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/TSG.2018.2857558, IEEE Transactions on Smart Grid

Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks

Pardeep Kumar, *Member, IEEE,* Andrei Gurtov, *Senior Member, IEEE,* Mangal Sain, Andrew Martin, and Phuong H. Ha

***Abstract*—Smart meters are considered as foundational part of the smart metering infrastructure (SMI) in smart energy networks. Smart meter is a digital device that makes use of two-way communication between consumer and utility to exchange, manage and control energy consumptions within a home. However, despite all the features, a smart meter raises several security-related concerns. For instance, how to exchange data between the legal entities (e.g., smart meter and utility server) while maintaining privacy of the consumer. To address these concerns, authentication and key agreement in SMI can provide important security properties that not only to maintain a trust between the legitimate entities but also to satisfy other security services. This work presents a lightweight authentication and key agreement (LAKA) that enables trust, anonymity, integrity and adequate security in the domain of smart energy network. The proposed scheme employs hybrid cryptography to facilitate mutual trust (authentication), dynamic session key, integrity, and anonymity. We justify the feasibility of the proposed scheme with a test-bed using 802.15.4 based device (i.e., smart meter). Moreover, through the security and performance analysis, we show that the proposed scheme is more effective and energy efficient compared to the previous schemes.**

***Index Terms*—Authentication, key agreement, smart metering infrastructure, smart energy networks.**

I. Introduction

SMART energy network (SEN) is known as a revolutionary solution for the future energy industry. In practice, it includes various notable features, such as reduce carbon footprint, provide uninterrupted energy supply, balancing supply-demand, monitoring inflicted load, efficient power quality, smart billing, and many more [1]. Altogether, SEN can operate much more reliably and efficiently to serve a number of entities, for instance customers (domestic or non-domestic), local societies and governments, etc. A smart metering infrastructure is one of the main application domains in the SEN. This infrastructure integrates the utility company and consumers to actively participate in the real time energy management programs. World-wide several smart metering projects are under-way, e.g., 30 millions electricity meters are smart in Italy. Several SMI-based pilot projects are under progress in Germany, e.g., E-DeMa, SmartWatts [2]. Moreover, in the Netherlands and Great Britain, smart gas and smart electricity meters being included together in SMI network. For more details on the EU smart metering projects refer to [3].

A SEN is an intelligent network where a massive number of heterogeneous devices, several open communications and networking technologies are anticipated to be deployed between the energy companies and consumers. For instance, Fig. 1 shows a typical SMI network – a home area network (HAN) where resource-constrained smart meters (e.g., gas and electricity) generally collect, control and manage the utility consumptions within a home. Furthermore, utilizing a two-way communication technology, the smart meter can transmit/receive data and control commands to/from the neighbourhood area network (NAN) gateway and then to/from the utility server (US).

Smart meters (i.e., gas and electricity) are usually installed outside of the home (i.e., in open environment), and are protected with a physical box [4]. Note that smart meter and meter are used interchangeably. Nevertheless, such openness of smart meters, inevitably surrender them to a number of potential vulnerabilities. For instance: (i) an unauthorized user may compromise a meter from the physical box and control the home appliances. Moreover, he/she may counterfeit device (e.g., smart meter) failures by tampering meter data and/or by injecting falsify data for "tripping" to cut the energy off. (ii) As a smart meter usually sends consumption usage every 15/30/60 minutes periodically [5], an ill-intention user may eavesdrop wireless communication channels, and may leak consumption data for own purposes [6]. Such message leaks can directly used to invade privacy of the consumer (e.g., what time the property is occupied or empty, etc.), as discussed in [7], [8]. (iii) Even worse, if vulnerabilities are exploited successfully then an adversary could surprisingly damage the entire home, city, and/or societies to tumble apart [5]. For instance, on December 23, 2015, three Ukrainian energy supply companies experienced massive cyberattack that resulted in the power blackout in a region for several hours, as reported in [9]. In this attack, one of the vulnerabilities is attributed to lack of adequate authentication that was exploited by the attackers to break the control systems of the grid [9].

1) Related work: Authentication is considered as an imperative property in the identification of an entity to protect unauthorized accesses and to eliminate several security attacks [10]. Recently, many authentication and key agreement schemes have been discussed and presented in the context of SMI for smart grid (SG) [11]–[23]. Many of these protocols (e.g., [13]–[16]) are originally focusing on one-way authentication while leaving out two-way authentication. For example, He

P. Kumar and A. Martin are with the University of Oxford, Oxford, United Kingdom, (email: pardeep.kumar@cs.ox.ac.uk, andrew.martin@cs.ox.ac.uk)

A. Gurtov is with Linkoping University, Sweden and ITMO University (e-mail: gurtov@acm.org)

M. Sain is with Dongseo University, South Korea (e-mail: mangalsain1@gmail.com)

P. H. Ha is with The Arctic University of Norway, Norway (e-mail: phuong.hoai.ha@uit.no)

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/TSG.2018.2857558, IEEE Transactions on Smart Grid

et al. [13] proposed an enhanced public key infrastructure (PKI) for securing SG networks. The scheme performed one-way authentication from a smart meter to the NAN gateway. The authors exploited PKI based digital signatures especially resisting denial of service attack. To justify the feasibility of enhanced scheme, He et al. implemented elliptic curve cryptography (ECC) via TinyECC library for the resource-constrained smart meter. Their scheme takes 3.169 seconds to generate a signature for per-packet, and 4 seconds for per-packet signature verification. As a result, the scheme required high complexity at the meter. Similar to He et al. [13], Chim et al. [14] proposed privacy-preserving scheme that utilized cryptographic commitments to send consumption usages from the meter to utility via the NAN gateway. The Chim et al.'s scheme mainly supports one-way authentication and achieves privacy. Note that in [13], [14], a smart meter is being authenticated at the NAN gateway, but it cannot verify whether the NAN gateway is a legal entity. Consequently, the schemes proposed in [13]–[16] may lead to many security threats, e.g., a smart meter may accept fake control commands from an attacker, since the NAN gateway is not being verified at the smart meter. Furthermore, in a worst scenario, a fake control command can turn the house blackout. As a result, one-way authentication may not provide enough security in two-way communication use-cases.

On the other hand, the protocols presented in [11], [17]–[21], [23], performed mutual authentication in smart grid but most of the schemes required high computational overhead that may pose performance (i.e., availability) issue in such critical infrastructure. For instance, to perform mutual authentication and key establishment, Fouda et al. [11] suggested a lightweight and secure authentication where a smart meter is expected to be verified before it communicates with other entities. The authors utilized the Diffie-Helman protocol to perform mutual authentication, and established a session key between two entities (i.e., smart meter and NAN). The scheme requires higher packet delay for executing numbers of messages. Moreover, the packet delay is ≈ 11 seconds which could be a strongest link from an attacker perspective: if thousands of smart meters are deployed then the attacker may easily mount various security attacks, e.g., denial-of-service.

To generate a secure session key between the smart meter and authentication server, Nicanfar et al. proposed a scheme that verifies communicating entities mutually [17]. The authors used a key generator to refresh the public and private keys along with multicasting keys, which are then broadcasted periodically to all smart meters. However, the authors in [1] and [22] argued that the Nicanfar et al.'s scheme is neither comparatively practical nor efficient for the smart meter, as the scheme required heavy computations.

In 2016, Tsai-Lo proposed a secure anonymous key distribution scheme for SG communications [19]. The authors utilized an identity based signature to achieve mutual authentication and anonymity at low computational cost. Moreover, it can resist to a number of attacks, e.g., replay, impersonation, man-in-the-middle (MITM), etc. However, the scheme of Tsai-Lo is being failed to provide session key (SKey) security and smart meter's credientials privacy underneath the Canetti-Krawczyk's attack model, as pointed out by Odelu et al. in [20]. Then in [20], the authors proposed another (secure) authentication and session key agreement scheme in SG. Odelu et al. asserted that their scheme required low computational cost and more secure than the Tsai-Lo's scheme. However, the Odelu et al.'s scheme is vulnerable to impersonation attack and that may lead to forgery of the messages, MITM, and/or message integrity issue, as pointed out in [24]. Using ECC, He et al. proposed a new lightweight, anonymous, and key distribution (AKD) scheme in [21]. AKD adopts Schnorr's signature [25] technique to achieve the efficiency. Mohammadali et al. [22] proposed a novel identity based key establishment scheme for MICAZ-based smart metering networks. The authors claimed that their scheme is secure against many real attacks, e.g., replay, impersonation, man-in-the-middle attack, etc. However, the scheme may not withstand against identity spoofing attack, since the smart meter identity is used as a plain-text.

Considering PKI, Mahmood et al. proposed a lightweight message authentication scheme for SG [23]. The authors utilized hybrid cryptosystem (i.e., AES and RSA). Recent studies revealed that the operation of public key (e.g., encryption) may be practical but the operations of private key are still time consuming (e.g., decryption takes 5.2s and signature generation takes 5.21s [22]) for a resource constrained device (e.g., MICAZ-based smart meter).

To mitigate outsider and insider attacks, Saxena et al. [10] discussed another authentication and authorization scheme in SG. In the scheme, an individual needs to perform authentication and authorization to access a smart meter. An attribute-based access control is utilized to confirm individual's identity together with the device. The overall overhead of the scheme is 328.37 bytes, which is still expensive for those meters that have limited computational power, transmission capability and energy-source (e.g., a smart gas meter [26]).

Indeed, the power source may not be the main concern for a smart electricity meter, which is usually connected with the main-supply. While on the contrary, the power source is a major issue for a smart gas meter, which is a battery-powered device [26]. For instance, a smart meter periodically sends consumption usages to the utility, however, such periodic communications need more energy to send a large number of packets. Hence, the security scheme should be energy-efficient (in the terms of computational and communicational costs) so as to maximize the smart meter and network lifetime, while providing the adequate level of security.

2) Motivation: The one-way authentication schemes, and the high computational and communicational costs can raise concern in two-way smart energy communications. Moreover, in the SEN communication, the integrity of messages is equally important as other security properties, since message integrity provides assurance that the messages are not been altered/forged in transit (or from the origin), as suggested by the National Institute Standards Technology (NIST) [27]. A loss of integrity may cause destruction of information and may lead to incorrect decision in smart energy network. However, the most of recently proposed schemes (e.g., [17], [19], [20], [21]), are vulnerable where an attacker can violate 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/TSG.2018.2857558, IEEE Transactions on Smart Grid

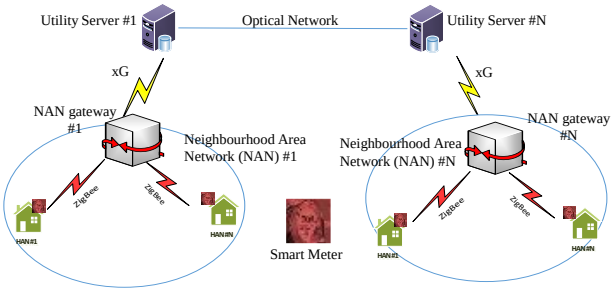

Fig. 1. Considered Smart Metering Infrastructure.

integrity. Therefore, it becomes necessary to establish a mutual authentication that can support dynamic key agreement to realize its efficiency while providing the adequate level of security functionalities.

3) Our contribution: We propose a new lightweight authentication and key agreement (LAKA) scheme for SMI from the perspective of SENs and the main contributions are:

- LAKA supports mutual authentication, key establishment, anonymity, integrity, and realizing its practicality in the SMI. The scheme requires less computational cost as it is built upon the ECC, symmetric encryption, hash function and message authentication code.
- We analyze the security strength of LAKA and utilize AVISPA (i.e., automated verification of Internet security protocol and application) tool to formally prove that the SMI is semantically secure with the help of our scheme.
- The viability of LAKA is validated using IEEE 802.15.4 based smart meter. Furthermore, we report performance evaluation results, and demonstrate that the proposed scheme is lightweight and provide more security services than the previously proposed schemes.

II. Network Architecture, Threat Model and Security Goals

1) Network architecture: By generalizing the previous proposals [11], [14], [28], [29], consider a hierarchical smart energy network model (Fig. 1), including a home area network (HAN), and a neighbourhood area network (NAN).

- Every HAN contains a smart meter that measures and collects the utility usages within a home. Through the smart meter, the consumption usages are not only be received (periodically) by the utility (refer to Fig. 1) but a consumer can also received them to monitor and control in day-to-day life.
  To do this, a smart meter communicates to the NAN gateway via public channels. A smart meter data is vulnerable as the communication channels between the source (i.e., smart meter) and destination (i.e., NAN) can be manipulated purposefully. Thus it is necessary to authenticate both the entities prior their participation in the SEN [11] [14].
- The NAN gateway collects consumption readings from several smart meters, and forwards collected readings to the utility server, securely. The NAN gateway provides the interface between the upper layer (i.e., utility server) and the lower layer (i.e., meter). It is usually integrated with wireless (ZigBee, WiMAX, WiFi, etc.) or wired technologies, and distributed over many cities, or villages. Moreover, the physical security of the NAN gateway can be protected as it is located inside substation and locked from outsider access as recommended by [14] [30]. Note that the main focus of our scheme is to establish a secure and efficient communication between the two ends (i.e., smart meter and NAN). We assumed that the NAN gateway is securely connected with the utility server (US).

2) Threat Model: Following Fig. 1, we assume that an attacker (e.g., Dolve-Yao threat model [31]) can eavesdrop and intercept two-way wireless channels between the smart meter and the NAN gateway. An attacker can attempt to replay the old messages either to SM or to NAN gateway. He/she can attempt to inject new messages and forge messages for own purpose. Moreover, an adversary can spoof identities or other important parameters in order to learn sensitive information from the consumer to the NAN communication and vice-versa.

3) Security goals: Towards a SMI network an adequate security suite essentially satisfies the following goals: *1) Mutual authentication and key establishment:* In a SMI network, it is paramount security requirement that a NAN gateway must authenticate to a smart meter, since consumption data collected from smart meters will be utilized for many purposes e.g., billing, load balancing, etc. Similarly, a smart meter should authenticate the NAN gateway in order to protect from fake messages (e.g., control commands, etc.) from an attacker. Thus mutual authentication is highly required [32]. As soon as mutual authentication verified, a fresh session key agreement should be generated for the legal parties, so that subsequent communication could take place securely. *2) Confidentiality:* As per the NIST security policies, the messages which are being exchanged over public channels between any two or more legal entities should not be disclosed against illegal access and modification. *3) Message Integrity:* Similar to confidentiality, message integrity is also important requirement in smart grid as suggested in the NIST security guideline. So that protocol's messages can not be forged in transit or from their origin. *4) Availability:* The messages should available timely – the SMI requires high computational and communicational efficiency to execute the security mechanisms. Therefore, the process and/or overhead of authentication should be as low as possible [27]. *5) Forward security:* An adversary should not be correlated to any two communication sessions, and also should not be derived the past messages according to the ongoing session. *6) Anonymity:* Smart meters are supposed to transmit attributable fine grained data to the utility for the billing use-case. Nevertheless, the attributable fine grained data including device identity, energy usage, and so on, is vulnerable. For instance, an adversary can easily spoof/correlate the identities of smart meters that are reporting detailed fine grained information from the HAN to NAN. Thus, the identity of a meter should be kept private.

III. Proposed Scheme

The proposed scheme involves mainly two entities (the smart meter (SM) and the NAN gateway). Before describing

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/TSG.2018.2857558, IEEE Transactions on Smart Grid

TABLE I
SYMBOLS AND DESCRIPTIONS

Symbols	Descriptions
N_{ID}	Neighborhood Area Network (NAN) identity
SM_{ID}	Smart meter identity
ST, id_{ST}	Secret token and its identity
$E_K[ms]$	Encrypt ms using key *(K)*
$D_K[ms]$	Decrypt ms using key *(K)*
p, n	Large prime numbers
F_q	A finite field
E	Elliptic curve defined on finite field F_q with prime order n
G	Group of elliptic curve points on E
P	A point on elliptic curve E with order n
$H(.)$	One-way hash function (e.g., SHA-1, SHA-2, MD5, etc.)
MAC, $\|\|$	Message authentication code, and concatenation operation
ϕ, ϕ_N	SM's and NAN's pseudo random numbers, respectively

the proposed scheme, we have made few assumptions: (i) The clocks of SM and NAN gateway are synchronized as recommended in [14], [33]–[35]. (ii) The NAN gateway is a trusted service provider and resource-rich entity [11], [14], [28], [29] and (iii) The smart meters have to be registered with NAN to obtain the security parameters. Table I describes used notations and symbols throughout the paper.

1) System setup phase: As a trusted entity, the NAN gateway should be able to perform the off-line tasks, such as, assigning security parameters, assigning identity to SMs and keeping access logs, securely. In this phase, the NAN gateway sets up security parameters, as follows.

Note: due to the page limit we omitted background of the ECC, the reader may refer to [36], [37]. The NAN chooses an elliptic curve E and a point P of order n over the curve E. Generates a high entropy master key (M_k) and public key $P_s = M_k \cdot P$. Now it selects one way secure hash function (e.g., $H()$). Finally it keeps M_k secure in own database, and publishes $F_p, P, E, n, P_s, H()$.

2) Registration phase: The household smart meter needs to be registered at the NAN gateway before participating into the SEN and obtained security parameters, as follows. For each SM (say *j*), the NAN generates and assigns an unique identity (SM_{ID_j}) and a secret token ST_j with its identifier (id_{ST_j}). It uses SM_{IDj} to compute $\sigma_j = H(SM_{ID_j})$ and public key, i.e., $(SM_{pub_j} = (\sigma_j + M_k)P = \sigma_j P + P_s)$. Then it uses the master key M_k to compute SM's corresponding private key $SM_{pr_j} = \frac{1}{M_k+\sigma_j} P \in G$. Similar to [19] [20], the NAN stores all the security parameters $(F_p, P, E, n, ST_j, id_{ST_j}, H(), \sigma_j, SM_{pr_j})$ in SM's tamper-proof memory. In addition, the NAN gateway also stores SM_{IDj}, N_{ID} in the memory of meter so that it can recognize the respective NAN gateway. Finally, the NAN gateway keeps all the parameters in own database to keep records of the deployed SMs.

3) Authentication and key establishment phase: To attain LAKA's goals, i.e., lightweight authentication and key establishment, the detailed procedure is as follows.

(A) The SM chooses random number $u_{SM_j} \in Z_n^*$ and computes $A_{SM_j} = u_{SM_j} \cdot P$ and $B_{SM_j} = u_{SM_j} \cdot SM_{pr_j}$. Then it computes $L1 = H(SM_{ID_j}||N_{ID}||A_{SM_j}||B_{SM_j}||T1)$ and $Q1 = E_{ST_j}[SM_{ID_j}, N_{ID}, T1]$. Note: $T1$ denotes the current time stamp of SM. In order to provide the message integrity, the SM computes $Y1 = MAC_{L1}[SM_{ID_j}, T1, A_{SM_j}]$. It generates a pseudo number (ϕ) and computes $\alpha = H(N_{ID}||\phi) \oplus id_{ST_j}||T1$, and finally, sends a message, *start* $\{\alpha, Q1, A_{SM_j}, Y1, \phi, T1\}$ to the NAN.

(B) Upon receiving the message, the NAN gateway first checks the validity of time using $(T2 - T1) \leq \Delta T$, if it does not hold then aborts the system. Note: $T2$ denotes the current time stamp of NAN and ΔT is the transmission delay. Otherwise, it computes $H(N_{ID}||\phi)$ and obtains id_{ST_j}, gets corresponding token (ST_j) of id_{ST_j}, and SM_{ID_j} from own database. Decrypts $D_{ST_j}[Q1]$, and obtains $SM^*_{ID_j}, N^*_{ID}, T1^*$. Now checks $(SM^*_{ID_j} = SM_{ID_j}$, $N^*_{ID} = N_{ID}$, and $T1^* = T1)$, if these conditions are not being verified then it aborts current session request. Now, the NAN gateway computes $\sigma'_j = H(SM_{ID_j})$, $B'_{SM_j} = \frac{1}{M_k+\sigma'_j} A_{SM_j}$, and $L1' = H(SM_{ID_j}||N_{ID}||A_{SM_j}||B'_{SM_j}||T1)$. Furthermore, it computes $Y1'(= MAC_{L1'}[SM^*_{ID_j}, T1^*, A_{SM_j}])$ and then verifies $Y1' = Y1$, if yes, goes to the next step.

(C) The NAN gateway selects a random number $v_N \in Z_n^*$ and computes $C_N = v_N \cdot P$, and $F_N = v_N \cdot A_{SM_j}$. Then, it computes $Q2 = E_{ST_j}[SM_{ID_j}, N_{ID}, T2]$, and $Y2 = MAC_{L1'}[N_{ID}, T2, C_N]$. Here, $T2$ denotes the current time stamp of NAN. Now, it generates a session key $(SK = H(SM_{ID_j}||N_{ID}||A_{SM_j}||C_N||F_N)$. Finally, it generates a pseudo number (ϕ_N), computes $\beta = H(N_{ID}||\phi_N) \oplus id_{ST_j}||T2$, and sends *Response* = $\{\beta, C_N, Q2, Y2, \phi_N, T2\}$ to the SM.

(D) The SM first checks $(T3 - T2) \leq \Delta T$, it will terminate the session if time stamp verification produces negative result. Otherwise, obtains id_{ST_j} from β and then, decrypts $D_{ST_j}[Q2]$ to obtain $SM^*_{ID_j}, N^*_{ID}, T2^*$, and verifies $N^*_{ID} = N_{ID}$ and $T2^* = T2$. If conditions are not true then terminates the session. Otherwise, it computes $Y2'(= MAC_{L1}[N_{ID}, T2^*, C_N])$ and verifies $Y2' = Y2$, if the condition is true then only proceeds to the next step. Otherwise the NAN is not a legitimate entity and the session will be terminated. Finally, the SM computes $W_{SM_j} = u_{SM_j} \cdot C_N$ and generates the session key $SK = H(SM_{ID_j}||N_{ID}||A_{SM_j}||C_N||W_{SM_j})$ in order to secure further communication between the SM and NAN gateway. The flow of LAKA is shown in Fig. 2.

IV. SECURITY ANALYSIS

A. Formal analysis of LAKA using AVISPA

The AVISPA tool is designed for the Automated Verification of Internet Security Protocols and Applications and it is quite well known in the academia [17], [22], [38]–[40]. It has four different backend model checkers: (i) on-the fly model-checker; (ii) constraint-logic-based attack searcher; (iii) SAT-based model-checker; and (iv) tree automata based on automatic approximations of the analysis of security protocols. The tool uses a role-based language, i.e., high level security protocol specification language (HLPSL), for specifying the role of each agent. The roles are: (i) *basic role*, describes what initial data can be used by an agent and how the transitions are being

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/TSG.2018.2857558, IEEE Transactions on Smart Grid

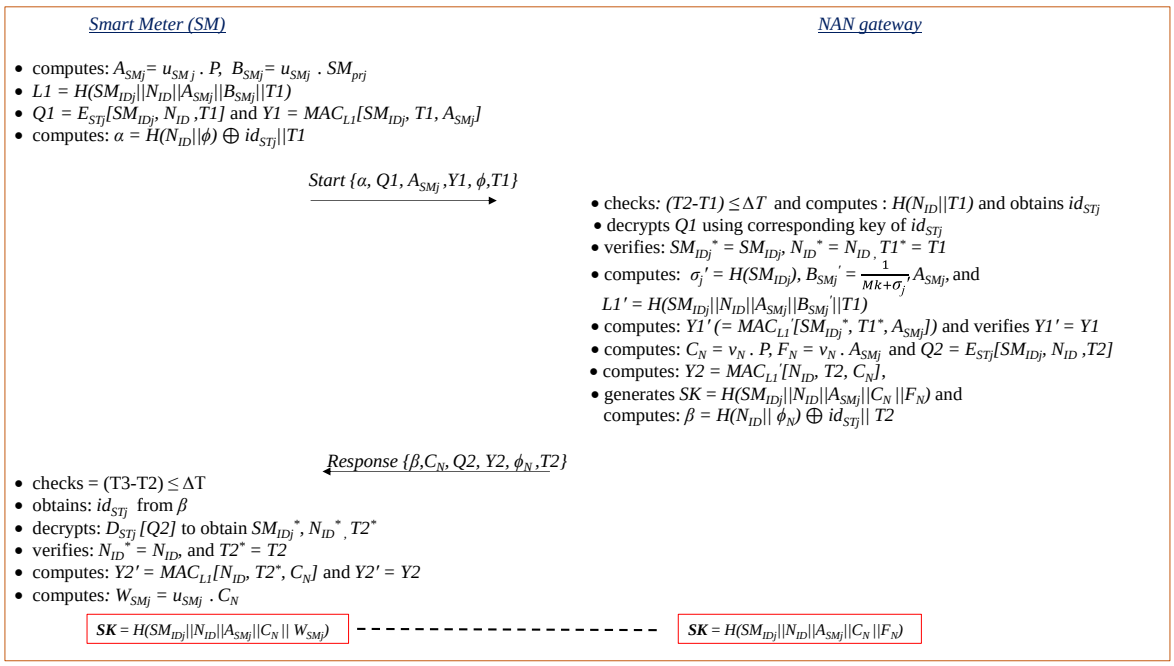

Fig. 2. Flow of the LAKA.

taking place in the protocol; (ii) *composition role*, describes the session in which legitimate entities are communicating; and (iii) *environment role*, details the global parameters, sessions and an intruder knowledge in the protocol. Moreover, the tool utilizes the *channel(dy)* to exploit the Dolve-Yao model [31].

1) ***Specifying LAKA in HLPSL script****:* We describe the specification for the authentication and key establishment phase, where two basic roles are involved, i.e., smart meter (SM) and NAN gateway. In addition, the proposed scheme has another two roles involved, namely, session and environment. Fig. 3 represents the role specification of the smart meter – the receive (RCV) signal starts initial state, i.e., 0 and changes state to 1. It (i.e., smart meter) then sends $\{alpha', Q1', A_{SM_j}', Y1', \phi, T1'\}$ using SND signal to the NAN. In State 3, using RCV signal the smart meter receives a message $\{beta', (vN' \cdot P), [SM_{ID_j}, N_{ID}, T2']_{ST}, H(N_{ID}, T2', C_N'), \phi_N, T2\}$ from the NAN. Similarly, Fig. 4 represents the role specification of the NAN gateway – at initial state (i.e., 0), RCV signal receives a message (i.e., $\{alpha', Q1', A_{SM_j}', Y1', \phi, T1'\}$) from the smart meter. Now it changes state to 1 and then SND signal sends $\{beta', (vN' \cdot P), [SM_{ID_j}, N_{ID}, T2']_{ST}, H(N_{ID}, T2', C_N'), \phi_N, T2\}$ to the smart meter. Upon specifying the basic roles (i.e., smart meter and NANGateway), we now specify the session role of LAKA, as shown in Fig. 5. The session role includes the parametrized instantiation of the basic role, e.g., *SmartMeter(SM NAN, SK, H, SM_S, SM_R)* and *NANGateway(SM NAN, SK, H, NAN_S, NAN_R)*. The *channel (dy)* means that all the messages sent by the SmartMeter and NANGateway are also going to the attacker.

Finally, Fig. 6 describes the top-level role called environment. This role comprises of the global constants and also describes the construction of sessions in the protocol. Moreover, in this role, an attacker may participate as a legal agent since all the messages sent by the agents are also

```
role SmartMeter (SM, NAN : agent,
        SK, ST : symmetric_key,
        SMpub : public_key,
        H      : hash_func,
        RCV, SND : channel (dy) )
played_by SM def=
local State                 : nat,
      idST, SMid, Nid, P    : text,
      phi, phi_N            : text,
      T1, T2, SMpr          : text,
      Q1, Q2, Y1, Y2        : message,
      alpha, beta           : message,
      H                     : hash_func
Const SmartMeter_NAN_uSM, NAN_SmartMeter_vN: protocol_id,
 NAN_SmartMeter_Nid, SmartMeter_NAN_SMid : protocol_id,
 SmartMeter_NAN_T1,  NAN_SmartMeter_T2 : protocol_id,
SmartMeter_NAN_alpha, NAN_SmartMeter_beta : protocol_id,
 sub1, sub2, sub3 : protocol_id,
init  State := 0
transition
1. State = 0 /\ RCV (start) =|>
   State' := 1 /\ uSM' := new ()
             /\ T1' := new ()
             /\ ASM' := (uSM . P)
             .....
             .....
             /\ Y1' := H(L1, SMid,T1', ASM')
             /\ alpha' := xor(H(Nid,phi'), idST)
             /\ SND (alpha', Q1', ASM', Y1', phi', T1')
             /\ secret ({SMid, Nid}, sub1, {SmartMeter, NAN})
             /\ witness (SM, NAN, SmartMeter_SM_uSM,  uSM')
            % SmartMeter has freshly generated the value of uSM
             /\ witness (SM, NAN, SmartMeter_SM_uSM,  T1')
            % SmartMeter has freshly generated the value of T1
2. State = 3 /\ RCV (beta, (vN' . P), {Smid, Nid, T2'}_ST, H(Nid,T2',Cn'),
             phi'_N, T2') =|>
State' := 2  /\ WSM' := (uSM' . Cn')
             /\  SK := H3(SMid, Nid, ASM', Cn', WSM')
             /\ secret ({SMid, Nid}, sub1, {SmartMeter, NAN})
             /\ request (NAN, SmartMeter, NAN_SmartMeter_t2, T2')
            /\ request (NAN, SmartMeter, NAN_SmartMeter_vN, vN')
end role
```

Fig. 3. SmartMeter Specification in HLPSL.

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/TSG.2018.2857558, IEEE Transactions on Smart Grid


```
role NANGateway (SM, NAN : agent,
        SK : symmetric_key,
        ST : symmetric_key,
        SMpub : public_key,
        H       : hash_func,
        RCV, SND : channel (dy))
played_by NAN def=
local State                     : nat,
      idST, SMid, Nid, P        : text,
      phi, phi_N                : text,
      T1, T2, SMpr              : text,
      Q1, Q2, Y1, Y2            : message,
      alpha, beta               : message,
       H                        : hash_func
Const  SmartMeter_NAN_uSM, NAN_SmartMeter_vN: protocol_id,
 SmartMeter_NAN_SMid, NAN_SmartMeter_Nid: protocol_id,
 SmartMeter_NAN_T1, NAN_SmartMeter_T2: protocol_id,
SmartMeter_NAN_alpha, NAN_SmartMeter_beta : protocol_id,
 sub1, sub2, sub3 : protocol_id,
init  State := 0
transition
1. State = 0 /\ RCV (alpha', Q1', ASM', Y1', phi', T1') =|>
State' := 1     /\ {SMid, Nid, T1'}_ST
                /\ secret ({SMid, Nid}, sub1, {SmartMeter, NAN})
                .....
                .....
State' := 2 /\ SND (beta', (vN' . P), {Smid, Nid, T2'}_ST, H(Nid,T2',
                Cn'), phi'_N,T2')
               /\ secret ({SMid, Nid}, sub1, {SmartMeter, NAN})
                /\ witness (SM, NAN, NAN_SmartMeter_vN,  vN')
               % SmartMeter has freshly generated the value of vN
                /\ witness (SM, NAN, NAN_SmartMeter_t2,  T2')
               % SmartMeter has freshly generated the value of T2
end role
```

Fig. 4. NAN gateway Specification in HLPSL.

```
role session (SM, NAN : agent,
        SK : symmetric_key,
        ST : symmetric_key,
        SMpub : public_key,
        H : hash_func)
def=
local SM_S, SM_R, NAN_S, NAN_R : channel (dy)
composition
        SmartMeter (SM, NAN, SK, H, SM_S, SM_R)
        /\ SmartMeter (SM, NAN, SK, H, NAN_S, NAN_R)
end role
```

Fig. 5. Session role in HLPSL.

going to the attacker. In our specification the attacker is represented by constant 'i' who has initial *intruder knowledge* of the agent names, public keys, hash functions, etc. Moreover, one secrecy and four authentication goals have been initially verified, as follows: secrecy_of sub1, authentication_on authentication_on SmaterMeter_NAN_SMid, authentication_on NAN_SmartMeter_Nid, authentication_on SmaterMeter_NAN_T1, authentication_on NAN_SmaterMeter_T2.

*2) **Formal verification simulation results**:* LAKA is verified using the on-the-fly model checker (OFMC) backend, which is widely utilized by several schemes, e.g., [17], [22], [39], [40]. The OFMC verifies against the replay attack and the MITM attack with the bounded number of sessions. Fig. 7 depicts the verification results, i.e., *SAFE* from the Dolve-Yao attack model and *GOAL*s are achieved as specified.

```
role environment()
def=
Const SmartMeter, NANGatway: agent,
        SK : symmetric_key,
        ST : symmetric_key,
        SMpub : public_key,
        H: hash_func,
        SMid,Nid,uSM, vN, alpha, beta, t1, t2 : text,
        SmartMeter_NAN_uSM, NAN_SmartMeter_vN, : protocol_id,
        SmartMeter_NAN_SMid, NAN_SmartMeter_Nid : protocol_id,
        SmartMeter_NAN_T1, NAN_SmartMeter_T2 : protocol_id,
        SmartMeter_NAN_alpha, NAN_SmartMeter_beta : protocol_id,
        sub1, sub2, sub3 : protocol_id
intruder knowledge = {SmartMeter, NANGateway, H}
composition
        session (SmartMeter, NANGateway, H)
        /\ session (SmartMeter, i, H)
        /\ session (NANGateway, i, H)
end role

goal
secrecy_of sub1
% secrecy_of sub2
% secrecy_of sub3
authentication_on SmaterMeter_NAN_SMid
authentication_on NAN_SmartMeter_Nid
authentication_on SmaterMeter_NAN_T1
authentication_on NAN_SmaterMeter_T2
end goal
environment()
```

Fig. 6. Environment and goal in HLPSL.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/project/LAKA.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.07s
  visitedNodes: 12 nodes
  depth: 1000 plies
```

Fig. 7. Simulation verification output.

B. Informal security analysis under Dolve-Yao

The security of LAKA is built on the hardness of elliptic curve discrete logarithm problem (ECDLP), encryption and hashing algorithms and therefore it (LAKA) can safe against the popular attacks.

*1) **Replay attack**:* LAKA can resist the replay attack.

Replay attack at the NAN gateway: Assume that in the authentication and key establishment phase, an ill-intention adversary (i.e., Eve) eavesdrops communication from the SM to NAN gateway and captures *start* $\{\alpha, Q1, A_{SM_j}, Y1, \phi, T1\}$ message. To launch the replay attack at time (T_{eve_1}), an attacker can resend the message $\{\alpha, Q1, A_{SM_j}, Y1, \phi_{eve}, T_{eve_1}\}$ to the NAN gateway. Here eve_1 is Eve's time stamp. However, this message will be detected due to the verification of the time stamp, i.e., $(T2 - T_{eve_1}) \leq \Delta T$ at the NAN gateway. Moreover, assume that if the attacker go-through the time stamp verification, somehow, then he/she must need to provide u_{SMj} to compute $L1_{eve} = H(SM_{ID_j}||N_{ID}||A_{SM_j}||B_{SM_j}||T1)$ that

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/TSG.2018.2857558, IEEE Transactions on Smart Grid

is being used to verify $Y1 = MAC_{L1}[SM_{ID_j}, T1, A_{SM_j}]$. However, following the ECDLP assumptions, obtaining u_{SMj} is a hard problem. Furthermore, Eve cannot change the real time stamp in sub-message $Q1 = E_{ST_j}[SM_{ID_j}, N_{ID}, T1]$ since $Q1$ is ciphered with the encryption key (i.e., ST_j), which is only owned by the legal meter and NAN gateway. Thus the attacker replay message will be failed again (i.e., $T1^* \neq Teve_1$) at the NAN gateway.

Replay attack at the smart meter: Assume that if Eve eavesdrops on communication from the NAN gateway to meter and captures *Response* = $\{\beta, C_N, Q2, Y2, \phi_N, T2\}$ message. To launch replay attack at time (T_{eve_2}), the attacker could resend $\{\beta, C_N, Q2, Y2, \phi_{N_{eve}}, T_{eve_2}\}$ to the meter. Nevertheless, this message will be detected due to the time stamp verification, i.e., $(T3 - T_{eve_2}) \leq \Delta T$. Furthermore, to verify $Y2 = MAC_{L1'}\ [N_{ID}, T2, C_N]$, the attacker must have to provide v_N, which is not feasible due to the hardness of the ECDLP. Despite that, the sub-message $Q2 = E_{ST_j}[SM_{ID_j}, N_{ID}, T2]$ also contains the real time stamp, which cannot be changed without knowing the encryption key (ST_j). Thus the attacker replay message cannot be succeeded ($T2^* \neq Teve_2$) at the meter. Thus, the replay attack is thwarted.

*2) **Man-in-the-middle attack (MITM)**:* In this attack scenario, a hostile intruder (e.g., Eve) may intercept communication channels that connecting two legal parties and make believe them (i.e., SM and NAN gateway) that both are communicating directly with each other. Assume that Eve intercepts *start* $\{\alpha, Q1, A_{SM_j}, Y1, \phi, T1\}$ message and replaces it with $\{\alpha_{eve}, Q1, A_{SM_{eve}}, Y1_{eve}, \phi_{eve}, T_{eve1}\}$ to initiate the process of LAKA. This message however is not helpful for Eve, since $Y1$ is a keyed MAC, which is computed over $L1$. Note that Eve cannot attempt to generate true $L1$ that includes B_{SMj}, computed over long-term secret key of the meter SM_{pr_j}, which is not known to the attacker. Moreover, Eve has no way to alter $Q1 = E_{ST_j}[SM_{ID_j}, N_{ID}, T1]$ without knowing ST_j. Therefore, Eve cannot play as MITM.

Similar to aforementioned, assume that if Eve intercepts *Response* = $\{\beta, C_N, Q2, Y2, \phi_N, T2\}$ and replaces it with a fabricated message $\{\beta_{eve}, C_{N_{eve}}, Q2, Y2_{eve}, \phi_{N_{eve}}, T_{eve2}\}$. Likewise *start* message, Eve cannot compute right $Y2_{eve}$ and $Q2$. Thus, he/she cannot succeed to mount MITM.

*3) **Impersonation attack**:* In this attack, assume that Eve tries to impersonate as a legal meter to the NAN gateway. To do that, Eve randomly picks $u_{SM_{eve}}$ and computes $A_{SM_{eve}}$ using $u_{SM_{eve}} \cdot P$ and fabricates a false $B_{SM_{eve}}$. Eve then computes own messages, i.e., $L1_{eve} = H(SM_{ID_{eve}}||N_{ID}||A_{SM_{eve}}||B_{SM_{eve}}||T1_{eve})$ and $Y1_{eve} = MAC_{L1_{eve}}[SM_{ID_{eve}},\ T1_{eve}, A_{SM_{eve}}]$ and sends $\{\alpha_{eve}, Q1,\ A_{SM_{eve}}, Y1_{eve}, \phi_{eve}, T1_{eve}\}$ to the NAN gateway. However, the NAN gateway cannot obtained the real identity of the meter since it is encrypted in $Q1 = E_{ST_j}[SM_{ID_j}, N_{ID}, T1]$ therefore Eve's fake identity cannot be verified i.e., $(SM^*_{ID_j} \neq SM_{ID_{eve}})$. In addition, the NAN gateway cannot determine the correct $L1_{eve} = H(SM_{ID_{eve}}||N_{ID}||A_{SM_{eve}}||B_{SM_{eve}}||T1eve)$ due to the fabricated $B_{SM_{eve}}$ instead of $B'_{SM_j} = \frac{1}{M_k + \sigma'_j} A_{SM_j}$. Therefore $Y1 \neq Y1_{eve}$ will be detected.

Similarly, Eve cannot present as a legal NAN gateway to a meter because he/she does not possess the NAN's secret key M_k, ST_j and identity (N_{ID}). Therefore, it is not feasible to launch impersonation attack.

*4) **Attacks to Forward security (FS)**:* The FS refers – compromise of the long term keys (e.g., secret shared or private keys) of legitimate partners should not be disclosed the secrecy of old sessions and their keys. The FS mainly has two notations, (i) perfect forward security (PFS) and (ii) master-key forward secrecy(MFS). Here, PFS defines that if a compromise of long-term private key of either the legitimate parties (e.g., a SM or NAN gateway) should not be compromising secrecy of the previously established sessions. Whereas, MFS satisfies – whenever the master key of a legitimate entity is being compromised then the protocol should hold the security of session key. The proposed LAKA therefore holds both PFS and MFS properties. For instance, assume that if the long-term secret keys (e.g., (ST_j, SM_{prj}, M_k) of meter and NAN are exposed to Eve. However Eve still cannot determine the previous session keys because each previous session between the meter and NAN is computed independently and fresh i.e., $(SK = H(SM_{ID_j}||N_{ID}||A_{SM_j}||C_N||W_{SM_j})))$ that includes A_{SM_j} (= $u_{SM_j} \cdot P$), C_N (=$v_N \cdot P$) and W_{SM_j} (=$u_{SM_j} \cdot C_N$). Here u_{SM_j} and v_N are random numbers of the meter and NAN, respectively. In addition, with the fact of the ECDLP hardness, Eve cannot determine the real value of uSM and vN, which are random numbers. Therefore, the proposed scheme holds FS.

*5) **Smart meter key compromise impersonation**:* Typically, smart meters are deployed outside the homes in an open environment. Assume that if the attacker compromises a meter by damaging the physical box and tries to learn the secret. Eve can use these secrets to mount key compromise impersonation attack of other non-compromise smart meters. However, in LAKA, the compromise of a smart meter's secrets does not imply that the secrets of other non-compromised smart meters. Moreover, in our scheme, each smart meter has a shared token (ST_j), which is unique and shared with the NAN gateway. Therefore, such attack cannot work on LAKA.

*6) **Known session key attack**:* In the known key attack, Eve can intercept messages (e.g., *Start* and *Response*) in authentication and key establishment phase. Then he/she tries to obtain the session key from previous sessions. In such cases, it is paramount requirement that the security of current session key is remain secure. The proposed LAKA however is secure against known session key attack, since it establishes a shared session key (i.e., SK). Note that the security strength of SK relies upon the hardness/security of the one-way hash function and secrets. Therefore, with the fact of the output of one-way hashing, Eve cannot determine a relation with pre-images of the hash values and so the secrets.

*7) **Denial-of-Service (DoS) attack**:* To mitigate DoS threats is very challenging, since these threats can aim malicious activities at various level in the SENs. For instance, the attacker can mount a DoS attack by replaying old messages. However, the scheme proposed in this paper can mitigate to DoS attack to some extent. As described in the Section III.3, the proposed approach exploits the advantages of timestamps (e.g., $T1$ and $T3$, and $T2$) and random numbers (e.g., u_{SM_j} and v_N) of the

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/TSG.2018.2857558, IEEE Transactions on Smart Grid

TABLE II
SECURITY SERVICES COMPARISONS

	[14]	[17]	[19]	[20]	[21]	[22]	[23]	**LAKA**
Mutual authentication		√	√	√	√	√	√	√
Session-Key security		√	Weak	√	√	√	√	√
Message Integrity						√	√	√
Anonymity	√		√	√	√			√
Forward security		√	√	√	√	√	√	√
Protect replay attack	√	√	√	√	√	√	√	√
Impersonation attack safeguard					√	√		√
MITM attack protection		√			√	√	√	√
Safe from DoS attack								√

meter and NAN gateway, respectively. Therefore, the proposed scheme can resist such DoS attacks.

C. Security goals

*1) **Mutual authentication and key agreement**:* A mutual authentication is performed between the meter(SM_{ID_j}) and NAN gateway (N_{ID}). The NAN gateway authenticates SM by checking $SM^*_{ID_j} = SM_{ID_j}$, refers step B in Section III-3. Similarly, the SM authenticates to NAN gateway by checking $N^*_{ID} = N_{ID}$, thus, the proposed LAKA maintains mutual trust between the legitimate parties. Moreover, after performing mutual trust for each session, LAKA establishes a session key (SK). This session key agreement (SK) can provide subsequent secure communication to involved entities.

*2) **Confidentiality**:* To prevent eavesdropping threats, confidentiality is one of the highest requirement, which is recommended by the NIST security guidline, the readers may refer to [27]. In the energy network, the security of the protocol messages is as important as the data security (i.e., confidentiality). Otherwise the protocol messages may reveal many useful information, e.g., device identities, etc. Nevertheless, to avoid such eavesdropping threats, the proposed scheme exploits symmetric cryptosystems that provide confidentiality, e.g., $Q1 = E_{ST_j}[\ SM_{ID_j}, N_{ID}, T1]$, $Y1 = MAC_{L1}[SM_{ID_j}, T1, A_{SM_j}]$, $Q2 = E_{ST_j}[SM_{ID_j}, N_{ID}, T2]$ and $Y2 = MAC_{L1'}[N_{ID}, T2, C_N]$, refer to Section III-3. Moreover, each SM device possesses a unique secret token ST_j and its identifier id_{ST_j} in the tamper-proof memory. Here, ST_j is used to encrypt $H_{ID_j}, N_{ID}, T1$. Moreover, to decrypt $D_{ST_j}[Q1]$, the NAN gateway must possess corresponding key of id_{ST_j}, otherwise, it cannot decrypt the garbled message. Finally, the subsequent messages can be kept secure using the session key.

*3) **Integrity**:* Integrity is another main security property in the SG, which is recommended by the NIST security guidelines [27]. Assume that an adversary tries to alter the wireless messages during the transit. However, the proposed scheme prevents message alteration during the transit. As we can see from Step (A) in Section III-3, the SM device computes $Y1(= MAC_{L1}[SM_{ID_j}, T1, A_{SM_j}])$, which is computed over $L1$. Note that – $L1$ is computed by only the legitimate SM, therefore Eve cannot alter SM's messages when they are in transit. Likewise, the messages of NAN gateway are also protected with such integrity checks.

*4) **Anonymity**:* Assume that an adversary overhears on wireless packet and spoofs the identities, e,g., SM_{ID_j} and id_{ST_j} for own purpose. In our scheme, when a smart meter connects to the NAN gateway, it does not send SM_{ID_j} as a plaintext but hide the identity in $Q1 = E_{ST_j}[SM_{ID_j}, N_{ID}, T1]$. Moreover, it can be noticed from the proposed scheme that the pseudonymity of id_{ST_j} is being provided using α and β. Resultant, only the legitimate NAN gateway can learn the identity of meter by decrypting $Q1 = E_{ST_j}[SM_{ID_j}, N_{ID}, T1]$ using the secret token (ST_j). Thus, it achieves identity anonymity and protects from identity spoofing attack.

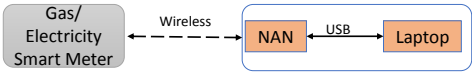

Fig. 8. Experimental Setting.

TABLE III
EXECUTION TIME *(in* ms*)*

	Point multiplication	Encryption	Decryption	Hash	MAC
time	2,900	3.8	41.1	39	8.6

In addition, the comparison on security services among [14], [17], [19]–[23] and the proposed scheme is given in Table II. We can notice that the proposed LAKA can provide more security services than previously proposed ones.

V. PERFORMANCE ANALYSIS

Experimental setup: As shown in Fig. 8, consider a SMI network, where a (gas or electricity) smart meter (SM) communicates with the NAN gateway over wireless channels. We used TelsoB mote as a SM equipped with a 16 bit processor runs at a clock frequency 8 MHz, 48 KB of ROM and 10 KB of RAM, and 2AA battery powered [41]. The laptop is used as the NAN gateway (e.g, Intel 2.59 GHz, and 16 GB of RAM). Note that in this paper we measure the computational and communicational energy costs only for the smart meter, as it is a resource-constrained meter. We intentionally omitted the computation and communication energy costs for the NAN gateway since it is a resource-rich system, which can execute cryptographic operations much faster compared to a SM.

For the ECC computations, we used TinyECC library [42] [43] which supports all operations, including point addition, point doubling and point multiplication, exponentiation operations for the TelsoB device. In our experiment settings, we used MD5 function for one-way hashing as the base hash functions. For encryption, the AES (Advanced Encryption Standard) symmetric-key algorithm has been used, which is

TABLE IV
ENERGY COSTS FOR CRYPTOGRAPHIC OPERATIONS AT SMART METER

Operations at SM	Energy costs *(in* µJ*)*
Point multiplication	15,660
Encryption	20.52
Decryption	221.94
Hash (MD5)	210.6
MAC	46.44
Total computational energy costs *(in* µJ*)*	$\approx$ 16,160

integrated in MSP430s CC2420 radio. The MAC operation is computed via cipher block chaining (CBC).

Computation cost: In order to measure the computation cost, following message sizes have been used for authentication and key establishment phase (Section III). For instance, IDs = 1 byte, hashing = 16 bytes, pseudo random number = 8 bytes, MAC = 4 bytes, time stamp = 4 bytes, key size = 16 bytes and we choose to exploit secp160r1 defined over a 160-bit prime field. Therefore, the length of messages in LAKA, i.e., *start* = $\{\alpha, Q1, A_{SM_j}, Y1, \phi, T1\}$ and *Response* = $\{\beta, C_N, Q2, Y2, \phi_N, T2\}$ are 68 and 68 bytes long, respectively. Table III shows the execution time (t) taken by the proposed scheme for each operation, e.g., a point multiplication takes 2,900 ms, AES takes 3.8 ms, and hash and MAC operation requires 39 ms and 8.6 ms, respectively. Moreover, we evaluate energy-efficiency considering, for example, smart gas meters which are incorporated in the SMI by the energy companies, such as EDF energy [44], Scottish Power [45], etc. The meter (e.g., gas [26]) is running on battery-powered, where energy-efficiency is a prime concern. However, to evaluate energy efficiency – we consider energy price of cryptographic primitives on the SM. By using voltage (Vol), current ($Curr$) and time (t), i.e., $Vol \times Curr \times t$, we can calculate the energy incurred by cryptographic operations. Here, Vol is the battery (AA) voltage, $Curr$ is the electric charge, and t is the execution time for a cryptographic operation. Without loss of generality, $Vol = 3$ V and $Curr = 1.8$ µA values are taken from the (TelosB) data-sheet [41]. Table IV shows the sum of computational energy consumed by LAKA is $\approx$ 16,160 µJ.

Finally, the comparisons on total computational cost among LAKA and other schemes, such as [17], [19]–[23] are given in Table V. It can be noticed from Table V, the proposed LAKA is more akin than the protocol proposed in [22] by $1t$, but the total computation cost of the proposed scheme is less than the others. However, the proposed LAKA can provide more security services as shown in Table II.

Communication cost: The proposed scheme needs two communication exchanges (*Start* and *Response*) from a smart meter to the NAN gateway and vice-versa, as shown in Fig. Fig. 2. Whereas the schemes proposed in [17], [19], [20], [21], [23] required three communication rounds to establish a session key. Moreover, the data transmission and reception are expensive in terms of energy, for instance transmitting one-bit over a wireless channel needs more energy than computing one-bit. To calculate the communication cost, Meulenaer el al's communicational model has been used in this paper, where sending and receiving one-bit needed 0.72 µJ and 0.81 µJ, respectively, for a TelosB mote.

For the comparison purposes, Table VI shows that how many number of bits are transmitted and received at smart meter in [19], [20], [21], and [23]. Moreover, considering the Meulenaer el al's communicational model, the schemes proposed in [19], [20], [21], [23] required ≈ 2572µJ, ≈ 1443µJ, ≈ 1247µJ and ≈ 4850 µJ, respectively, energy to send and receive the messages.

On the contrary, in the proposed LAKA, a battery-powered smart meter required ≈ 832 µJ energy to send and receive the messages. Hence, we conclude that the proposed LAKA is a lightweight scheme than [19]–[21], [23], and it can be suitable for the resource-constrained smart gas meter and smart electricity meter in the SMI.

VI. CONCLUSION

This paper has proposed a comprehensive lightweight security scheme for smart energy networks. The proposed LAKA protocol achieves two-way authentication between a remote SM and a NAN and obtains proper session key agreement for securing data communications. Security analysis has been presented using the AVISPA tool. Moreover, our informal security analysis indicated that the proposed LAKA fulfilled the NIST model security requirements. Finally, the test-bed results have shown that this scheme can improve communicational and computational efficiency than the other schemes.

ACKNOWLEDGMENT

Pardeep Kumar and Andrew Martin's work was supported by a grant from the UK EPSRC EP/N020170/1 (Security and Privacy in Smart Grid Systems: Countermeasure and Formal Verification); A. Gurtov was supported by the Center for Industrial Informatics (CENIIT); and P. H. Ha was supported the Research Council of Norway (PREAPP project, grant no. 231746/F20 and eX3 project, grant no. 270053).

REFERENCES

[1] N. Saxena and B. J. Choi, "State of the art authentication, access control, and secure integration in smart grid," *Energies*, vol. 8, no. 10, pp. 11 883–11 915, 2015.
[2] "German energy blog," http://www.germanenergyblog.de/?p=11635.
[3] "European smart metering landscape report," http://www.escansa.es/usmartconsumer/documentos/USmartConsumer_European_Landscape_Report_2016_web.pdf.
[4] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.
[5] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: issues, challenges and countermeasures," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 4, pp. 1933–1954, 2014.
[6] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.
[7] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1732–1745, 2015.
[8] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 75–86, 2013.
[9] "Analysis of the Cyber Attack on the Ukrainian Power Grid ," https://ics.sans.org/media/E-ISAC˙SANS˙Ukraine˙DUC˙5.pdf.

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/TSG.2018.2857558, IEEE Transactions on Smart Grid

TABLE V
COMPUTATION COST COMPARISONS AT SMART METER AND NAN GATEWAY

Schemes	Smart meter	NAN gateway	Total costs
[17]	$3t_{exp} + 8H + 1_{SV} + 2AS_{ED}$	$3t_{exp} + 7H + 1_{SG} + 2AS_{ED}$	$6t_{exp} + 15H + 1_{SG} + 1_{SV} + 4AS_{ED}$
[19]	$4t + 1t_{add} + 1t_{exp} + 5H$	$3t + 2t_{bp} + 1t_{add} + 1t_{exp} + 5H$	$7t + 2t_{bp} + 2t_{add} + 2t_{exp} + 10H$
[20]	$3t + 3t_{add} + 1t_{exp} + 6H$	$2t + 2t_{bp} + 3t_{add} + 1t_{exp} + 6H$	$5t + 2t_{bp} + 6t_{add} + 2t_{exp} + 12H$
[21]	$4t + 1t_{add} + 5H$	$6t + 2t_{add} + 6H$	$10t + 3t_{add} + 11H$
[22]	$2t + 3H$	$3t + 4H$	$5t + 7H$
[23]	$1H + 1MAC + 2S_{ED} + 3AS_{ED}$	$1H + 1MAC + 2S_{ED} + 3AS_{ED}$	$2H + 2MAC + 4S_{ED} + 6AS_{ED}$
LAKA	$3t + 4H + 2MAC + 2S_{ED}$	$3t + 5H + 2MAC + 2S_{ED}$	$6t + 9H + 4MAC + 4S_{ED}$

t - point-multiplication; t_{bp} - bilinear pairing; t_{add} - point addition; t_{exp} - exponentiation operation; H - one-way hash function; S_{ED} - encryption and decryption; AS_{ED} - asymmetric encryption and decryption;SG - signature generation; SV - signature verification; MAC - message authentication code.

TABLE VI
COMMUNICATION COSTS IN [19], [20], [21], [23] AT SMART METER *(in* µJ*)*

Smart meter	[19]	[20]	[21]	[23]	**LAKA**
Send	2240×0.72	1248×0.72	832×0.72	3712×0.72	544×0.72
Receive	1184×0.81	672×0.81	800×0.81	2688×0.81	544×0.81
Total energy costs *(in* µJ*)*	≈ 2572	≈ 1443	≈ 1247	≈ 4850	≈ 832

[10] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 907–921, May 2016.

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

[12] E. Ayday and S. Rajagopal, "Secure device authentication mechanisms for the smart grid-enabled home area networks," Tech. Rep., 2013.

[13] D. He, S.-C. Chan, Y. Zhang, M. Guizani, C. Chen, and J. Bu, "An enhanced public key infrastructure to secure smart grid wireless communication networks," *Network, IEEE*, vol. 28, no. 1, pp. 10–16, 2014.

[14] T. W. Chim, S. M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, Jan 2015.

[15] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *Systems Journal, IEEE*, vol. 8, no. 2, pp. 655–663, 2014.

[16] M. Nabeel, S. Kerr, X. Ding, and E. Bertino, "Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012, pp. 324–329.

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

[18] Y. Yan, R. Hu, S. K. Das, H. Sharif, and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *Network, IEEE*, vol. 27, no. 4, pp. 64–71, 2013.

[19] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.

[20] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[21] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications*, vol. 10, no. 14, pp. 1795–1802, 2016.

[22] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. M. Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[23] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon, and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector," *Computers & Electrical Engineering*, vol. 52, pp. 114–124, 2016.

[24] Y. Chen, J.-F. Martnez, P. Castillejo, and L. Lpez, "An anonymous authentication and key establish scheme for smart grid: Fauth," *Energies*, vol. 10, no. 9, 2017.

[25] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[26] "Texas instruments: Power solution for battery operated meters with 30-dbm wm-bus at 169 mhz," http://www.ti.com/lit/ug/tiduad5/tiduad5.pdf.

[27] https://www.nist.gov/sites/default/files/documents/smartgrid/NIST-SP-1108r3.pdf.

[28] "The smart security behind the GB Smart Metering System," https://www.ncsc.gov.uk/articles/smart-security-behind-gb-smart-metering-system.

[29] A. J. Paverd, "Enhancing communication privacy using trustworthy remote entities," Ph.D. dissertation, University of Oxford, 2015.

[30] C.-M. Yu, C.-Y. Chen, S.-Y. Kuo, and H.-C. Chao, "Privacy-preserving power request in smart grid networks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 441–449, 2014.

[31] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, Mar 1983.

[32] "Smart grid cyber security potential threats, vulnerabilities and risks," http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf.

[33] N. Saxena, B. J. Choi, and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid," *IEEE transactions on information forensics and security*, vol. 11, no. 5, pp. 907–921, 2016.

[34] S. Rinaldi, D. D. Giustina, P. Ferrari, A. Flammini, and E. Sisinni, "Time synchronization over heterogeneous network for smart grid application: Design and characterization of a real case," *Ad Hoc Networks*, vol. 50, pp. 41 – 57, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S157087051630097X

[35] R. Onica, N. F. Neves, and A. Casimiro, "Fault-tolerant precision time protocol for smart grids," in *Proceedings of the 7th Simposio de Informatica (INFORUM)*, Covilha, Portugal, 2015.

[36] H. Debiao, C. Jianhua, and H. Jin, "An id-based client authentication with key agreement protocol for mobile client–server environment on ecc with provable security," *Information Fusion*, vol. 13, no. 3, 2012.

[37] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[38] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *International conference on computer aided verification*. Springer, 2005, pp. 281–285.

[39] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 968–979, April 2017.

[40] A. K. Das, "A secure and effective biometric-based user authentication

scheme for wireless sensor networks using smart card and fuzzy extractor," *Int. J. of Communication Systems*, vol. 30, no. 1, 2017.
[41] "TelosB datasheet," www.willow.co.uk/TelosB˙Datasheet.pdf.
[42] "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," http://discovery.csc.ncsu.edu/software/TinyECC/.
[43] L. Marin, A. Jara, and A. S. Gomez, "Shifting primes: Optimizing elliptic curve cryptography for 16-bit devices without hardware multiplier," *Mathematical and Computer Modelling*, vol. 58, no. 5, pp. 1155–1174, 2013.
[44] https://www.edfenergy.com/.
[45] www.scottishpower.co.uk.