A Lightweight Authentication Protocol in Smart Grid

Debsmita Ghosh, Celia Li, Cungang Yang
(Corresponding author: Cungang Yang)
Department of Electrical and Computer Engineering, Ryerson University
350 Victoria St, Toronto, ON M5B 2K3, Canada
(Email: cungang@ee.ryerson.ca)
(Received Oct. 16, 2016; revised and accepted Feb. 21 & June 5, 2017)

Abstract

Smart grids allow automated meter readings and facilitate two-way communications between the smart meters and utility control centers. As the smart grid becomes more intelligent, it becomes increasingly vulnerable to cyber-attacks. Smart grid security mainly focuses on mutual authentication and key management techniques. An impeding factor in grid security is the memory and processing constraints of the smart meters. The aim of this paper is to propose a lightweight mutual authentication protocol between a residential smart meter and a gateway. The authentication protocol provides source authentication, data integrity, message confidentiality, and non-repudiation. The security analysis renders this protocol robust against several attacks. Its performance analysis provides meticulous results as to how the proposed protocol is efficient in terms of computation overhead, average delay and buffer occupancy at the gateway.

Keywords: Authentication Protocol; Key Management; Smart Grid

1 Introduction

The coexistence of the intelligent devices and the traditional power grid is termed as smart grid technology. Smart grid follows a distributed mode of control over the power system, as opposed to the centralized approach adopted by the traditional grid. The traditional power grid allows one-way electricity flow from a few power plants towards a large customer base. The NIST 3.0 framework, released in October 2014, mentions that the smart grid is the inclusion of communication and information technologies to the traditional power grid, and enabling duplex communication between smart meters and utility control centers [26]. If an active adversary is successful in obtaining and manipulating the meter readings, he may alter the readings to reflect incorrect usage. If this happens on a large-scale, it will significantly hamper the restricted energy resources and the economy as well.

A passive adversary, on the other hand, may collect reports for a long duration of time for a specific house. By analyzing the meter readings, the attacker will be able to understand the number of occupants in the house, the time at which the house is empty or the occupants are asleep, and other information describing the activity occurring inside the house. The attacker may use this information to launch an attack on the house. Hence, meter readings are extremely sensitive and must be protected. A limiting factor is the memory and processor capabilities of the smart meter device. For instance, a Home Area Network (HAN) smart meter configuration may comprise of MSP430-F4270 microcontroller along with 128 KB of flash and RAM memory [14]. Efficient protocols and mutual authentication schemes are already in use in the smart grid industry, but they also incur additional overhead. A few instances that increase overhead are long key sizes, ciphers and certificates, maintenance of Public Key Infrastructure (PKI), keeping track of Certificate Revocation Lists and timers. Furthermore, as the grid becomes smarter, it becomes increasingly vulnerable to software attacks. Smart meter devices depend on communication protocols such as TCP/IP, HTTP and FTP to exchange data. By default, these protocols do not have security built into them [3]. These conditions highlight the need for a lightweight authentication protocol between smart meters.

2 Related Work

Extensive research is being conducted in devising lightweight approaches using techniques such as Diffie-Hellman, ECC-based cryptography and ID-based cryptography. H. So proposes a zero-configuration signcryption protocol to ensure safe and secure communications between two ends [29]. The communication overhead for encryption and signature schemes of the protocol increases with the degree of encryption. Also, the security

level of the signature is directly proportional to the degree of encryption. The advantage of this protocol is it doesn't use asymmetric key algorithms. This protocol assures key protection but it is too expensive, keeping in mind that several smart meters generate packets every 15 minutes.

Nicanfar *et al.* proposes a mutual authentication scheme between a HAN smart meter and an authentication server [25]. They use Secure Remote Password protocol (SRP) and decrease the number of steps in SRP from five to three. The proposed protocol also reduces the number of exchanges from four to three. It is essentially based upon Enhanced ID-based Cryptography (EIBC). EIBC essentially uses True Random Number Generator and Pseudorandom Number Generator to keep changing the secret master key, along with the public/private keys of the meters. The paper is robust against several attacks. Also, the key renewal mechanism is efficient in terms of refreshing the public/private and multicast keys. However, it requires synchronization of three timers between the smart meter and authentication server. This adds to the overhead of the protocol. Also, as mentioned previously, having two random number generators means memory consumption for storing the generator states. Hence, the protocol doesn't favor scaling of the smart grid environment.

Fouda *et al.* proposes a lightweight mutual authentication protocol and generates a shared session key on the basis of computational Diffie-Hellman exchange protocol [8]. The protocol is applicable between the HAN smart meters and Building Area Networks (BAN) gateway, each of which have a public/private key pair issued by a certificate authority. The paper describes the protocol steps after the HAN smart meter and BAN gateway have extracted and verified their certificates. Fouda *et al.* use computational Diffie-Hellman scheme to establish mutual authentication. The generated shared session key is then combined with hash-based authentication code techniques to authenticate messages between the two entities. The proposed protocol is successful in establishing a semantically secure shared key in the mutual authentication environment. The main disadvantage of this protocol is usage of RSA protocol to establish authentication. The involvement of certificate authority and certificate revocation lists is a costly process for limited devices like HAN smart meters.

Li *et al.* propose a protocol that uses homomorphic encryption to attain secure demand response exchanges in a smart grid environment [15]. The protocol achieves forward secrecy, by renewing the users' key after appropriate intervals. It also achieves entity authentication, and message integrity and confidentiality. Homomorphic encryption is a method in which plaintext is encrypted using algebraic expression. They combine homomorphic encryption with pairing-based cryptography to create the mutual authentication process. In this paper, authentication process is applicable between control center and BAN, as well as between HAN and BAN. Once two entities have successfully established a session key between each other, then message exchange commences. The messages are signed using ID-based signature mechanism. A drawback of the protocol is the absence of explicit key confirmation. As the session key is generated separately at the two entities, it is advisable to confirm the key before commencing message exchange.

3 Background Knowledge

3.1 Topology of Smart Grid

The topology of the smart grid has been adapted from the NIST Conceptual Reference Model for Smart Grid that is shown in Figure 1. Smart grid architecture consists of four main domains: generation, transmission, distribution and consumers. The generation domain consists of the large-scale power plants and small-scale DERs that generate electricity. This is followed by the transmission domain consisting of step-up transformers (transmission voltage), transmission substations and transmission lines that aid in transmitting the electricity to the next domain, the distribution domain. The distribution domain consists of step-down transformers (distribution voltage and service voltage), distribution substations and distribution lines.

Lastly, the consumers include the smart meters at the homes or businesses that directly use electricity. Consumers may be residential or commercial. Electrical sensors and circuit breakers are placed along the entire length of the communication medium between smart meters and generators to constantly monitor voltage and flow. Smart meters also have a hierarchy of their own. The lowest level of the hierarchy consists of the meters installed at the home/business, and is called the HAN smart meter. Several HAN smart meters regularly send their meter readings to a designated BAN gateway, which is the next level in the hierarchy. Lastly, a number of BAN gateway send the collection of meter readings to the Neighborhood Area Network (NAN) gateway. The NAN gateway then forward these meter readings to the utility center. The utility centers are located in the distribution substations.

3.2 Smart Grid Communications

The communication technology used in the smart grid is a combination of wireless and wired technology [7,28]. The generation and transmission domains are entirely based on wired technology such as optical fiber or power line carriers (PLC). Optical fiber technology is advantageous because it is flexible, suitable for the core network, and capable to carry high volume of traffic with the least latency [8]. The consumer domain favors wireless technology to communicate with the distribution domain. The distribution domain consists of wireless technology at the end connected to the consumer domain, and wired technology for the end connected to the transmission domain.

The Smart Grid environment primarily consists of three areas - HAN, BAN and WAN. The potential technologies for HAN are ZigBee, Wi-Fi, Ethernet, Z-Wave

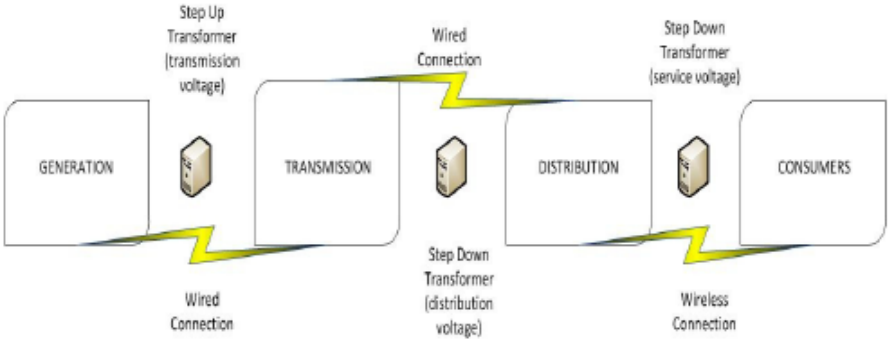

Figure 1: Reference model for smart grid

and PLC. ZigBee is preferred over other wireless technologies such as Wi-Fi or Bluetooth because it consumes the least amount of power and delivers high performance. In BAN, ZigBee, Wi-Fi, PLC and cellular technologies may be used. Wi-Fi and WiMAX are preferred over PLC because they are cost-effective and flexible. As the coverage distance is in tens of kilometers for WAN, potential technologies are Ethernet, microwave, WiMAX, 3G/LTE, and fiber optic links. Wired technologies are typically favored in the WAN connections because wired connections are more robust and secure compared to the wireless connections [2].

3.3 ID-based Cryptography (IBC)

This technique replaces traditional digital certificates with unique identifying attributes, such as email addresses or phone numbers, for encryption and signature verification [21]. IBC replaces the certificate authority with a Private Key Generator (PKG). Before the system nodes enter into mutual authentication processes with one another, the PKG generates a master private-public key pair. The master public key is distributed to all the system nodes. The following procedure describes the encryption and decryption using IBC:

Encryption Process: Node A uses Node B's identifier and the master public key to encrypt Message M. This produces the cipher text C. Node A sends C to Node B. The ease of using IBC is that Node A did not have to make prior arrangements to be able to send a message to Node B, unlike in the traditional certificate process.

Decryption Process: Upon receiving C, Node B contacts PKG to get its secret private key to decrypt C. The PKG then transmits Node B's private key to it over a secure channel. This secure channel may be an SSL link that allows Node B to download its private key. Node B is now able to successfully decrypt C to obtain plaintext M.

Signature: Node A wants to send a signed message to Node B. Upon receiving its private key from the PKG, Node A creates a signature S for Message M and sends it to Node B, along with the plaintext Message M. Signature ensures data integrity as well as non-repudiation of a message. In other words, because the message is signed with a private key and private keys are secret, hence the sender cannot deny having sent the signed message.

Verification: Upon receiving M and S from Node A, Node B applies Node A's identifier and the master public key on M. If the generated signature is the same as S, then Node B accepts the Message M. Else, it rejects Message M.

3.4 Bilinear Pairing

Bilinear degenerate maps are mathematical functions, which when used in combination with ID-based cryptography, produces computationally efficient cryptographic systems [12, 18]. A bilinear map is a pairing function which produces a mapping of elements from one cyclic group to another cyclic group, provided both cyclic groups is of the same prime order [9,10]. The discrete log problem of the first group is hard. Bilinear maps are considered to be secure because they are chosen as one-way functions. In other words, it is easy to calculate the result from a known set of pair of elements, but it is hard vice-versa.

3.5 Zero-knowledge Password Proof

Zero-knowledge password proof (ZKPP) is a technique in which Node A (prover) proves to Node B (verifier) that it possesses knowledge of a password without actually knowing the password [1]. This possession of knowledge about the password works as a verification that the node may be trusted. The password belongs to Node B and never leaves Node B. Node B generates a verifier related to this password and conveys this verifier to all nodes it wants to communicate with. This technique works as an advantage for systems using password-authenticated key agreement (PAKE) protocol because it is robust against off-line dictionary attacks, as is mentioned in IEEE P1363.2. In IEEE P1363.2, ZKPP is defined as "An interactive zero knowledge proof of knowledge of password-driven data shared between a prover and the corresponding verifier."

3.6 Secure Remote Password Protocol

Secure Remote Password Protocol (SRP) is also a modified password-authenticated key agreement protocol [5]. SRP is more secure than SSH protocol, and faster than Diffie-Hellman key exchange in terms of user authentication and data integrity [13,16,17]. Compared to Kerberos protocol, SRP doesn't rely on third parties. The SRP is instantiated with the client node selecting a small random salt. The client node also shares a password with the server node [11, 20, 24]. At the end of the exchange protocol, the client and server nodes now have a symmetric session key. The two nodes need to explicitly confirm that their keys match in order to complete authentication process.

4 Proposed Mutual Authentication Protocol

The proposed protocol ensures a lightweight mutual authentication and key renewal mechanism between the HAN smart meter and the BAN gateway. It also provides confidentiality, authentication and integrity; the three essential requirements for Smart Grid security mentioned by NIST [26].

4.1 Pre-authentication Protocol

Let G be an additive cyclic group of prime order q, and GT be a multiplicative cyclic group of prime order q; let g be the generator of these cyclic groups. In order to build cryptographic systems, pairing-based cryptography utilizes a symmetric bilinear pairing between two elements of an additive group to an element of a multiplicative group [19]. In the proposed protocol, we have used the map e: $G1 \times G2 = GT$, where $G1 = G2 = G$. This mapping satisfies the properties stated below:

Bilinearity: $\forall x, y \in Z_q*$, $\forall A, B \in G : e(A^x, B^y) = e(A, B) \in G_T$;

Non-degeneracy:] $e(A, B) \neq 1$;

Computability:] There exists an efficient algorithm to compute e.

Let there be a bilinear parameter generator which runs an algorithm that takes in as input a security parameter L, and outputs the system's 5-tuple (q, g, G, GT, e).

In the proposed protocol, the BAN gateway also acts as the public key generator (PKG). Hence, as is the function of the PKG, the BAN gateway determines the 5-tuple (q, g, G, GT, e) by providing input L to the bilinear parameter generator. The BAN gateway randomly chooses a master secret key s that belongs to Z_q*. It does not convey the master secret key to any other entity. The cryptographic secure hash functions are determined by the BAN gateway. This protocol utilizes 5 hash functions:

$$H_1(\cdot) : (0,1)* \times (0,1)* \rightarrow (0,1)*$$
$$H_2(\cdot) : (0,1)* \rightarrow G*$$
$$H_3(\cdot) : Z_N* \times G* \rightarrow G*$$
$$H_4(\cdot) : G_T* \rightarrow Z_q*$$
$$H_5(\cdot) : Z_q* \times Z_q* \times G_T* \rightarrow G*.$$

Two messages are exchanged prior to commence of the mutual authentication protocol between the smart meters which is shown in Figure 2. Owing to its steady rise in popularity, WMN is considered as the communication protocol running between the HAN and BAN smart meters.

Each smart meter/gateway bears a unique identifier. Also, each HAN smart meter contains a password its corresponding verifier, which is required to execute the Zero Knowledge Password Proof. The first message conveys the identifier and the verifier of a HAN smart meter (HAN SM) to the BAN gateway (BAN GW) through a secure channel [6]. On receiving the message, the BAN GW stores the received identifier and verifier in its memory. A BAN GW has ten times more memory than a HAN [8]. After receiving the first message, the BAN GW functions as the public key generator. In other words, the BAN GW uses hash function H1 to generate the public key for the HAN SM. Next, it applies its master secret key on this newly-generated public key to create the HAN SM's private key. In this manner, the HAN SM initiates the authentication process between itself and the BAN GW.

The second message serves as an acknowledgement for the HAN SM having sent its authentication request to the designated BAN GW. The private key as well as the public system parameters (q, g, G, GT, e, H_1, H_2, H_3, H_4, H_5) are conveyed via the message from the BAN GW to the HAN SM through a secure channel [6]. Once the HAN SM receives the message, it stores its private key and the public parameters. It then uses hash function H1 from the list of public parameters to create the public key for the BAN GW using the identifier sent by the BAN GW.

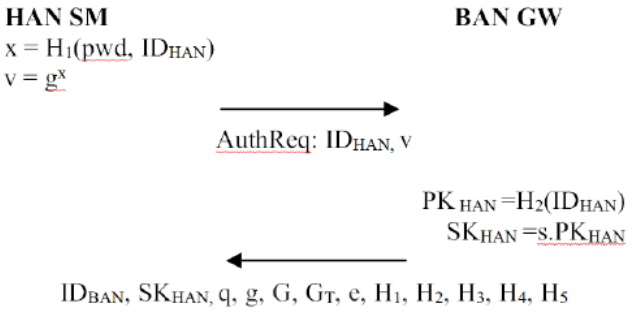

Figure 2: Pre-authentication phase exchange

4.2 Authentication Protocol

In Figure 3, the HAN SM randomly choose a number Z_q*. The HAN SM generates the public key of the BAN as well as variable A using a random number. The HAN SM encrypts A using the public key of the BAN GW. The first message contains the HAN SM's identifier and the encrypted value of A. At the BAN GW, the variable A is first decrypted using the BAN GW's private key. The identifier sent by the HAN SM is used to lookup the verifier corresponding to that identifier. The BAN GW will not be successful if it has the wrong verifier corresponding to a HAN SM identifier. This is because the verifier is derived from the password associated with that specific HAN SM. After storing the value of A and locating the verifier corresponding to the identifier of the HAN SM, the BAN GW then chooses a random number that belongs to Z_q*, which is used to compose B which is utilized in calculating variable J. Variable B also requires k. Referring the Secure Remote Password Protocol, k is derived by applying hash function $H3$ on N and g. N is a safe prime which is equal to $2q+1$, where q is the prime order of the cyclic groups used in pairing-based cryptography; g is the generator of these cyclic groups.

The variable k is calculated by both sides HAN and BAN. Furthermore, when an active adversary impersonates a smart meter, then variable k helps to eliminate 2-for-1 guess. The next step for the BAN GW is to use these values to calculate variable B and variable J. Variable J holds the bilinear pairing map using the private key of the HAN SM, variable A received from HAN SM, and the random number selected by the BAN GW itself. Variable A is sent to the BAN GW in an encrypted manner. Variable J helps enforce one half of the pairing based cryptography because it stores the bilinear mapping at the BAN GW. After J is calculated, W is also devised by applying hash function on J. BAN GW then sends B and W to the HAN SM. On receiving the second Message from the BAN GW, the HAN SM stores B. As mentioned above, k is calculated once again.

The variable J' is constituted of B and other parameters. J' forms the other half of the bilinear pairing because it comprises of the bilinear mapping held at the HAN SM. Based on the properties of bilinear pairing, variables J and J' have to be equal in order for the HAN SM to be able to authenticate the BAN GW. Hence, if W and W' are not equal to each other, then that reflects inconsistencies in its constituent variables resulting in the abortion of the authentication process. If W is equal to W' then the HAN SM authenticates the BAN GW. To complete the mutual authentication protocol, the BAN GW should also trust the HAN SM. To do so, the HAN SM introduces a valid-period and a sequence number initialized to 0. It then forms the first session key, $K1$, by applying a hash function on the valid-period, J' and the sequence number.

Furthermore, this session key is signed with the private key of the HAN SM. In Message 3, the sequence number, valid-period and the signed session key, Signk1, are sent to BAN GW. Upon receiving Sign $k1$, the BAN GW extracts the key, $K1$, using the identifier of the HAN SM on the cipher text received in Message 3. Using the received valid-period and sequence number and the previously calculated J, the BAN GW calculates a session key k' at its end. This key K' is then compared with $K1$. If they are the same, then BAN GW authenticates HAN SM as well.

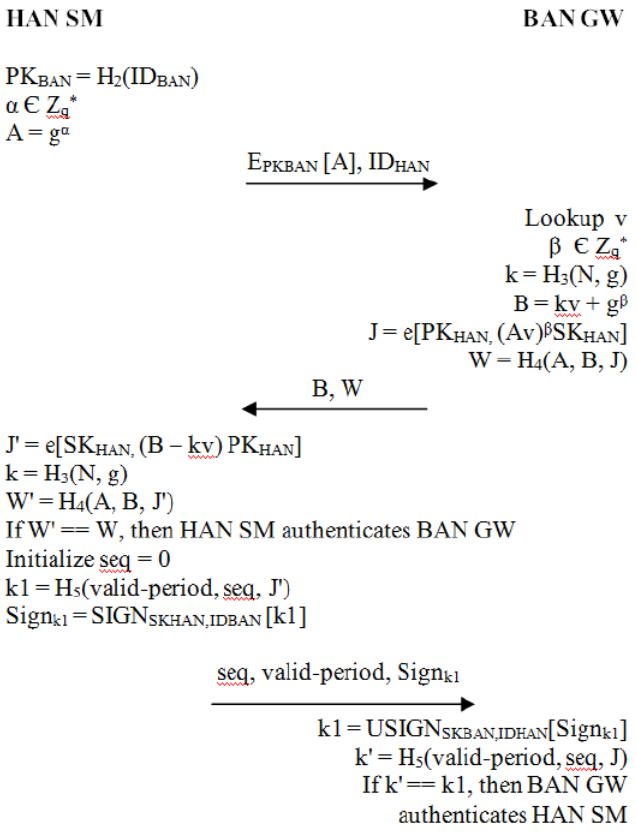

Figure 3: Mutual authentication protocol

Being an public-key based authentication protocol, the proposed authentication protocol provides data integrity, message confidentiality, and non-repudiation.

5 Security Analysis

The proposed protocol is resistant to several attacks. Here, we assume that an active or a passive attack can be made. A passive attacker may observe all exchanges between two smart meters. An active attacker, on the other hand, may make changes to the actual messages. He may further enters into a smart meter and takes control of its operation.

Replay Attack: The protocol is resistant against the replay attack because the adversary does not know the private key of the BAN smart meter, it cannot decrypt the value of A. Owing to the one-directional nature of hash functions, it is extremely difficult and

time-consuming to feed the hash function with random inputs until the known output is achieved. Also, the adversary has no previous knowledge about the password verifier and random value A.

Man-in-the-Middle Attack: A combination of random values, passwords, hashed messages and keys create a strong mutual protocol. Furthermore, the HAN smart meter's private key is exchanged through a secure channel. The attacker will not be able to decrypt or verify any signed messages. The advantage of the proposed protocol lies in the fact that if a message contains a sensitive value, then that is encrypted or signed. Otherwise, the message contains a hash of a value, which can only be verified by being recomputed at the sender's end.

Known Session Key Attack: After an exchange of verifier, random values and keys, the sender and receiver use a different combination of variables and apply a hash function on it. These constituent variables are complex and difficult to guess. The HAN smart meter uses a combination of its private key and the BAN smart meter's public key, along with random value B. The BAN smart meter uses its private key, the HAN smart meter's public key, and random variable A. Both of these values give the same session key but with different set of variables.

Impersonation Attack: During the authentication process, the adversary attempting such an attack will always be unsuccessful owing to several factors. Firstly, the adversary might have access to the HAN smart meter's identifier and public key. But owing to ZKPP, the impersonating attacker will not know the password or the corresponding verifier of the actual HAN SM. Since the mutual authentication depends on the password and its related verifier, hence impersonation attack will definitely not succeed.

Key Control Attack: In the proposed protocol, the session key and mutual authentication process depends on the verifier and its corresponding password, and also between two random numbers exchanged between the two smart meters. The key is calculated individually at both the ends and then verified. Hence, it does not depend on one end alone. Furthermore, bilinear mapping involves using the public and private keys of the entities.

6 Performance Analysis

6.1 Computational Costs

This section evaluates the performance of the proposed protocol. We compare our proposed protocol with a smart grid mutual authentication protocol put forward by Nicanfar *et al.* [4]. The protocol proposed by Nicanfar *et al.* is an efficient mutual authentication scheme between a HAN smart meter and an authentication server. Notations used in this section are shown in Table 1.

Table 1: Parameter notations for performance analysis

T_{bm}	Latency of a bilinear map operation
T_{mul}	Latency of a scalar multiplication operation
T_{add}	Latency of an addition operation
T_{sub}	Latency of a subtraction operation
T_{xor}	Latency of an XOR operation
T_{exp}	Latency of a modular exponentiation operation
T_{pow}	Latency of a power operation
T_h	Latency of a hash operation

Table 2: Computational costs of the proposed protocol

	Proposed Protocol
HAN Side	$5T_h + 2T_{exp} + 1T_{bm} + 1T_{mul} + 1T_{sub}$
BAN Side	$4T_h + 1T_{exp} + 1T_{bm} + 3T_{mul} + 1T_{sub}$ $+1T_{add}$
BAN Side	

Table 3: Computational costs of Nicanfar *et al.* protocol

	Nicanfar *et al.* protocol
SM Side	$10T_h + 2T_{exp} + 1T_{mul} + 1T_{sub}$ $+1T_{xor} + 1T_{add} + 1T_{pow}$
SAS Side	$8T_h + 1T_{exp} + 3T_{mul} + 1T_{bm}$ $+1T_{add} + 2T_{pow}$

The computational costs of our protocol and Nicanfar *et al.* are shown in Tables 2 and 3. To summarize, in regards to the HAN side/SM side, the proposed protocol uses less number of operations compared to the protocol proposed by Nicanfar *et al.* The proposed protocol uses 5 hash operations, whereas the other protocol uses 10 hash operations. Hash operations are one of the least computationally intensive operations, but keeping in mind the memory constraints of the HAN smart meter, it is best to save memory and CPU power under any circumstances. The number of scalar multiplication, modular exponentiation and subtraction operations used in both the protocols is the same. Coming to the BAN side/SAS side, the proposed protocol uses 4 hash function operations and 2 power operations, as compared to the protocol proposed by Nicanfar *et al.*, which uses 8 hash functions and 3 power operations. The number of addition, scalar multiplication and modular exponentiations between the two protocols is the same. In case of similar operations, the protocol proposed in this thesis is always using a lesser

number of operations as compared to the other protocol. As is shown in Table 4 the proposed protocol ensures mutual authentication with one encryption/decryption operation, and one sign/verify operation.

Table 4: Encryption/Signature in the proposed protocol

	HAN Side	BAN Side
Encryption/Decryption	1 Encryption	1 Decryption
Sign/Verify	1 Sign	1 Verify

Table 5: Encryption/Signature in Nicanfar *et al.* protocol

	SM Side	SAS Side
Encryption/Decryption	1 Encryption 1 Decryption	1 Decryption 1 Encryption
Sign/Verify	1 Sign 1 Verify	1 Verify 1 Sign

On the other hand, Table 5 shows that the other protocol has 2 encryption/decryption operations, and 2 sign/verify operations. As these operations are expensive for the resource-constrained smart meters, hence the proposed protocol proves to be more lightweight by using the common principles of SRP protocol, ID-based cryptography, bilinear mapping and ZKPP.

6.2 Simulation Results

The following subsection compares the performance of the proposed protocol with the Elliptic Curve Digital Signature Algorithm (ECDSA). The simulation parameters are shown in Table 6. As the proposed protocol uses AES-128 and SHA-256, therefore its equivalent algorithm ECDSA-256 has been chosen. The reason for choosing ECDSA is that it is a standardized algorithm, already in practice in the smart grid environment. MATLAB [22] and OpenSSL [27] have been used to generate results which depict that the proposed protocol is a better alternative.

Communication Overhead: The communication overhead of the proposed protocol and ECDSA is shown in Figure 4. When the number of HAN smart meters is 50, the communication overhead experienced by the BAN smart meter is around 100 KB for the proposed protocol, and around 300 KB for the ECDSA algorithm. As the number of HAN smart meters increase to 125, the disparity between these two methods increase further. ECDSA algorithm has a communication overhead close to 775 KB. On the other hand, the proposed protocol displays a communication overhead of less than 300 KB. In the last scenario, when the number of HAN smart meters is 250, the communication overhead for ECDSA algorithm is almost 1550 KB, whereas the proposed protocol consumes 600 KB. This value is less than half of the communication overhead experienced in the ECDSA algorithm. Hence, with an increasing number of smart meters at the HAN, the communication overhead will increase greatly for the ECDSA algorithm. This may act as a barrier in further expansion of the smart meter network.

Table 6: Simulation parameters

Simulation Parameters	Value
Interval of Message Generation	Once every hour
Simulation Time	24 Hours
TCP Header	20 Bytes
IPv4 Header	20 Bytes
Ethernet Header	26 Bytes
Payload	32 Bytes
SHA-256 Header	32 Bytes
ECDSA Signature Size	64 Bytes
ECDSA Certificate Size	125 Bytes
Number of HAN Smart Meters	Maximum of 250 per BAN Gateway

Average Delay: Average delay refers to the mean time take to perform decryption/signature verification for the cipher text. In Figures 5 and 6, the BAN gateway experiences an average delay of 0.075 seconds for 250 smart meters, each generating meter reports once every hour over 24 hours. Considering the highest number of smart meters in this simulation, which is 250, the proposed protocol experiences an average delay of 0.0085ms for 50 smart meters. Similarly, for 175 and 250 smart meters, the average delay generated is 0.095 ms and about 0.01 ms respectively. On the other hand, the ECDSA algorithm experiences an average delay of 0.05 seconds for 250 smart meters. This comparison shows the wide difference between the ECDSA algorithm and the proposed protocol. Furthermore, RSA displays a very high delay of 0.075 seconds for the same number of smart meters.

Considering the highest number of smart meters in this simulation, which is 250, the proposed protocol experiences an average delay of 0.0085ms for 50 smart meters. Similarly, for 175 and 250 smart meters, the average delay generated is 0.095 ms and about 0.01 ms respectively. On the other hand, the ECDSA algorithm experiences an average delay of 0.05 seconds for 250 smart meters. This comparison shows the wide difference between the ECDSA algorithm and the proposed protocol. Furthermore, RSA displays a very high delay of 0.075 seconds for the same number of smart meters.

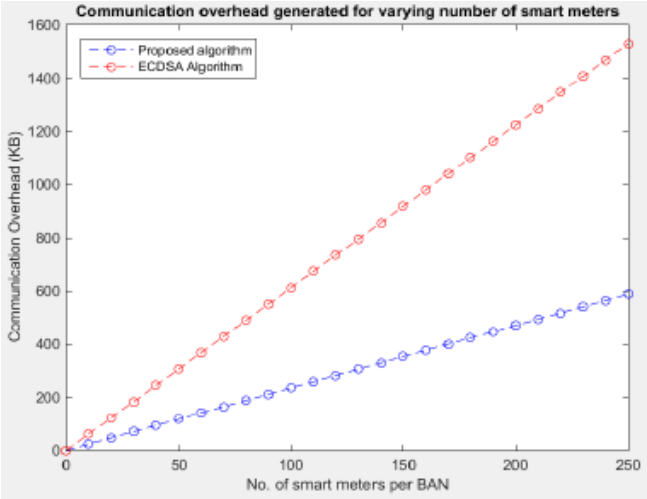

Figure 4: Communication overhead

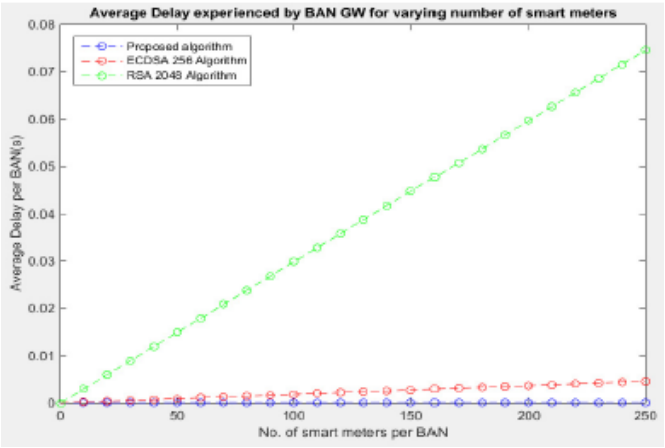

Figure 5: Average delay experienced for proposed protocol

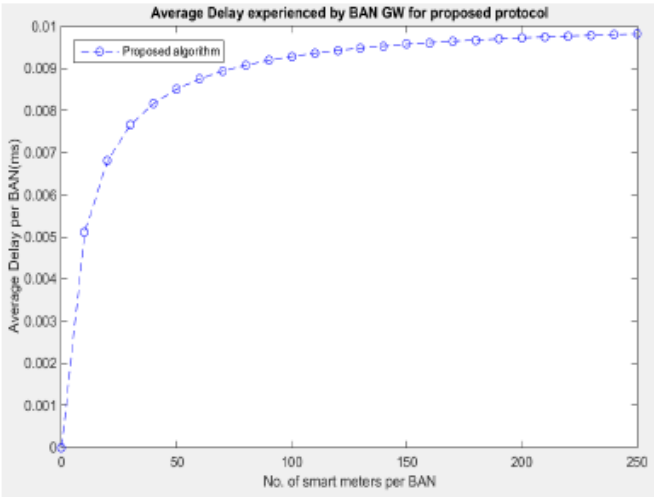

Figure 6: Average delay experienced by BAN GW

7 Conclusion

The proposed authentication protocol describes an efficient lightweight scheme to provide mutual authentication between the HAN smart meter and BAN gateway. This scheme provides source authentication, data integrity, message confidentiality, and non-repudiation as well. The proposed protocol is secure against Replay, Man-in-the-Middle, Known Session Key, Impersonation and Key Control Attacks. On comparison with the efficient mutual authentication protocol proposed by Nicanfar *et al.* [25], the proposed protocol utilizes lesser number of computation operations, while achieving the same results in terms of message security. To be specific, the main difference between these two protocols is that the proposed scheme uses Pairing-based Cryptography, whereas the other protocol uses Enhanced ID-based Cryptography (EIBC). In addition, the proposed protocol is compared with ECDSA, which is currently used in smart meter authentication. The parameters of comparison between these two schemes are as follows: communication overhead, average delay, and buffer occupancy. In each case, the proposed protocol proves to be more lightweight and efficient. Firstly, the proposed protocol incurs a communication overhead of 98 bytes, whereas ECDSA incurs 255 bytes (mainly owing to the ECDSA signature and certificate). Secondly, the BAN gateway has an average delay of 0.01ms and 0.05 seconds in the proposed protocol and the ECDSA scheme respectively. Lastly, using ECDSA, the BAN gateway exhausts its 1128 KB buffer while handling an incoming message rate of 100 messages every 15 minutes across a simulation period of 8 hours. On the other hand, the proposed protocol consumes 775 KB in the same simulation environment. Hence, proving that it is scalable as well as lightweight.

References

[1] A. Ahmed, A. Younes, A. Abdellah, Y. Sadqi, "Strong zero-knowledge authentication based on virtual passwords," *International Journal of Network Security*, vol. 18, no. 4, pp. 601-616, 2016.

[2] M. Badra, S. Zeadally, "An improved privacy solution for the smart grid," *International Journal of Network Security*, vol. 18, no. 3, pp. 529-537, 2016.

[3] M. Balakrishnan, *Security in Smart Meters*, Aug. 2012. (`https://cache.freescale.com`)

[4] M. Balakrishnan, M. Mienkina, *Designing Smart Meters for the Smart Grid*, Jan. 6, 2018. (`http://docplayer.net/27262011-Designing-smart-meters-for-the-smart-grid.html`)

[5] T. Y. Chang, W. P. Yang, M. S. Hwang, "Simple authenticated key agreement and protected password change protocol", *Computers & Mathematics with Applications*, vol. 49, pp. 703–714, 2005.

[6] C. Chou, K. Tsai, C. Lu, "Two ID-based authenticated schemes with key agreement for mobile envi-

ronments," *Journal of Supercomputing*, vol. 66, no. 2, pp. 973-988, Nov. 2013.

[7] C. Chrysoulas, "Shielding the grid world: An overview," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 23-28, 2014.

[8] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, S. Xuemin, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675-685, Dec. 2011.

[9] X. Fu, X. Nie, and F. Li, "Outsource the ciphertext decryption of inner product predicate encryption scheme based on prime order bilinear map," *International Journal of Network Security*, vol. 19, no. 2, pp. 313-322, 2017.

[10] P. Hu, H. Gao, "A key-policy attribute-based encryption scheme for general circuit from bilinear maps," *International Journal of Network Security*, vol. 19, no. 5, pp. 704-710, 2017.

[11] M. S. Hwang, C. C. Lee, Y. L. Tang, "An improvement of SPLICE/AS in WIDE against guessing attack", *International Journal of Informatica*, vol. 12, no. 2, pp.297–302, Apr. 2001.

[12] B. King, "A dynamic threshold decryption scheme using bilinear pairings," *International Journal of Network Security*, vol. 17, no. 6, pp. 771-778, 2015.

[13] P. Kuacharoen, "An anti-phishing password authentication protocol," *International Journal of Network Security*, vol. 19, no. 5, pp. 711-719, 2017.

[14] H. Li, *Enabling Secure and Privacy Preserving Communications in Smart Grids*, Springer, Aug. 2015.

[15] H. Li, X. Lin, H. Yang, X. Liang,R. Lu, X. Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2053-2064, Apr. 2013.

[16] C. W. Lin, C. S. Tsai, M. S. Hwang, "A new strong-password authentication scheme using one-way hash functions", *International Journal of Computer and Systems Sciences*, vol. 45, no. 4, pp. 623–626, July 2006.

[17] C. H. Ling, C. C. Lee, C. C. Yang, M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN," *International Journal of Network Security*, vol. 19, no. 2, pp. 177-181, 2017.

[18] J. Ling, G. Zhao, "An improved anonymous password authentication scheme using nonce and bilinear pairings," *International Journal of Network Security*, vol. 17, no. 6, pp. 787-794, 2015.

[19] N. Liu, J. Chen, L. Zhu, J. Zhang, Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 10, pp. 4746-4756, Aug. 2013.

[20] Y. Liu, C. C. Chang and S. C. Chang, "An efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, no. 1, pp. 1–10, 2017.

[21] C. March and C. Youngblood, *An Introduction to Identity-based Cryptography*, Jan. 6, 2018. (`https://www.researchgate.net`)

[22] MatLab, *MATLAB and Statistics Toolbox Release 2014b*, Jan. 6, 2018. (`https://www.mathworks.com`)

[23] J. Menezes, O. P. C. Van, S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton: CRC Press, 1997.

[24] J. Moon, D. Lee, J. Jung, D. Won, "Improvement of efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, no. 6, pp. 1053-1061, 2017.

[25] H. Nicanfar, P. Jokar, K. Beznosov, V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629-640, July 2014.

[26] NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*, NIST Special Publication 1108R2, Aug. 2015.

[27] OpenSSL, *OpenSSL*, Jan. 6, 2018. (`https://www.openssl.org/`)

[28] R. Singh and M. S. Manu, "An energy efficient grid based static node deployment strategy for wireless sensor networks," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 32-40, 2017.

[29] H. K. H. So, S. H. Kwok, E. Y. Lam, and K. S. Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in *Proceedings of First IEEE International Conference on Smart Grid Communications*, pp. 321-326, Oct. 2010.

Authors' Biographies

Debsmita Ghosh completed her MASc student in computer networks at Ryerson University. Her research interest is on security and privacy of smart grid and power system computer networks.

Celia Li completed her Ph.D degree in electrical engineering and computer science department in 2015 at York University. Her research is focused on security and privacy, role-based access control and wireless mesh network security.

Cungang Yang completed his Ph.D degree in computer science in 2003 at University of Regina, Canada. In 2003, he joined the Ryerson University as an assistant professor in the Department of Electrical and Computer Engineering. His research areas include security and privacy, enhanced role-based access control model, information flow control, web security and secure wireless networks.