# An Enhanced Public Key Infrastructure to Secure Smart Grid Wireless Communication Networks

**Daojing He, South China University of Technology and Zhejiang University**
**Sammy Chan, City University of Hong Kong**
**Yan Zhang, Simula Research Laboratory and University of Oslo**
**Mohsen Guizani, Qatar University**
**Chun Chen and Jiajun Bu, Zhejiang University**

## Abstract

It is expected that the smart grid will radically add new functionalities to legacy electrical power systems. However, we believe that this will in turn introduce many new security risks. With the smart grid's backbone communication networks and subnetworks, there are possible scenarios when these subnetworks can become vulnerable to attacks. Ensuring security in these networks is challenging because most devices are resource constrained. In addition, different protocols that are used in these networks use their own set of security requirements. In this article, the security requirements of smart grid communication networks are firstly identified. We then point out that although public key infrastructure (PKI) is a viable solution, it has some difficulties to satisfy the requirements in availability, privacy preservation, and scalability. To complement the functions of PKI, we introduce some novel mechanisms so that those security requirements can be met. In particular, we propose a mechanism to efficiently resist Denial-of-Service (DoS) attacks, and some suggestions to the security protocol design for different application categories.

When the legacy power infrastructure is augmented by a communication infrastructure, it becomes a smart grid. This additional communication infrastructure facilitates the exchange of state and control information among different components of the power infrastructure. As a result, the power grid can operate more reliably and efficiently [1].

Although deploying the smart grid enjoys enormous social, environmental and technical benefits, the incorporation of information and communication technologies into the power infrastructure will introduce many security challenges. For example, it is estimated that the data to be collected by the smart grid will be an order of magnitude more than that of existing electrical power systems. This increase in data collection can possibly introduce security and privacy risks. Moreover, the smart grid will be collecting new types of information that were not recorded in the past, and this can lead to more privacy issues [2–4].

As shown in Fig. 1, an essential part of the smart grid will be its communication networks. This is a three-tier network which connects the different components of the smart grid together, and allows two-way information flow. The first tier connects the transmission system located at the power plant and the control centers of Neighborhood Area Network (NAN). Each NAN comprises a number of Building Area Networks (BANs) and provides them interfaces to the utility's wide-area network. Here, BANs are customer networks and belong to the second tier of the shown system. Each BAN consists of a number of third-tier networks, Home Area Network (HANs). The HAN is a customer premises network which manages the on-demand power requirements of end users. Note that there is no standard definition of these networks yet. Their structures described above feature a practical configuration that can be found in established smart grids.

While different components of the power infrastructure of the smart grid are networked together to exchange information, as illustrated in Fig. 1, there is a potential increase of the security risk of the system. For example, it will increase the complexity of the electrical power grid, which in turn can increase new security vulnerabilities. Also, the number of entry points that can be used to gain access to the electrical power system will increase when all of the components are networked together [1, 3].

In the remainder of this article, we mainly focus on the security of wireless communication subnetworks of the smart grid. Security in wired links can be achieved by existing techniques such as firewalls, virtual private networks, Secure Shell or other higher layer security mechanisms. However, wireless communication networks' security in the smart grid is still considered a big challenge compared to its wired counterpart. Due to their dynamically changing topologies and the open nature of the communication medium, wireless communication networks are vulnerable to attacks that are easier to launch than in the wired domain. In addition, many of the

0890-8044/14/$25.00 © 2014 IEEE

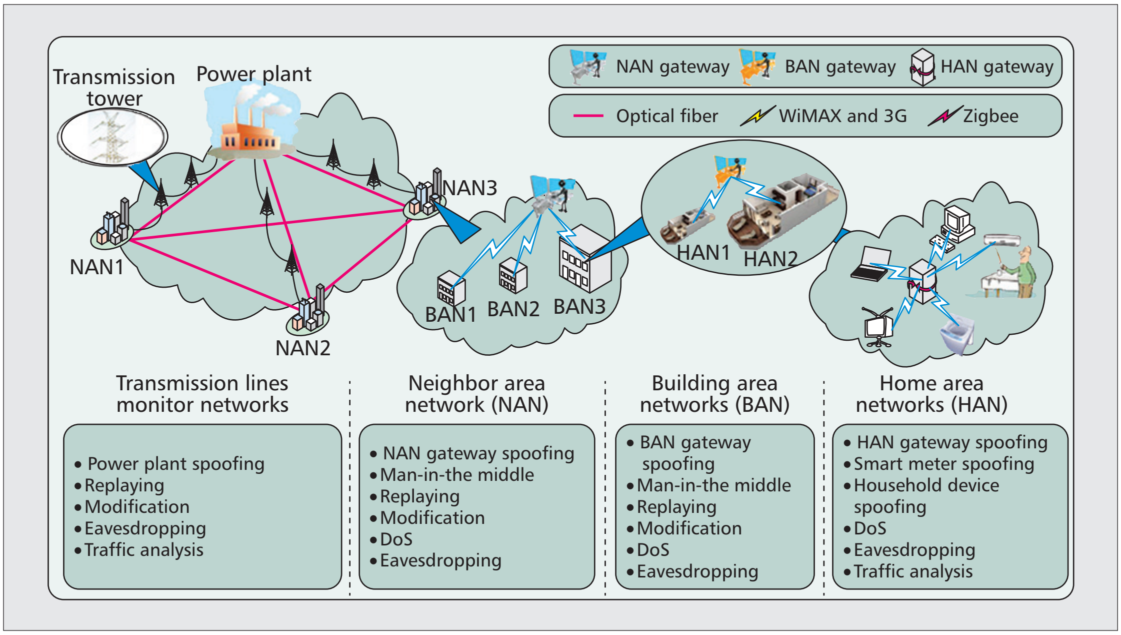

Figure 1. *Considered smart grid communication networks and security threats.*

already used protocols use their own sets of security requirements. Another issue is that legacy devices with constraints (e.g., limited CPU processing power, transmission rate, storage, etc.) are still deployed in the smart grid [2].

In this article, we first identify the requirements to secure smart grid wireless communication networks, and argue that public key infrastructure (PKI) is a promising solution. At the same time, we also point out some limitations of PKI in securing smart grids. We then introduce a set of novel mechanisms to mitigate the limitations of PKI. In particular, since DoS attacks have severe consequences on availability, which is the most important security objective of smart grids, we propose a mechanism to efficiently resist DoS attacks against adversaries and legitimate insiders. Also, some suggestions to the security protocol design for different application categories are presented.

## Securing Smart Grid Communication Networks

Referring again to Fig. 1, the security threats that can be encountered by the smart grid are diverse. They are either passive attacks such as eavesdropping and traffic analysis, or active attacks such as replaying and DoS attacks. Passive attacks attempt to access the information exchanged within a network, while active attacks would disrupt the normal functionality of a network. Essentially, these attacks lead to the most basic security service requirements in the smart grid: availability, efficiency, scalability, entity authentication, data integrity protection, non-repudiation, privacy preservation, and confidentiality. The system-level security requirements are as follows.

**Availability:** Because electricity must always be available, it is important that any security mechanism implemented in the smart grid does not impede power availability or safety. In the network security field, availability means that secure communication service should be available even when there are attacks such as DoS attacks. For example, when a smart meter authenticates other devices or smart meters, the authentication process itself can attract attacks from distributed DoS attackers.

**High efficiency and scalability:** Depending on where the mechanism will be employed, the smart grid has various real-time requirements that rely on high efficiency. Common use of resource-constrained devices and networks add to this need. For example, it is envisioned that wireless sensor networks (WSNs) will also be integrated into the smart grid to optimize different functions of the power infrastructure such as power generation and delivery [5]. These networks have limited bandwidth, and their sensor nodes have limited computation and energy resources. Also, scalability is important due to the large number of devices in the smart grid and the increasing number of interactions between grid entities.

Also, the protocol-level security requirements are as follows.

**Entity authentication and data integrity protection:** Entity authentication ensures that the communicating entities are legitimate, while integrity protection ensures that received data has not been altered during transmission and is not replayed data. In particular, in NANs, once this requirement is met, some attacks such as NAN gateway spoofing, replay and modification attacks can be resisted.

**Non-repudiation:** This is to prevent legitimate entities from denying the transmission of their messages and the corresponding contents. When there are third-party service providers in smart grids, non-repudiation must be satisfied in order to prevent someone from denying a particular action that he has done, e.g., making subscription to a certain service.

**Privacy preservation:** The data that the smart grid is collecting and generating has raised three different privacy-related issues.

- Conditional identity privacy preservation: Smart grid consumers will expect certain level of anonymity relative to what they have with the existing electrical power grid. At the same time, the smart grid is such a critical structure that in some cases complete anonymity may not be desirable. Law authority (e.g., local police offices) will need to be able to track consumers who attack the smart grid, but it should not be easy for any other parties to break the data anonymity. An example of conditional privacy preservation is a concealment of the identity information of a smart meter (e.g., the owner's name, the address, etc.).

- Complete identity privacy preservation: Much of the data in the smart grid does not need to be attributed to a specific sender (e.g., a specific consumer). In this case, data should be sent anonymously without violating data integrity constraints. In other words, anyone other than the sender, including the insider of trust authority (or law authority), should not be able

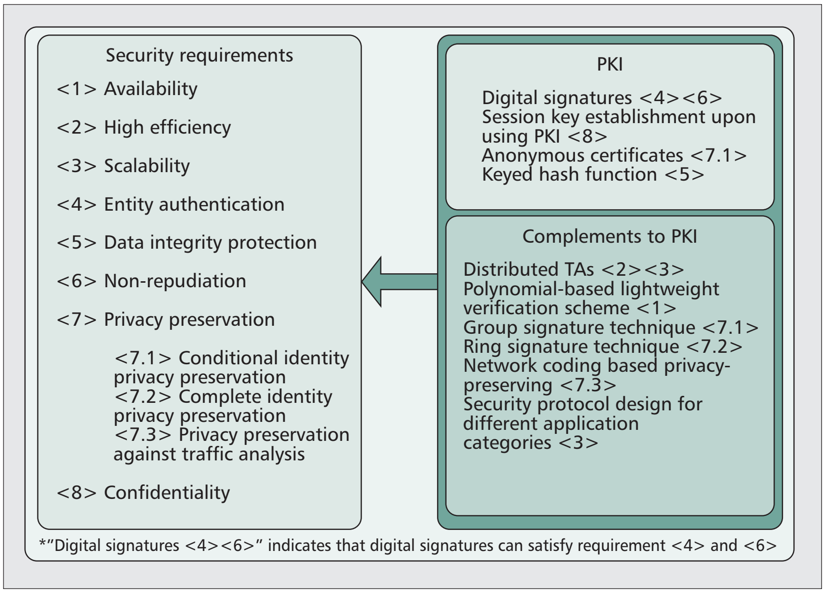
Security requirements
<1> Availability
<2> High efficiency
<3> Scalability
<4> Entity authentication
<5> Data integrity protection
<6> Non-repudiation
<7> Privacy preservation
<7.1> Conditional identity privacy preservation
<7.2> Complete identity privacy preservation
<7.3> Privacy preservation against traffic analysis
<8> Confidentiality
PKI
Digital signatures <4><6>
Session key establishment upon using PKI <8>
Anonymous certificates <7.1>
Keyed hash function <5>
Complements to PKI
Distributed TAs <2><3>
Polynomial-based lightweight verification scheme <1>
Group signature technique <7.1>
Ring signature technique <7.2>
Network coding based privacy-preserving <7.3>
Security protocol design for different application categories <3>
*"Digital signatures <4><6>" indicates that digital signatures can satisfy requirement <4> and <6>

Figure 2. *Security requirements of smart grid communication networks, public key infrastructure and the proposed mechanisms.*

to identify the sender of a message, or link different messages belonging to the same sender even though the sender is unknown.

**Privacy preservation against traffic analysis:** Some advanced attacks, e.g., traffic analysis and flow tracing [6], can compromise the privacy of consumers, violating source anonymity and traffic secrecy. Privacy preservation via general data encryption mainly focuses on how to encrypt a communication message. In contrast, traffic analysis is the process of examining the characteristics of network traffic, such as message length, frequency or other patterns, to extract useful information. Therefore, even if operational information were encrypted, traffic analysis could provide an adversary enough information on the operational situation to enable more sophisticated timing of physical or cyber attacks.

**Confidentiality:** Data encryption protects the sensitive transmitted data from passive attacks, such as eavesdropping.

Clearly, the protocol-level security objectives depend on which components are communicating, and what data they are exchanging.

### Employing PKI to Secure Smart Grid Communication

In this subsection, we argue that PKI is a potential mechanism for securing smart grid communication as it can meet most security requirements of smart grid communication networks.

As shown in Fig. 2, security requirements of entity authentication and non-repudiation can be satisfied by employing digital signatures. A PKI binds the public keys and the entities' identities through the use of digital certificates. The binding is established through a registration process, and after a trust authority (TA) (consisting of the registration authority, certificate authority and validation authority) assures the correctness of the binding, the TA issues the certificate to the entity. Since the public key of each entity is made available to all other entities in the network, entity authentication can be achieved. The simplest form of a certificate consists of the following contents: $Cert_j = \{id_j, PK_j, Exp_T, \{SIG_{SK_{TA}}\{h(id_j||PK_j||ExpT)\}\}$, where $id_j$ denotes entity $j$'s identity, $PK_j$ represents the public key of entity $j$, $ExpT$ denotes certificate expiry time, $SK_{TA}$ denotes the private key of TA and $SIG_{SK_{TA}}\{h(id_j||PK_j||ExpT)\}$ is a signature over $h(id_j||PK_j||ExpT)$ based on $SK_{TA}$. Here, $h(.)$ indicates hash function operation. Thus, any entity can sign any outgoing message using its unique private key. An outgoing message is then transmitted as $\{\mathcal{M}, SIG_{SK_j}\{h(id_j||\mathcal{M})\}, Cert_j\}$, where $\mathcal{M}$ denotes the outgoing message and $SK_j$ denotes the private key of entity $j$. Of course, timestamps should be included in $\mathcal{M}$ to prevent the replay attack. When it is received, the receiver verifies the signature of the sender using its public key. Upon successful verification, the identity of the sender is confirmed and it can also be concluded that the message content has not been altered. In other words, entity authentication and non-repudiation are achieved. In addition, conditional privacy can be preserved using anonymous certificates, as they do not contain the identity information of their holders. In this case, when necessary, the identity of the holder of an anonymous certificate can only be revealed by a TA.

Because public key operations are considerably slower than the symmetric algorithm, session keys will be used to provide confidentiality for the bulk exchange of messages while public key cryptography is used to secure and distribute session keys. In order to provide data integrity protection, a keyed hash function should be used. That is, $\mathcal{M} = \{data, h(data, K)\}$, where $data$ is the transmitted data item by entity $i$ while $h(data, K)$ denotes the keyed hash function with a session key $K$ for $data$. Subsequently, entity $i$ delivers $\{\mathcal{M}, SIG_{SK_j}\{h(id_i||\mathcal{M})\}, Cert_i$ to another entity, say $j$. Upon receiving such a packet, entity $j$ checks the validity of $h(data, K)$. If the result is positive, entity $j$ believes this message is not altered; otherwise, entity $j$ simply drops the packet.

In very large systems, PKI could be significantly more efficient than shared keys in terms of setting up and maintaining operational credential. This is due to the fact that each entity is only configured with its own certificate. On the other hand, when symmetric key is used, a unique key pair needs to be configured between every pair of entities. This makes key management complicated since many symmetric keys need to be maintained and the decrypting entity may not know in advance which key should be used.

In the smart grid, most devices are capable of asymmetric cryptographic operations, e.g, signature verification. We consider WSNs in smart grids as an example. Even the resource-limited sensor nodes can perform a certain number of such operations, given their large energy consumptions. To accurately measure the consumed energy of various cryptographic operations considered in this article, a circuit connecting a 3 V battery (but measured to be 3.16 V), a mote and a 20.36 Ω resistor in series has been built. Other voltage and resistance values can also be used as long as the mote is in its normal operating region. When the mote is executing a certain cryptographic operation, voltage $V_r$ across the 20.36 Ω resistor is measured by a Tektronix TDS 2012B oscilloscope. From $V_r$, the current through the circuit $I$ and the voltage across the mote $V_m$ can be obtained. At the same time, we also measure the execution time $t_o$ of the operation. Then, the consumed energy of the operation at the mote is given by $V_m \times \mathrm{I} \times t_o$. The sensor nodes used in our experiments are MicaZ and TelosB motes. The MicaZ mote is based on an 8-bit, 8 MHz Atmel microcontroller, and has 4KB RAM and 128KB ROM. For the TelosB mote, it is based on a 16-bit, 4 MHz MSP430 microcontroller, and has 10KB RAM and 48KB ROM. For each experiment on motes to be presented below, it was repeated one thousand times to obtain average values of measurements. The computational power and memory size of

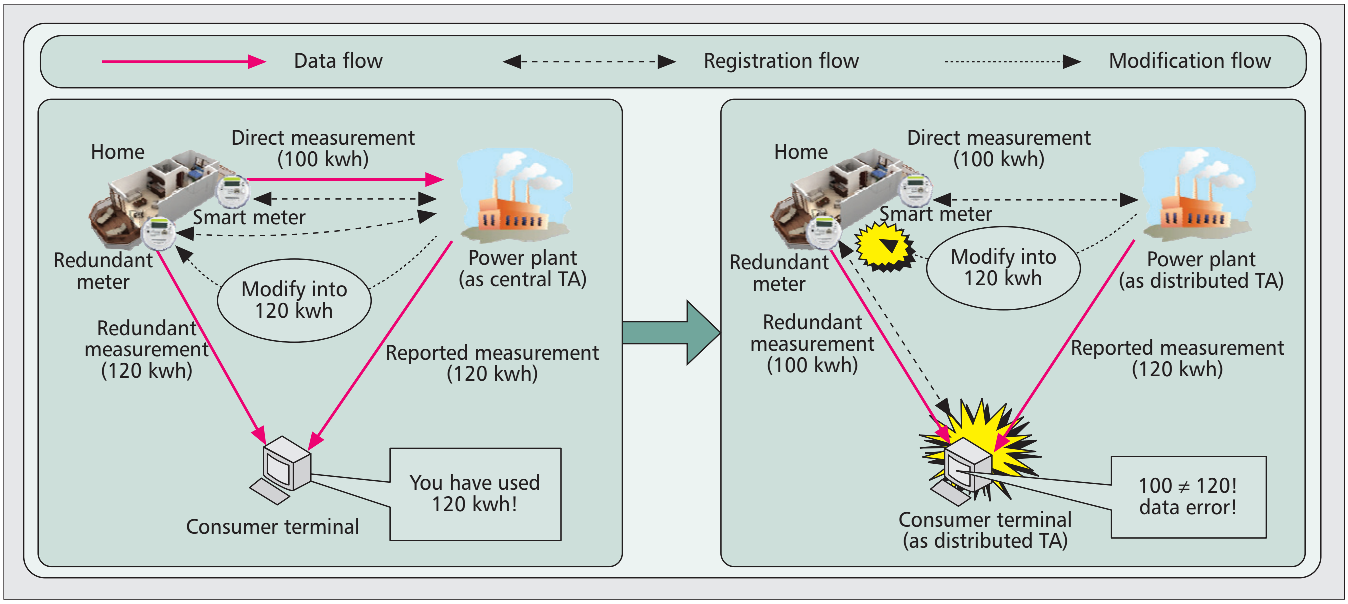
Data flow
Registration flow
Modification flow
Home
Direct measurement (100 kwh)
Smart meter
Redundant meter
Modify into 120 kwh
Power plant (as central TA)
Redundant measurement (120 kwh)
Reported measurement (120 kwh)
Consumer terminal
You have used 120 kwh!
Home
Direct measurement (100 kwh)
Smart meter
Redundant meter
Modify into 120 kwh
Power plant (as distributed TA)
Redundant measurement (100 kwh)
Reported measurement (120 kwh)
Consumer terminal (as distributed TA)
100 ≠ 120! data error!

Figure 3. *Smart meter and redundant meter reading.*

these motes are comparable to that of a smart meter functioning as a HAN gateway. Thus, besides WSNs in a smart grid, experimental results on TelosB and MicaZ motes are also applicable for those smart meters in a smart grid.

In the first experiment, we implement the 160-bit Elliptic Curve Cryptography (ECC) algorithm of TinyECC library [7] in MicaZ and TelosB motes. The signature generation times are measured to be 2.002 and 3.169 seconds, respectively. Also, the signature verification times are measured to be 2.436 and 4.039 seconds, respectively. The energy consumptions for the signature generation are 48.04 mJ and 17.11 mJ, and that for the signature verification are 58.48 mJ and 21.82 mJ for MicaZ and TelosB motes, respectively. Thus, these energy consumptions are regarded as acceptable under normal operation (without DoS attacks).

## Shortcomings of Existing PKI for Use in the Smart Grid

Although PKI is a potential solution to secure the smart grid when compared with other approaches, it has some limitations. We first describe the PKI system-level limitations as follows.

*Availability* — In smart grid PKI, authentication on each entity consists of two steps: certificate verification and signature verification. This procedure is vulnerable to DoS attacks, because the expensive operation of scalar multiplication is involved. An adversary may keep sending fake certificate and signature to legitimate entities for preventing others from connecting to them. For example, when a smart meter authenticates other devices or smart meters, the authentication process itself can attract attacks from distributed DoS attackers. Accordingly, a mechanism for preventing DoS attacks is needed to overcome this PKI limitation.

*Distributed TAs* — In the PKI, another challenge is that access (e.g., register and authenticate) to a central server (i.e., the sole TA) is not ideal, so it will need to be distributed. Moreover, the smart grid entities may belong to different organizations and, possibly, have conflicting interests. For example, in 2009, thousands of customers from Pacific Gas and Electricity (PG&E) of California complained that their smart meters overcharged them [8]. Consequently, some PG&E customers installed redundant meters to verify the integrity of their bills independently. Obviously, different from the primary smart meters, the redundant meters should be authorized by the consumers, but not the supplier. Thus, the management policy in PKI should be further explored from a sole TA to distributed TAs. As illustrated in Fig. 3, in the central TA approach, the keying materials of primary smart meters and redundant meters are distributed by the electric utility. Thus, the electric utility can modify the measurement reading of redundant meters, which cannot be detected by the consumer and lead to incorrect billings. However, in the distributed TAs approach, a primary smart meter registers to the electric utility while a redundant meter registers to a consumer. Thus, the electric utility has no ability to access the measurement reading of a redundant smart meter.

*Scalability* — The smart grid is a large system made up of many types of devices with different computational power, and different communication protocols with their own sets of security requirements. One major obstacle to provide secure communication in such a system is to ensure that the security mechanisms can be implemented in all devices, and satisfy the security requirements. Therefore, PKI should be enhanced to accommodate the different devices and security needs. The PKI also has the following protocol-level limitation.

*Privacy Preservation* — In order to provide identity privacy protection, an entity needs to frequently change its one-time anonymous certificate, thus each entity possesses a number of certificates. Clearly, this solution is not suitable for smart grid because preloading a large pool of certificates is not feasible for memory-limited entities (e.g., smart meters and sensor nodes). Furthermore, even though anonymous certificates in PKI can guarantee conditional identity privacy, PKI cannot support complete identity privacy preservation and privacy preservation against traffic analysis.

## Resisting DoS Attacks Against Adversaries and Legitimate Insiders

DoS attacks have severe consequences on availability, which is the most important security requirement of the smart gird communication network. Inspired by the work in [9], we propose the following lightweight polynomial-based verification mechanism to defend against DoS attacks.

|  | TelosB mote |  |  | 800MHz Processor |  |  | 1.6GHz Processor |  |  | 2.4GHz Processor |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | $t = 50$ | $t = 100$ | $t = 200$ | $t = 100$ | $t = 500$ | $t = 1000$ | $t = 100$ | $t = 500$ | $t = 1000$ | $t = 100$ | $t = 500$ | $t = 1000$ |
| Time (ms) | 8.23 | 16.39 | 33.48 | 0.333 | 1.645 | 3.265 | 0.148 | 0.799 | 1.623 | 0.102 | 0.517 | 1.075 |

Table 1. *Timings for evaluating a* t*-degree polynomial.*

We require that in the registration phase, the TA of each entity group randomly generates a bivariate $t$-degree polynomial $f(x, y) = \sum_{i,j=0}^{t} a_{ij}x^iy^j$ over a finite field $F_p$, with $p$ being a large prime number. Note that $f(x, y) = f(y, x)$. When entity $i$, with identity $id_i$, registers to the TA, the TA computes a polynomial share of $f(x, y, f(id_i, y)$, and then delivers it to $i$ by any secure transmission protocol (e.g., SSL). When $i$ wants to communicate with another entity, say $j$ with identity $id_j$, it evaluates $f(id_i, y)$ at point $id_j$ to obtain the common key $f(id_i, id_j)$. Similarly, $j$ can evaluate f$id_j$,y) at point $id_i$ to obtain the same key since $f(id_j, id_i) = f(id_i, id_j)$. Then, $j$ can verify the legitimacy of $i$ by using $f(id_j, id_i)$.

Table 1 gives the time of evaluating a $t$-degree polynomial in a TelosB mote and a laptop PC for different $t$. The computation involves $2t$ modular multiplications and $t$ modular additions over $F_p$, where $p$ is chosen to be 64 bits long in our implementation. Such a key length is considered to be sufficiently secure for now and immediate future. For example, the execution time on a TelosB mote is 8.23 ms when $t = 50$, which is much faster than that of signature verification based on ECC. Thus, entity $j$ can efficiently verify the legitimacy of entity $i$ before performing expensive verification on the certificate and the signature to mitigate the DoS attacks. Note that our approach would not impose much computational burden on a legitimate entity since it already knows the communication key of the other entity. However, the situation is opposite for an adversary. It needs to guess the correct communication key first in order to generate a valid connection request. Therefore, our approach can effectively mitigate DoS attacks even in the presence of powerful adversaries. In addition, our approach is unconditionally secure and $t$-collusion resistant, which means that the secret polynomial function $f$ is disclosed only when there are $t + 1$ compromised entities. Moreover, the proposed lightweight verification approach can resist DoS attacks against legitimate insiders, because any entity can identify which particular entity launched the attacks by the lightweight verification. Next, we investigate the energy consumption in a TelosB mote when it evaluates a $t$-degree polynomial. The resistor's voltage is 352 mV, the current is 17.2888 mA, hence the power consumption is 48.5469 mW. For a 50-degree polynomial, the energy consumption is 0.3995 mJ. Thus, evaluating a $t$-degree polynomial consumes much less energy on TelosB motes than signature generation (or verification).

Based on this scheme, PKI is modified as follows. In the *beacon messages*, a LIGHTWEIGHT VERIFICATION flag is added. If entity $j$ is under attack (e.g., when it notices that the rate of incoming connection requests exceeds a pre-defined threshold), it sets the LIGHTWEIGHT VERIFICATION flag to "TRUE," and adds the identity $id_j$ and a timestamp $t$ into the beacon messages, which are periodically broadcast to announce the service. An entity, say $i$, generates $K = f(id_i, id_j)$ and the corresponding authentication code $Aut = h(K||T||\mathcal{M})$, where $T$ is a timestamp used to resist the replay attack. Finally, entity $i$ sends $Aut$ and $\mathcal{M}$, $SIG_{SK_i}\{\{h(id_i||\mathcal{M})\}, Cert_i\}$ to entity $j$. After receiving the connection request message, $j$ generates a verification code $Ver = h(K^*||T||\mathcal{M})$ and compares it with $Aut$, where $K^* = f(id_j, id_i)$. Entity $j$ performs the expensive operations of verifying the certificate and signature only if $Ver = Aut$.

This scheme is applicable to various subsystems in the smart grid. For example, in a HAN, the administrator is responsible to generate a bivariate t-degree polynomial and securely assign a polynomial share for each communication device of the HAN. Then, any two devices can be mutually authenticated and, more importantly, DoS attacks against the HAN can be resisted.

## Supporting Distributed TAs and Privacy Preservation

From the above discussions (as shown in Fig. 2), we observe that besides PKI, additional security mechanisms supporting distributed TAs and privacy preservation are required to efficiently secure wireless communication networks for the smart grid. These mechanisms are described in details as follows.

### Distributed TAs

All smart grid entities should be divided into groups. The entities in the same group have the same TA. PKI allows for a chain of trust, where the TA (called the root TA) gives an entity (called the second-level TA) a TA-certificate, which specifies the privilege and public key of the entity. Thus, a second-level TA has the capability to act as the TA of the same group. Also, for efficiency and scalability consideration, the entities in a group can be further divided into multiple sub-groups. Similarly, the entities in the same subgroup have the same responsible TA. Each TA is responsible for maintaining (e.g., distributing and updating) public key certificates for its group members. For example, in Fig. 1, the root TA (e.g., the power plant or the local police office) distributes a TA-certificate to the control center of each NAN. Similarly, as the second-level TA, the control center of a BAN (respectively, a NAN) distributed a TA-certificate to each HAN gateway (respectively, the control center of each BAN). Distributed TAs eliminates single point failures and relieves the performance bottleneck of a single TA in the traditional PKI. Another example is that, referring to Fig. 3, each consumer hopes to act as the TA for the redundant smart meters of his/her residency.

### Privacy Preservation

**Conditional identity privacy preservation:** To resolve the efficiency problem of one-time anonymous certificate described earlier, we have proposed achieving conditional identity privacy preservation by using a group signature technique [10], where an entity signs an outgoing message and then transmits the message with the signature to another entity through a group signature algorithm. In a group signature scheme, any member of the group can sign a message. The receiver of the message can only verify if the message is generated by a group member. Meanwhile, only the group manager can open a group signature to unambiguously reveal the identity of the signer. Thus, different from the anonymous certificate method, only the group public key needs to be preloaded into each entity. So, the proposed method is applicable to storage-constrained entities.

**Complete identity privacy preservation:** A ring signature technique can be used to achieve complete user identity pri-

| Application Category | The relationship among security requirements | Sender | Sender Resource | Receiver | Receiver Resource | Communication Technologies |
|---|---|---|---|---|---|---|
| Wide Area Protection | availability > integrity > confidentiality | sensor node or PMU | limited or moderate | control center/ substation | sufficient | Zigbee/WiMAX |
| Demand-Response | non-repudiation = integrity > confidentiality > availability | control center or NAN/BAN/ HAN gateways | sufficient | home appliance | limited | WiMAX/3G |
| Operation and Control | availability > integrity > confidentiality | control center | sufficient | field device | limited and moderate | WiMAX/3G/ WLAN |
| In-Substation Protection | availability > integrity > confidentiality | protective relay | limited and moderate | circuit breaker | limited | WLAN |
| Smart Meter Data Collection | Integrity = Privacy preservation = confidentiality > availability | home devices | limited | smart meter | limited and moderate | Zigbee |

Table 2. *A summary of the constraints and opportunities of security protocols in smart grid.*

vacy preservation. Suppose that with the use of PKI, the entities in a group have public/private key pairs (PK1, SK1), (PK2, SK2), …, (PKn, SKn). Entity i can compute a ring signature s on an outgoing message m, on input (m, SKi,PK1,…, PKn), and then transmits {m, s} to another entity. Anyone can check the validity of a ring signature given m, s, and the public keys involved, PK1, …, PKn. Similar to group signature, ring signature protects the anonymity of a signer since the receiver of a message can only verify if the message is signed by a member of a ring. However, it is impossible to revoke signer anonymity in ring signature. At the same time, the proposed approach does not violate data integrity constraints.

**Privacy preservation against traffic analysis:** The scheme proposed in [6] can be used to defend against traffic analysis in multi-hop wireless networks. Based on homomorphic encryption on global encoding vectors, it can achieve packet flow untraceability and message content confidentiality.

Here, we consider a smart meter as an example to illustrate how these techniques are actually used to preserve privacy. Smart metering is necessarily privacy invasive and a balance needs to be struck between privacy and the social utility of fine-grained billing. For billing purpose, the metering data are typically collected on a monthly or quarterly basis, and should be attributable i.e., securely associated with a particular account holder with a utility. In this case, the group signature technique can be employed, where the utility is the group manager while each smart meter acts as a group member. Each meter can sign the metering data so that a verifier can only check if the data is originated from the group. Only the utility can identify which meter (i.e., which consumer) a signed metering data is from. On the other hand, for the control of power generation and distribution network, it is not necessary for metering data to be attributable. Instead, data can remain anonymous as long as it can be authenticated and securely associated with a particular entity, e.g., a substation. In this case, the ring signature technique can be used, where each meter can use its private key and the public keys of the other meters of the same substation to sign the metering data and then transmit the signed message to the utility. Anyone including the utility only knows that the message is signed by a meter associated with the substation, but does not need to know the identity of the signer. Moreover, in all cases, the communication from each smart meter to the utility can be strengthened with the network coding technique in order to ensure privacy preservation against traffic analysis.

## Supporting Scalability

In order to complement the scalability provided by PKI, we provide some suggestions to the security protocol design for different application categories.

As shown in Fig. 1, the smart grid will have many different communication protocols, and each of them will have their own sets of protocol-level security requirements (i.e., entity authentication, data integrity protection, non-repudiation, privacy preservation, and confidentiality), sender and receiver resources, and communication technologies (e.g., optical fiber, WiMAX, 3G, Zigbee). Note that the stronger the security algorithm is, the more resource consumption on the CPU, bandwidth and storage. Thus, as listed in Table 2, as with any large-scale system, the security protocols to specific applications should carefully consider these constraints and requirements. This is especially true regarding the grid's ongoing modernization. Here, as examples, we compare different approaches to provide data confidentiality, and study the design considerations for wide area protection protocols.

RC5, Data Encryption Standard (DES), Triple-DES (i.e., 3DES) and Advanced Encryption Standard (AES) are all symmetric-key encryption/decryption algorithms. It is commonly known that AES is more efficient than all other algorithms for the same security level. In addition, hardware AES acceleration is available in many hardware platforms in the smart grid. Thus, AES is the preferred solution.

Additionally, the performance of RC5 and AES algorithms on sensor nodes is investigated. To this end, the RC5 implementation in the TinySEC library for TinyOS 1.x is ported to TinyOS 2.x. For AES, its encryption module is implemented in one of the most commonly used radios, CC2420, which supports hardware AES acceleration. The maximum length of packet payload is set to be 200 bytes. RC5 is used with 12 rounds (with a 64-bit key and 64-bit block size) while a stand-alone AES module is used with 10 rounds (with a 128-bit key and 128-bit block size). Table 3 shows the execution time of RC5 (encryption and decryption) and hardware-based AES encryption in MicaZ and TelosB motes, respectively. Clearly, hardware-based AES encryption is much faster than the RC5 operation.

Cascaded failures can be prevented by recently developed wide area protection protocols. For these protocols, system parameters such as current and voltage are measured by phasor measurement units (PMUs) or WSNs and then transmitted to the control center or substation. The most important security objective of the wide area protection is availability. The electrical power system must be available at all times, so the wide area

| | RC5-64 | | | | | | AES-128 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | TelosB | | | MicaZ | | | TelosB | | | MicaZ | | |
| Plaintext length (bytes) | 16 | 32 | 48 | 16 | 32 | 48 | 16 | 32 | 48 | 16 | 32 | 48 |
| Encryption time (ms) | 2.576 | 5.141 | 7.708 | 1.849 | 3.708 | 5.567 | 0.116 | 0.195 | 0.278 | 0.043 | 0.074 | 0.108 |
| Decryption time (ms) | 2.604 | 5.180 | 7.747 | 1.864 | 3.703 | 5.554 | — | — | — | — | — | — |

Table 3. *The execution time of RC5 and hardware AES for MicaZ and TelosB motes with the plaintext of different lengths.*

protection monitoring the power system must also be always available. The data integrity of the wide area protection is the next important security objective. It will not be able to make correct decisions if it is given false data as input. Confidentiality is the least important security objective. The wide area protection needs to run in real time, and that means the system must have minimal overhead. Implementing confidentiality may be too time-consuming to meet latency requirements. According to the above analysis, the proposed polynomial-based lightweight verification scheme should be employed in a wide area protection system to mitigating the effect of DoS attacks.

## Conclusion and Future Research

In this article, we have addressed security and privacy issues in smart grid wireless communication networks. Several security mechanisms have been proposed to complement the PKI security services for availability, privacy preservation and scalability. Moreover, we have proposed a mechanism to efficiently resist DoS attacks against adversaries and legitimate insiders. We believe that it can be used as a reference for the research on smart grid security and privacy. For example, when designing a security protocol for a specific application, the designers could check whether the security requirements concluded by this article have been satisfied.

Deploying PKI requires manpower from the electric utility to maintain the PKI servers, handles entity software issues and manages the network infrastructure. Thus, it will require a considerable number of staff to maintain the PKI environment with a large number (e.g., several millions) of network entities. Future research should consider how to simplify the PKI environment so that less staff are required to manage it. On the other hand, with the development of the smart grid, more third-party service providers will be involved, which will introduce some new security and privacy risks into the system. We recommend that future research should focus on how to complement the enhanced PKI system to prevent these risks.

### Acknowledgment

This research is partially supported by the European Commission FP7 Project EVANS (grant no. 2010-269323), SmartGrids ERA-Net project PRO-NET funded through Research Council of Norway (project 217006), a strategic research grant from City University of Hong Kong [Project No. 7004054], the Fundamental Research Funds for the Central Universities, and the Specialized Research Fund for the Doctoral Program of Higher Education.

### References

[1] Y.-J. Kim *et al.*, "A Secure Decentralized Data-Centric Information Infrastructure for Smart Grid," *IEEE Commun. Mag.*, vol. 48, no. 11, 2010, pp. 58–65.

[2] T. Baumeister, "Literature Review on Smart Grid Cyber Security," Technical Report, University of Hawaii, 2010.

[3] J. Liu *et al.*, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, 2012, pp. 981–97.

[4] E.-K. Lee, M. Gerla, and S.Y. Oh, "Physical Layer Security in Wireless Smart Grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46-52, Aug. 2012.

[5] V.C. Gungor, B. Lu, and G.P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, Oct. 2010, pp. 3557–64.

[6] Y. Fan *et al.*, "Network Coding based Privacy Preservation Against Traffic Analysis in Multi-Hop Wireless Networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, 2011, pp. 834–43.

[7] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," *Proc. IPSN*, 2008, pp. 245–56.

[8] D. P. Varodayan and G.X. Gao, "Redundant Metering for Integrity with Information-Theoretic Confidentiality," *Proc. IEEE SmartGridComm*, Oct. 2010, pp. 345–49.

[9] C. Blundo, *et al.*, "Perfectly-Secure Key Distribution for Dynamic Conferences," *Advances in Cryptology-Crypto'92*, LNCS 740, 1993, pp. 471–86.

[10] D. He *et al.*, "Privacy-Preserving Universal Authentication Protocol for Wireless Communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, 2011, pp. 431–36.

### Biographies

DAOJING HE [S'07, M'13] (hedaojinghit@gmail.com) received the B.Eng.(2007) and M. Eng. (2009) degrees from Harbin Institute of Technology (China) and the Ph.D. degree (2012) from Zhejiang University (China), all in Computer Science. He is an associate professor in the School of Computer Science and Engineering, South China University of Technology, P.R. China. His research interests include network and systems security. He is an Associate Editor or on the editorial board of some international journals such as *IEEE Communications Magazine, Springer Journal of Wireless Networks, Wiley's Wireless Communications and Mobile Computing Journal, Wiley's Security and Communication Networks Journal*, and *KSII Transactions on Internet and Information Systems.*

SAMMY CHAN [S'87, M'89] (eeschan@cityu.edu.hk) received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. He is an associate professor in the Department of Electronic Engineering, City University of Hong Kong.

YAN ZHANG (yanzhang@ieee.org) received a Ph.D. degree from Nanyang Technological University, Singapore. He is working with Simula Research Laboratory, Norway; and he is an adjunct Associate Professor at the University of Oslo, Norway. His research interests include resource, mobility, spectrum, energy, and data management in communication networks.

MOHSEN GUIZANI [S'85, M'89, SM'99, F'09] is currently a Professor and the Associate Vice President for Graduate Studies at Qatar University, Qatar. He received his B.S. (with distinction) and M.S. degrees in Electrical Engineering; M.S. and Ph.D. degrees in Computer Engineering in 1984, 1986, 1987, and 1990, respectively, from Syracuse University, Syracuse, New York. His research interests include Computer Networks, Wireless Communications and Mobile Computing, and Optical Networking. He currently serves on the editorial boards of six technical Journals and the Founder and EIC of "Wireless Communications and Mobile Computing" Journal published by John Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is an IEEE Fellow and a Senior member of ACM.

CHUN CHEN received the bachelor degree in mathematics from Xiamen University, China, in 1981, and the masters and Ph.D. degrees in computer science from Zhejiang University, China, in 1984 and 1990, respectively. He is a professor in the College of Computer Science, and the director of the Institute of Computer Software at Zhejiang University. His research activity is in image processing, computer vision, and embedded system.

JIAJUN BU received the B.S. and Ph.D. degrees in computer science from Zhejiang University, China, in 1995 and 2000, respectively. He is currently a professor in the College of Computer Science at Zhejiang University. His research interests include embedded system, mobile multimedia, and data mining.