificate(s). The CRA message has the following format:

$$TPD_U \rightarrow CA : ID_U, E_K(REV\_CONF, Ts, Cert\_IDs), Sig_U(E_K(REV\_CONF, Ts, Cert\_IDs))$$

Where ID_U is the identity of node U, REV_CONF indicates that the message type is revocation confirmation. $Sig_U(Y)$ is node U's signature on Y. After sending the message, node U immediately deletes the private keys of the revoked certificates.

If the CA does not receive the CRA message, e.g., because it is dropped, the CA has to re-send the CRC message. However, node U will not be able to compose a valid CRA message because it deleted the private keys. To resolve this, node U should store both the CRC and CRA messages for a period of time, so that it can re-send the CRA message when it receives the CRC. Note that if a device has multiple certificates from different CAs, revoking a CA's certificate should not affect the other CAs' certificates. This is because each CA is responsible for revoking the certificates it issues.

5.3 Certificate revocation list

In this scheme, certificates can be revoked by disseminating certification revocation information using Certificate Revocation Lists (CRLs) [28], [29]. A CRL is issued by each CA to list the identifiers of the revoked certificates that were issued by the CA. A certificate is revoked if its identifier is found in the CRL, otherwise it is valid. The CRLs are periodically updated and distributed, and each node has to store the most up-to-date version, otherwise, it verifies the certificate status against outdated list and may accept messages sent with revoked certificates.

The format of a CRL is given in Fig. 2. The CRL has the version, issuer, serial number, issuing date, expiration date, and complete list of the revoked (and not yet expired) certificates' identifiers together with their dates of revocation and the revocations' reasons (may be unspecified). The CRL also has the issuer's digital signature on its content and the algorithm used to generate the signature. The digital signature can guarantee the integrity and authenticity of the CRL. Expired certificates should be removed from the list since they are not accepted by the nodes.

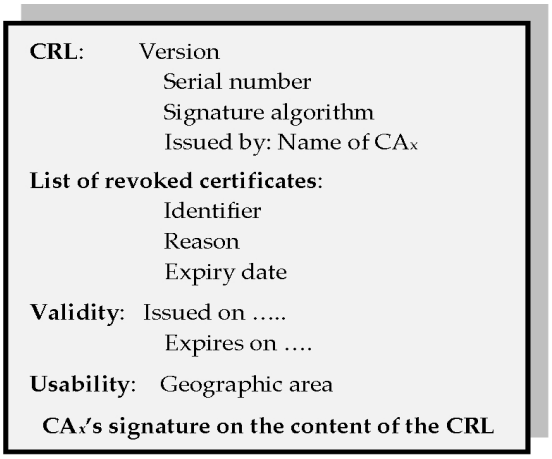


Fig. 2: The format of a CRL message.

To verify a CRL, each node has to do the following: (1) verify the CA's signature, (2) ensure that the CRL's serial number is the expected one, (3) check that the CRL has arrived at the expected time, and (4) check that the certificates declared as revoked in the last CRL (and not yet expired) are included in the current CRL. Two techniques can be used to sent CRLs: (1) CRLs are sent at fixed time interval even if there is no new updates; or (2) CRLs are sent after accumulating a proper number of certificate, passing a maximum time interval, or urgent revocation information needs to be distributed, e.g., revoking important nodes.

The CA attaches the certificate revocation reason to the CRL because it can resolve some problems. For example, two certificates $Cert_1$ and $Cert_2$ having the same public and private keys are issued to one device by two different CAs called CA_1 and CA_2, respectively. The problem arises if CA_1 revokes $Cert_1$ and CA_2 says nothing about $Cert_2$. This problem could be resolved if the reason of revocation is known. For example, if a certificate is revoked because of key compromise, all certificates with the same public/private key pair should be revoked. However, if the certificate is revoked because the subject is no longer affiliated with CA_1, the revocation of $Cert_1$ should not affect the status of the certificate $Cert_2$. An example from the smart grid for this case can be a premise that has two certificates: one for power distribution system and the other for power generation system. The certificate of the power generation system should be revoked if the premise is no longer operating renewable resources generator, but this should not affect the certificate of the power distribution system.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

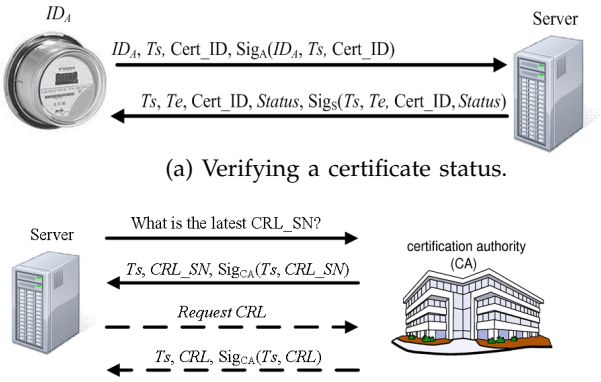
In the remainder of this section, we discuss two possible enhancements to CRL-based revocation scheme, named incremental CRL ($I-CRL$) and partitioned CRL ($P-CRL$). $I-CRL$ is a short CRL that provides incremental information about the certificates whose status changed since the last update [30]. This technique can reduce the size of the CRL updates because if a certificate is revoked in one CRL message, it will not be re-sent in the next messages. The devices should cache the base CRL and add to it the new certificates that have been revoked in the following updates. The certificates' revocation information should be stored in the devices until the certificates expire. Therefore, $I-CRL$ can reduce the overhead of distributing the revocation information because it is much shorter than a complete CRL.

In mobile networks, any two nodes can communicate because of the nodes' mobility. In many applications in the smart grid, the nodes will only communicate with a limited number of other nodes due to the stationary nature of the network. This means that the nodes do not need the revocation information of all the certificates, but only the certificates of interest. Using this observation, a partitioned CRL ($P-CRL$) can reduce the overhead by storing and distributing the revoked certificates of interest instead of all the revoked ones. The size of $P-CRL$ is much shorter than the complete CRL. To implement the $P-CRL$ technique, each node should register its certificates of interest with the CA.

In an ideal case, the certificate authority creates the $P-CRL$s that only has the nodes' certificates of interest. However, this fine level of granularity will impose overhead on composing and distributing the $P-CRL$s because a large number of signatures will be needed. To reduce the overhead, $P-CRL$ can be composed for the certificates of interest of a group of nodes, e.g., in one geographic region, in such a way that can keep the $P-CRL$ size acceptable with a reasonable overhead on the CA. What promotes this idea is that the function of many nodes in the smart grid is identical, i.e., a group of devices in one geographic area has identical or overlapped certificates of interests. It is worth mentioning that merging both incremental and partitioned CRLs in one scheme, called $IP-CRL$, can much reduce the overhead.

5.4 Online certificate status server

In this scheme, an online and interactive certificate status server is used. The server stores updated revocation information for the certificates of interest. These certificates are the ones needed by the nodes in the server's domain. As shown in Fig. 3a, the verification of the certificates status can be done by request/response packets. When a node needs to check the status of a certificate, it simply composes a *Certificate Status Query* packet with the certificate identifier and sends it to the server. ID_A, Ts, $Cert_{ID}$, and $Sig_A()$ are the identity of the node that



(a) Verifying a certificate status.

(b) Obtaining an updated CRL.

Fig. 3: Online certificate status server based scheme.

sends the query, the current timestamp, the identifier of the certificate that the sender needs to verify its status, and the sender's signature, respectively. Upon the receipt of the query, the server composes a signed response with the status information and sends the response back to the node. The format of the response packet is given in Fig. 3a, where $Status$ and T_e are the certificate status and the expiry date of the certificate status, respectively. The certificate status in the server response can be "Valid", "Revoked", or "Unknown". The nodes need to send a new request when the status expires. This scheme can provide the status of a particular certificate without the need to acquire the complete revocation list.

As shown in Fig. 3b, the server should periodically contact the CA to update its revocation information. The CA responds with the version of the current CRL together with a timestamp, all signed by the CA. The server compares the version of the current CRL with the one it stores. If the current CRL is newer, the server requests the new CRL from the CA. Alternatively, the CA can distribute the CRL when it is updated. It is worth noting that the $P-CRL$ and $I-CRL$ can be used to send the certificate revocation information to the server instead of the entire CRL to reduce the overhead.

5.5 Compressed CRL

Using one certificate with a unique identity jeopardizes the privacy of the users and enables the attackers to link the users' messages. Pseudonymous public key infrastructure ($PPKI$) [7], [8], [31] is an extension to the standard PKI which aims to preserve the users' privacy by concealing their real identities. Each node is preloaded with a set of certificates with different pseudonyms and public/private keys. Each certificate is used only for a short time, and thus the nodes need to frequently contact the CA to obtain new sets of certificates. Privacy can be preserved because the certificates do not have any information about the real identity of the user and linking pseudonyms is infeasible for the adversary. The certificates enable the nodes to authenticate themselves while preserving their privacy. This authentication can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

prove that the user is a legitimate member in the network, but without revealing its real identity.

In the smart grid, electric vehicles will need to communicate with the grid to charge and inject power. By allowing vehicles to charge during off-peak hours (storing surplus electricity generated during that time) and discharge during peak hours (returning the stored energy back into the grid), lots of benefits can be achieved. It can smooth the variable generations of renewable sources and improve the grid reliability by using the vehicles' stored energy when the energy demand exceeds the supply [32].

However, the location privacy of the vehicles' owners is a great concern. When a vehicle charges or discharges at the owner's home, it can be known that the owner is at home. Similarly, it can be known when a vehicle's owner is at work and shopping malls. Moreover, regularly parking at a clinic or at a lawyers office can reveal private information about a persons financial status, habits, or health situation. The followings are interested in the users' private data:-

- Employers wondering whether their employees return home late which can negatively affect their productivity.
- Car insurance companies are interested to know how the drivers use their cars.
- Law enforcement officials may be interested to know vehicles' locations for investigations, e.g., to confirm the presence of a driver at an certain location at a certain time.

Although $PPKI$ is a very promising approach to preserve privacy in vehicle-to-grid communications, certificate revocation is a challenge because of the dramatic increase in the number of certificates in the network. In PKI, a single certificate should be revoked when revoking a device, but all the certificates assigned to the device should be revoked in $PPKI$. Using the regular CRLs is not efficient because revoking a device requires adding many certificates to the CRL which much increases its size. Obviously, distributing a large CRL is inefficient and bandwidth consuming. Therefore, an efficient certificate revocation scheme is essential for the success of $PPKI$. We introduce compressed CRL ($C-CRL$) scheme that can significantly reduce the size of the CRL. Reducing the overhead can enable distributing CRLs more often with acceptable overhead, which can make them fresher and reduce the vulnerability period.

The CA creates a group of certificate identifiers that appear to be unrelated, but in fact they are related by a secret key chain known only to the CA. As illustrated in Fig. 4, for each group of certificates, the CA creates the key chain K_1, K_2, .., K_n by iteratively hashing an initial key K_1. Then, the CA computes the pseudonyms $ID^{(1)}$, $ID^{(2)}$, ..., $ID^{(n)}$ using a random nonce (R) and the key chain. From the figure, it can be seen that each pseudonym is the hash value of the the corresponding key in the key chain and the previous pseudonym, i.e., $ID^{(i)} = h(K_i, ID^{(i-1)})$ and $1 \leq i \leq n$, where $h(X,Y)$

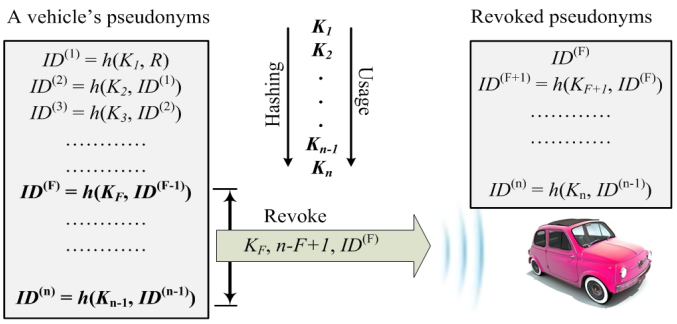


Fig. 4: $C-CRL$-based scheme.

denotes the hash value of X concatenated to Y, n is the size of the hash chain, and $ID^{(0)} = R$. Each key in the key chain is used to compute one pseudonym. It is obvious that without knowing K_1, linking the pseudonyms is infeasible. Also, with knowing K_{i+1} and $ID^{(i)}$, the pseudonyms $\{ID^{(i+1)}, ID^{(i+2)}, ..., ID^{(n)}\}$ can be computed but the pseudonyms $\{ID^{(1)}, ID^{(2)}, ..., ID^{(i-1)}\}$ cannot be computed because the hash function is one way, i.e., given K_i, it is easy to compute K_{i+1} = $H(K_i)$, but it is infeasible to compute K_{i-1}, where K_i = $H(K_{i-1})$.

From Fig. 4, to revoke a vehicle, the CA releases the current pseudonym $ID^{(F)}$, the current key in the key chain that is associated with the current pseudonym (K_F), and the number of revoked certificates ($n-F+1$). The vehicles can compute the complete list of revoked certificates' identifiers locally. They first compute the key chain by iteratively hashing K_F to compute $\{K_{F+1}, K_{F+2}, ..., K_n\}$. Then, using the key chain and $ID^{(F)}$, the node can compute the revoked pseudonyms, i.e., $\{ID^{(F+1)}, ID^{(F+2)}, ..., ID^{(n)}\}$. In this way, a large set of certificates can be revoked by only adding a key and a pseudonym to the CRL.

In [33], Haas et al. propose a scheme to reduce the CRL size in the anonymous communications of VANETs. There are two main differences between this scheme and the one discussed in this section: 1) the efficient hashing operations are used instead of the symmetric key encryption/decryption operations; and 2) one secret value should be stored/computed for each certificate set instead of two in [33].

6 DISCUSSIONS AND EVALUATIONS

In this section, we evaluate the certificate revocation schemes discussed in the previous section using the metrics discussed in Section 4.2. We also discuss the potential smart grid applications for each scheme. A comparison between the certificate revocation schemes is given in Table 1.

6.1 Short-lived certificates

Unlike the certificate revocation list scheme, the short-lived-certificate scheme can save the overhead of dis-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

TABLE 1: A comparison between different certificate revocation schemes.

	Short-lived certificates	**Tamper-proof-device**	**Online server**	**CRL**
Overhead	• No distribution to the revocation information • Tradeoff with the certificates' lifetime	Low	Low storage at the nodes but always-available communication with the server	Depends on CRL size and the frequency of distributing CRLs
Check latency	None	None	Depends on the speed of the connection with the server	Depends on the CRL size
Scalability	Tradeoff with the certificates' lifetime	Scalable but expensive	The server can be a bottle neck	The CRL size increases with the increase of the number of certificates
Robustness	Depends on the security of the CA	Depends on the security of the CA and the tamper proof device	Depends on the security of the CA and the server, and the availability of the communications with the server	Depends on the security of the CA
Vulnerability period	Tradeoff with the certificates' lifetime	Short	• Depends on the freshness of the revocation information stored at the server • Tradeoff with the communication overhead	Tradeoff with the overhead

TABLE 2: Overhead measurements of tamper-proof-device and online certificate status server based schemes.

	Packet size	**Computational time**	**Computational energy**
***CRC*/*CRA* packets**	148 Bytes	• Composition: 15.64 ms • Verification: 0.55 ms	• Composition: 550 mJ • Verification: 16.2 mJ
Query/Response packets	• Query: 142 Bytes • Response: 144 Bytes	• Composition: 15.64 ms • Verification: 0.55 ms	• Composition: 550 mJ • Verification: 16.2 mJ

tributing the revocation information. The scheme can also reduce message authentication delay because it can reduce the latency of the certificate status check. Instead of checking both the expiration and the revocation of the certificates, only the expiration check is required because unexpired certificates are also unrevoked. There is an obvious tradeoff between the overhead and the revocation latency. Shorter certificate lifetime can reduce the revocation latency, but with more overhead to issue/distribute certificates more often. This could constitute a high load on the CA and the network. On the contrary, long certificate lifetime gives the attackers more time to operate before being revoked, but with lower certificate renewals overhead. There is an obvious tradeoff between revocation latency and scalability and this tradeoff can be controlled with the certificates' lifetime. The scheme is more scalable with using longer certificate lifetime but with more revocation latency. The scheme's overhead can be reduced by using the certificate renewal scheme proposed in [5] that can reduce the overhead of issuing/distributing certificates using hash chain. In this case, the revocation latency and scalability can be improved with acceptable overhead.

This scheme is suitable for the applications that require fast message authentication. It should not be used for the applications that require immediate revocation of the misbehaving nodes to decrease the time window in which the nodes can jeopardize the proper operation of the grid. Accordingly, the scheme can suit the nodes that have uncritical privileges that do not enable them to take important actions if compromised. It is also proper for the cases in which it is hard to compromise the nodes. Since the smart meters and the field devices are unattended and the attackers have full access to them, to use the short-lived certificates scheme securely, these devices should have hardware security. The scheme can also be used in substations or $SCADA$ because the devices are physically protected.

6.2 Tamper-proof-device based scheme

The main advantage of this scheme is the low communication and computation overhead. Only a couple of packets are required to revoke certificates. The low overhead can make the scheme more scalable than short-lived certificates scheme, but the widespread use of the scheme is costly because tamper proof devices should be installed in the nodes. The low overhead can improve the scheme's scalability but the widespread use of the scheme is costly because tamper proof devices should be installed in the nodes. Verifying a certificate revocation status takes no time because a certificate is valid if the signature is valid. This can expedite message authentication. Another important advantage is the very low revocation latency. Certificates are revoked instantly after receiving a CRC message.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

One signing operation and one symmetric-key encryption are required to compose a CRC or CRA message. One verifying operation and one symmetric-key decryption are required to verify a CRC or CRA message. In order to estimate the required computational times and energy to compose and verify a CRC or CRA message, we have implemented 1,024-bit RSA public key cryptosystem and 128-bit AES symmetric-key cryptosystem using Crypto++ library [34] and 1.6 GHz Intel processor. The signature size is 128 bytes and the signing and verifying operations require $15.63\ ms$ and $0.53\ ms$, respectively. The AES encryption/decryption operations require $1.52\ \mu s/16$ bytes. From [35], the energy consumption of AES encryption/decryption operation is $1.21\ \mu J$ per byte, and the energy consumptions for RSA signing and verifying operations are $546.5\ mJ$ and $15.97\ mJ$, respectively. A node's identity, packet type, timestamp, and one certificate identifier require four, one, five, and five bytes, respectively.

Our measurements indicate that the CRC and CRA packet size is 148 bytes. The computational delay and energy consumption for composing a CRC or CRA message are $15.64\ ms$ and $550\ mJ$, respectively. The computational time and energy consumption for verifying a CRC or CRA packet are $0.55\ ms$ and $16.2\ mJ$, respectively. These results are summarized in Table 2.

The scheme is suitable for the applications that require immediate revocation of misbehaving nodes. The low overhead can make the scheme suitable for $PPKI$ because all the certificates of a device can be revoked by one message. The immediate revocation property is important especially for the highly privileged nodes such as control centers, gateways, some $SCADA$ devices, etc.

6.3 Online certificate status server

This scheme requires low storage at the nodes, but it does require always-available communications to the server. The nodes can acquire the certificates' revocation status without the need to store complete CRLs. This is very beneficial when it is inefficient to store CRLs at the nodes because of limited memory or long CRLs. Obviously, the server is a single point of failure, i.e., the nodes cannot check the status of the certificates when the server fails. The server should be fully secure and tamper resistant. In addition, the scheme does not scale well to avoid creating a bottleneck at the server. One server cannot serve many nodes and deploying many servers is costly. The scheme can reduce the vulnerability period provided that the server keeps the most-updated revocation information. Decreasing the validity period of the responses decreases the window of vulnerability but increases the communication overhead with the server. The certificates revocation verification can be done in a timely manner if the connection between the devices and the server is fast.

We refer to Section 6.2 for the computation time and energy of signing and verifying operations. A node's identity, certificate status, timestamp, expiry date, and certificate identifier require four, one, five, five and five bytes, respectively. The signature size is 128 bytes. The size of the query and response packets are 142 and 144 bytes, respectively. These results are summarized in Table 2.

In *masquerade* attack, attackers attempt to masquerade the server and fabricate the responses. For *response integrity* attack, attackers try to modify the response sent by the server. For *replay* attack, an attacker could resend an old (valid) response prior to the revocation of a certificate. The scheme is resilient to these attacks because of signing the responses sent by the server. Since timestamp is attached to the response packet's signature, replayed packets can be identified and discarded.

This scheme is suitable for unscalable networks that can provide physical protection to the server such as $SCADA$ and substations. In AMI networks, the gateway can play the role of the certificate status server, but this scheme may not be efficient for large scale AMI networks because of the increased communication and computation overhead with the server.

6.4 Certificate revocation list

It is inefficient to compose and distribute an updated CRL momentarily after a certificate is revoked, because this imposes a huge overhead. Instead, the CA has to wait until it accumulates a number of revoked certificates and then release them as a batch. There is a tradeoff between the overhead in terms of distributing of CRLs and the vulnerability period. This scheme has an interesting feature for smart grid that is an offline certificate revocation check. CRLs are inappropriate for the applications that require momentary certificate revocation because the inherent overhead of CRL distribution prohibits timely distribution of revocation information [36]. The CA's signature on the CRLs can protect the authenticity and integrity of the CRLs.

Reducing the certificates' lifetime can help shorten the CRL because the revoked certificates' identifiers should stay in the list for a short time until they are expired. However, short-lifetime certificates imposes large overhead on the CA due to renewing/distributing the certificates often. The smart grid will implement different systems with different security/overhead requirements. A good certificate lifetime should depend on the longevity of its purpose. It is not expected that all the certificates will have the same lifetime. A certificate's lifetime should be determined to balance between the CRL size and the overhead of composing and distributing them. For example, when certificates are issued to employees who may change their position after few years, it would be appropriate to issue certificates with relatively short lifetime, so that in case of revocation, the certificates stay in the CRL for a short time. Some certificates may be issued to devices that are deployed with the intent to keep them operating for many years, and these devices

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

are housed in a secure environment and have low failure likelihood. In this case, the certificates' lifetime can be long as the probability of revoking them is low. Reducing the CRL size can expedite the message authentication because it takes less time to search for a certificate.

In $P-CRL$, each CA groups the full CRL into a series of partitioned CRLs that contain the certificates of interest of a group of nodes. This grouping should be done in such a way that decreases the number of partitioned CRLs with acceptable overhead on the CA. It is possible that one certificate is included in more than one group. For example, if the full CRL of a CA has $10,000$ revoked certificates and a node's list of revoked certificates of interest is only 50, without partitioning, the node will receive $9,950$ unneeded certificates, but with partitioning the $P-CRL$ size will be between 50 and $9,949$ certificates.

Partitioning is more efficient when the degree of overlapping among the nodes' certificates of interest is high, i.e., $P-CRLs$ are fewer and shorter. This can be applicable to the field sensor nodes. However, using $P-CRL$ may not reduce the overhead a lot in some applications, e.g., a substation has a large number of certificates of interest because it communicates with a large number of devices. In this case, the substation can receive multiple $P-CRLs$ that cover all its certificates of interest, or it may revert to a different certificate revocation scheme.

For $C-CRL$ scheme, the size of the certificate revocation list is linear with the number of revoked certificate series, irrelative to the number of revoked certificates in each series. Only a single entry needs to be added to the $C-CRL$ to revoke a series of certificates. In this scheme, *the CAs can provide the nodes with enough certificates for privacy preservation with keeping the size of the CRLs reasonable*. Linking the certificates is infeasible without knowing the secret key used to compute their identifiers, i.e., the certificates' identifiers appear unrelated but they can be linked using a secret key. This unlinkability property is important to preserve the nodes' anonymity. Our scheme needs a secure one-way keyed hash function that can satisfy the following properties [37]:

1) Given X and K, it is easy to compute $h(K,X)$, but given $h(K,X)$ and X, it is infeasible to compute K.
2) Given $h(K,X)$ and X, without knowing K, it is infeasible to link $h(K,X)$ and X.
3) Given X and K, it is computationally infeasible to find $X \neq X'$ such that $h(K,X') = h(K,X)$.

Fortunately, there are several secure and efficient hash functions. *SHA-1* has 20-byte hash value and can process 16.79 Mega bytes per second and consume only 0.76 J/byte as given in [38].

Backward unlinkability means that linking a certificate with the previously used ones in the same series is infeasible. In our scheme, certificates are not linkable without knowing the key chain used to generate their identifiers. If a device is revoked, the attackers are able to compute the certificate identifiers of the revoked certificates, but they cannot compute the identifiers of the used certificates before revoking the device. The attackers cannot also link the revoked certificates with the ones used before revoking the device because it is infeasible to compute the keys used to compute them due to the unidirectionality of the hash function, i.e., given K_F, it is easy to compute $\{K_{F+1}, K_{F+2}, ..., K_n\}$ but it is infeasible to compute $\{K_{F-1}, K_{F-2}, ..., K_1\}$. Specifically, the attackers cannot link the certificates that are used prior to revocation because the released key (K_F) cannot be used to generate the certificates' identifiers that were used earlier. The backward privacy property is desirable in several scenarios, e.g., if a vehicle' credentials are revoked due to changing the owner, the privacy of the old owner can be preserved. The CA can map the certificates' identifiers to the real identity of the vehicle when needed. This is important to enforce accountability. If the system suspects that a vehicle is malicious, the CA (that is trusted) can identify this node.

The total number of pseudonyms that should be loaded in each vehicle is $D \times T \times 365$, where D and T are the average time each vehicle communicates with the grid in one day and the pseudonyms' consumption rate (the number of pseudonyms used/minute), respectively. For example, if D and T are three hours and one pseudonym/minute, respectively, the number of pseudonyms is $65,700$. Without our scheme, revoking a vehicle will increase the CRL size by $65,700$ elements but in *C-CRL*, only one element will be added. Given the large number of vehicles, the CRL will dramatically grow. For example, if the total number of vehicles is 5 millions and only 1% of them are revoked, the number of elements in the CRL and *C-CRL* are $3,285$ millions and $50,000$, respectively. Note that during the charging/discharging times, each vehicle needs to frequently change its pseudonyms to preserve its location privacy. Using *SHA-1*, each element in *C-CRL* requires around 42 bytes, but the size of an element in the CRL is 4 bytes. Figs. 5 and 6 give the sizes of the *C-CRL* and CRL at different numbers of vehicles and certificate revocation rates, respectively. The figures can show that the size of *C-CRL*s are much smaller than the CRLs.

7 RELATED WORK

In [39], Raya et al. propose a certificate revocation scheme for vehicular ad hoc network (VANETs). They use Bloom filter to store the revoked certificates' identifiers compactly. However, Bloom filters suffer from false positive, i.e., there is a chance that a valid certificate is mistakenly considered revoked. Unlike VANETs, the communication availability is a priority in smart grid and false positives will not be acceptable. A meter may miss a command to disconnect power because of false positives. They can also cause financial losses if a meter misses power pricing information.

Papadimitratos et al [40] propose a scheme to distribute large CRLs efficiently across wide regions in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

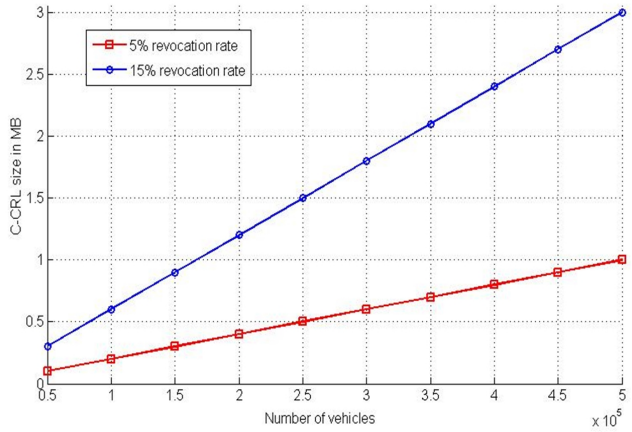


Fig. 5: *C-CRL* size versus the number of vehicles.

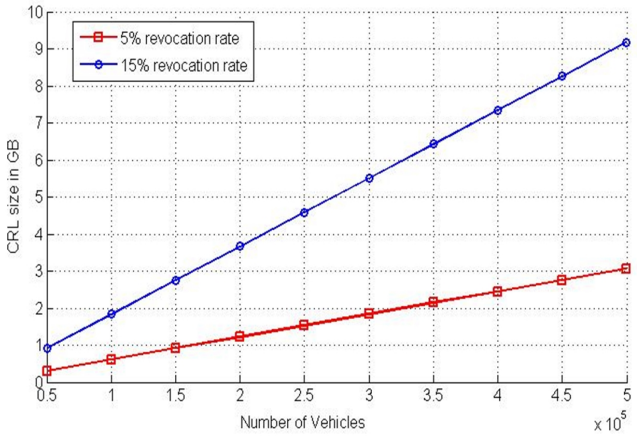


Fig. 6: CRL size versus the number of vehicles.

VANETs. In [41], Raya et al. propose a scheme to isolate misbehaving nodes until a centralized revocation is issued by the CA. In [42], a scheme is proposed to distribute the load of a server to a set of participating clients. The revocation information is available if up to $k-1$ participants fail. In [43], Wasef et al propose a distributed certificate-service scheme for VANETs. The scheme aims to offer flexible interoperability for certificate service in heterogeneous administrative authorities and reduce the complexity of certificate management.

Capkun et al [44] propose a fully self-organized public-key management system that allows users to generate their public/private key pairs, issue certificates, and perform authentication without any centralized services. Arboit et al [45] present a decentralized certificate revocation scheme that allows the nodes within a mobile ad hoc network to revoke the certificates of malicious nodes. In [46], H. Guo et al. propose a batch authentication protocol for vehicle to smart grid communication. Instead of verifying each packet for each individual vehicle, the aggregator waits for some time to receive multiple responses from a batch of vehicles. The aggregator verifies the received responses by only one signature verification.

In [47], H. Khurana et al. have discussed the main security issues in smart grid. The authors have identified public key management as a challenge due to the system scalability and complexity. From [48], the smart meters will have a remote off switch to ensure that customers who default on their payments can be switched off remotely. However, the attackers can launch attacks to interrupt the citizens' electricity supply. In order to address this attack, the authors use public key cryptography to secure the "turn off" commands. A. Metke et al. [49] survey the existing key security technologies for extremely large, wide-area communication networks. Based on studying the security requirements of the smart grid as well as the scale of the system, the authors strongly believe that the most effective key management solution for securing the smart grid will be based on public key infrastructure.

In [50], M. Qiu et al. measure the energy consumptions of various security algorithms using energy-constrained nodes. They propose a group of code optimization methods to increase the energy consumption efficiency of different security algorithms for smart grid. Chee-Wooi et al. [51] propose a vulnerability assessment framework to systematically evaluate the vulnerabilities of $SCADA$ systems. In [52], a survey on cybersecurity of critical infrastructures is reported. A supervisory control and data acquisition security framework has been proposed. In [53], the authors present a framework for cyber-attack impact analysis of a smart grid. The authors illustrate how cause-effect relationships can be conveniently expressed for both analysis and extension to large-scale smart grid systems.

In [54], the authors investigate the attacks and privacy concerns in the smart grid. They also expect that the public key cryptography will be implemented to secure the smart grid. In [55], the authors highlight the significance of cyber-infrastructure security in conjunction with power application security to prevent, mitigate, and tolerate cyber-attacks. Cheng et al. [56] introduce three main attack categories and their countermeasures in the smart grid communication networks. In [57], [58], privacy-preserving power consumption data aggregation schemes for AMI networks have been proposed. M. Fouda et al. [59] propose a lightweight message authentication scheme for securing smart grid communications. The PKC has been used in several works to secure the AMI networks such as [9]. In [60], X. Liang et al. propose a usage-based dynamic pricing scheme for smart grid in a community environment, which enables the electricity price to correspond to the electricity usage in real time.

However, although securing smart grid has recently gained extensive attention, certificate revocation in smart grid has not been well studied yet. In [11]–[13], we have introduced the problem of certificate revocation in AMI networks. Unlike this work that focuses only on AMI networks, this paper broadens our investigations to include certificate revocation in different applications of the smart grid.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2015.2408597, IEEE Internet of Things Journal

8 CONCLUSIONS AND FUTURE WORK

In this paper, we have investigated certificate revocation in smart grid applications. We have explained different certificate revocation schemes and defined several metrics to assess them. Based on our assessment, we identified the applications that are proper for each scheme and discuss how the schemes can be modified to fully meet the requirements of potential applications. Finally, we studied certificate revocation in pseudonymous public key infrastructure and explained an efficient scheme for vehicles-to-grid communications as a potential application. We have discussed that one revocation scheme cannot satisfy the overhead/security requirements of all smart grid applications. Rather, different schemes should be employed for different applications. This is because the smart grid applications have different security/overhead needs.

In our future work, we will further investigate this idea of partitioned CRLs ($P-CRL$s) and apply it on the AMI networks. A good certificate revocation scheme for AMI networks should balance the size of the CRLs and the overhead of forming and distributing them. It should also take into account the limited storage and computation power of the meters, and address the scalability and the large geographic deployment of the networks and require low communication overhead.

9 ACKNOWLEDGEMENT

This work is supported in part by US National Science Foundation under the grant number 1318872.

REFERENCES

[1] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, "Smart transmission grid: Vision and framework," *Smart Grid, IEEE Transactions on*, vol. 1, no. 2, pp. 168–177, Sept 2010.

[2] S. Amin, "For the good of the grid," *IEEE Power Energy Mag.*, vol. 6, pp. 48–59, 2006.

[3] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power Energy Mag.*, vol. 8, pp. 41–48, 2010.

[4] NIST, "Report to nist on smart grid interoperability standards roadmap epri," *Available [Online]: http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructured.pdf*, June 2009.

[5] M. Mahmoud, J. Misic, and X. Shen, "A scalable public key infrastructure for smart grid communications," *Proc. of IEEE Global Communication Conference (IEEE GLOBECOM'13), Atlanta, GA, USA*, December 2013.

[6] M. Mahmoud and X. Shen, "Esip: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 7, pp. 997–1010, July 2011.

[7] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[8] J. P. Hubaux, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 2, p. 4955, 2004.

[9] A. Beussink, K. Akkaya, I. Senturk, and M. Mahmoud, "Preserving consumer privacy on ieee 802.11s-based smart grid ami networks using data obfuscation," *IEEE INFOCOM Workshop on Communications and Control for Smart Energy Systems*, 2014.

[10] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 375–381, June 2011.

[11] K. Akkaya, K. Rabieh, M. Mahmoud, and S. Tonyali, "Efficient generation and distribution of crls for ieee 802.11s-based smart grid ami networks," *Proc. of IEEE SmartGridComm'14, Italy*, November 2014.

[12] M. Mahmoud, K. Akkaya, K. Rabieh, and S. Tonyali, "An efficient certificate revocation scheme for large-scale ami networks," 2014.

[13] K. Akkaya, K. Rabieh, M. Mahmoud, and S. Tonyali, "Customized certificate revocation lists for ieee 802.11s-based smart grid ami networks," *Smart Grid, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[14] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environments," *Vehicular Technology, IEEE Transactions on*, vol. 55, no. 4, pp. 1373–1384, July 2006.

[15] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "Caravan: providing location privacy for vanet," *Proceedings of International workshop on Vehicular ad hoc networks*, 2006.

[16] V. Balijepalli, V. Pradhan, S. Khaparde, and R. Shereef, "Review of demand response under smart grid paradigm," *IEEE PES Innovative Smart Grid Technologies*, 2011.

[17] C.-J. Tang, M.-R. Dai, C.-C. Chuang, Y.-S. Chiu, and W. Lin, "A load control method for small data centers participating in demand response programs," *Future Generation Computer Systems*, vol. 32, no. 0, pp. 232 – 245, 2014.

[18] A.-H. Mohsenian-Rad, V. W. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *Smart Grid, IEEE Transactions on*, vol. 1, no. 3, pp. 320–331, 2010.

[19] N. Ruiz, I. Cobelo, and J. Oyarzabal, "A direct load control model for virtual power plant management," *Power Systems, IEEE Transactions on*, vol. 24, no. 2, pp. 959–966, 2009.

[20] A. Gomes, C. Antunes, and A. Martins, "A multiple objective approach to direct load control using an interactive evolutionary algorithm," *Power Systems, IEEE Transactions on*, vol. 22, no. 3, pp. 1004–1011, 2007.

[21] H. Liu, H. Ning, Y. Zhang, and L. Yang, "Aggregated-proofs based privacy-preserving authentication for v2g networks in the smart grid," *Smart Grid, IEEE Transactions on*, vol. 3, no. 4, pp. 1722–1733, Dec 2012.

[22] P. Wohlmacher, "Digital certificates: a survey of revocation methods," *Proc. of the ACM Workshops on Multimedia, California*, pp. 111–114, 2000.

[23] P. Kocher, "On certificate revocation and validation," *Proceedings of the 2nd International Conference on Financial Cryptography, Anguilla*, pp. 172–177, 1998.

[24] M. Myer, "Revocation: options and challenges," *Proceedings of the 2nd International Conference on Financial Cryptography, West Indies*, pp. 165–171, Feb 1998.

[25] P. Zheng, "Tradeoffs in certificate revocation schemes," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, pp. 103–112, 2003.

[26] M. Jakobsson and S. Wetzel, "Efficient attribute authentication with applications to ad hoc networks," *in Proceedings of VANET'04*, 2004.

[27] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J. Hubaux, "Certificate revocation in vehicular networks," *Technical Report LCA-Report-2006-006*, 2006.

[28] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile," *Internet Request for Comments (RFC 3280)*, April 2002.

[29] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, *IEEE Std. 1609.2-2006*, 2006.

[30] D. A. Cooper, "A more efficient use of delta-crls," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 190–202, 2000.

[31] A. Wasef, Y. Jiang, and X. Shen, "Dcs: An efficient distributed-certificate-service scheme for vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 2, pp. 533–549, Feb 2010.

[32] Center for Carbon-Free Power Integration [Online], *Available: http://www.carbonfree.udel.edu/*.

[33] J. Haas, Y.-C. Hu, and K. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 595–604, March 2011.

[34] W. Dai, "Crypto++ library 5.6.0," *http://www.cryptopp.com*, last retrieved 2014.

[35] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *Mobile Computing, IEEE Transactions on*, vol. 5, no. 2, pp. 128–143, Feb 2006.

[36] B. Fox and B. LaMacchia, "Online certificate status checking in financial transactions: the case for reissuance," *Financial Cryptography - Lecture Notes in Computer Science*, vol. 1648, pp. 104–117, 1999.

[37] W. Mao, "Modern cryptography: Theory and practice," *Englewood Cliffs, NJ: Prentice-Hall*, 2003.

[38] M. Mahmoud and X. Shen, "Fescim: Fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 5, pp. 753–766, May 2012.

[39] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 8, pp. 1557–1568, Oct 2007.

[40] P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate revocation list distribution in vehicular communication systems," *Proc. 5th ACM Int. Workshop Veh. Inter-NETw.*, pp. 86–87, 2008.

[41] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J. P. Hubaux, "Certificate revocation in vehicular networks," *Swiss Fed. Inst. Technol., Lausanne, Switzerland, Tech. Rep. LCA-Rep.-2006-006*, 2006.

[42] R. Wright, P. Lincoln, and J. Millen, "Efficient fault-tolerant certificate revocation," *Proc. of CCS'00*, 2000.

[43] A. Wasef, Y. Jiang, and X. Shen, "Dcs: An efficient distributed-certificate-service scheme for vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 2, pp. 533–549, Feb 2010.

[44] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *Mobile Computing, IEEE Transactions on*, vol. 2, no. 1, pp. 52–64, Jan 2003.

[45] G. Arboit, C. Crpeau, C. R. Davis, and M. Maheswaran, "A localized certificate revocation scheme for mobile ad hoc networks," *Elsevier Ad Hoc Networks*, vol. 6, no. 1, pp. 17–31, January 2008.

[46] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "Ubapv2g: A unique batch authentication protocol for vehicle-to-grid communications," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 707–714, Dec 2011.

[47] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *IEEE Security and Privacy*, vol. 8, no. 1, pp. 81–85, January-February 2010.

[48] R. Anderson and S. Fuloria, "Who controls the off switch?" in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010, pp. 96–101.

[49] A. Metke and R. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, June 2010.

[50] M. Qiu, W. Gao, M. Chen, J.-W. Niu, and L. Zhang, "Energy efficient security algorithm for power grid wide area monitoring system," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 715–723, Dec 2011.

[51] C. Ten, C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for scada systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, November 2008.

[52] C. Ten, G. Manimaran, and C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, July 2010.

[53] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2010, pp. 244–249.

[54] S. Iyer, "Cyber security for smart grid, cryptography, and privacy," *International Journal of Digital Multimedia Broadcasting*, vol. 2011, 2011.

[55] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan 2012.

[56] P. Chen, S. Cheng, and K. Chen, "Smart attacks in smart grid communication networks," *IEEE Communications Magazine*, August 2012.

[57] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1621–1631, Sept 2012.

[58] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," *Systems Journal, IEEE*, vol. 8, no. 2, pp. 598–607, June 2014.

[59] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675 – 685, December 2011.

[60] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, "Udp: Usage-based dynamic pricing with privacy preservation for smart grid," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 141–150, March 2013.