JOURNAL OF OPTOELECTRONICS LASER ISSN: 1005-0086

Volume 41 Issue 8, 2022

A D2D Communication Based Lightweight Customer Side Data Securing Scheme in Smart Grids

Bakhe Nleya[1] & Philani Khumalo[2]

[1&2]Department of Electronic and Computer Engineering, Durban University of Technology, Durban, South Africa

ABSTRACT

With the emergence of modernized power grids into smart equivalents referred to as smart grids (SGs) the bulk generation, transmission, distribution, and end-user infrastructures must be appropriately long-term planned concurrently with the required privacy and security. Notably, the objectives of modern SGs are to minimize power energy losses through theft or physical dissipation. The embedded device-to-device (D2D) communication technology in 5G networks will enable an affordable fail-safe ICT subsystem platform for the SGs. However, Privacy preservation is necessary for D2D services in SGs. In this paper, we propose an anonymity privacy-preserving, and data aggregation scheme. We carry out both security and performance and obtained theoretical analysis and simulation results the privacy algorithm is effective and at the same time, fewer communication overheads are exchanged.

Keywords: lightweight encryption, smart grid, NTRU cryptosystem, computational load, communication overheads.

I. INTRODUCTION

Future SGs can be regarded as the "next generation "of engineered power systems blended with ICT technologies to hence their operational efficiencies and reliability. In a way, various entities are networked together to monitor, control, and regulate such a power system. . The emergence of Fog-cloud computing paradigms and related models has contributed immensely towards running SG-related services efficiently. Various entities such as smart metering, and sensor/data aggregation typically generate large volumes of data for data analysis and inferences that would further enhance the SG's efficiency. This is because the acquisition of key data from various sensors, and systems assist it in making smart decisions, However, challenges arise, regarding security and privacy, [1, 2].

In this section, we describe a security and privacy framework for SGs. The framework is based on the Fog-Computing paradigm [3, 4,5]. It also rather uses a public network infrastructure, namely IoT, and thus will also take advantage of the use of new 5G network technologies such as D2D communication. In proposing such a framework, we are also taking into consideration current cyber security trends: We summarily list these trends as follows:

- The SG cyber-attack surface has expanded thus necessitating data security automation.
- An adoption of multi-layered as well as multi-factor authentication to enhance privacy. The adoption of new cybersecurity technology stack trends This trend in development means the cybersecurity technology stack gives guidance on the architecture framework needed to secure both privacy and security.
- Some SG elements and devices are mobile and hence this necessitates mobile software security enhancements.
- Periodic cybersecurity awareness training will ensure that both manufacturers and utility operators operate at the same pace and direction in combating security threats and vulnerabilities in modern SGs [6,7].

Illustrated in Fig. 1 is a Fog-Computing paradigm. The key entities would be the smart grid objects and sensors, Fog servers deployed within the vicinity of the clustered objects, devices, and elements constituting the SG. Finally, we have a centralized cloud server. The Fog layer is necessary to improve round trip response times for some of the SG's services and applications. Overall, the proposed approach (i.e Fog-cloud paradigm) approach has taken into consideration of the resources-constrained nature of some of the elements, devices, and objects constituting the SG infrastructure.

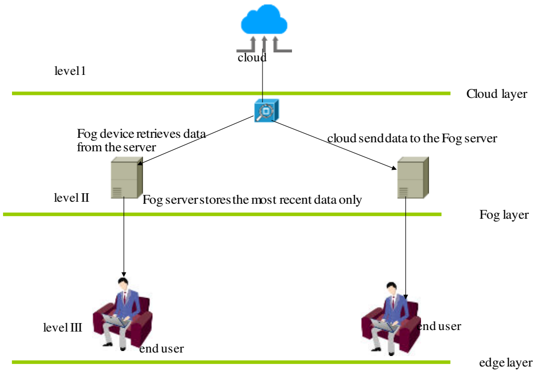

Fig. 1, Typical cloud-fog computing architecture

To provide privacy as well as security in surveillance secure, secure authentication and key exchange among the D2D communication compliant SG devices, elements, and objects, [7, 8, 9]. We make an overall assumption that the 5G network has evolved sufficiently enough At the SG base level, we will assume that all SG-associated devices, elements, and entities are under the coverage of 3GPP IoT-enabled network architecture as illustrated in Fig. 2.

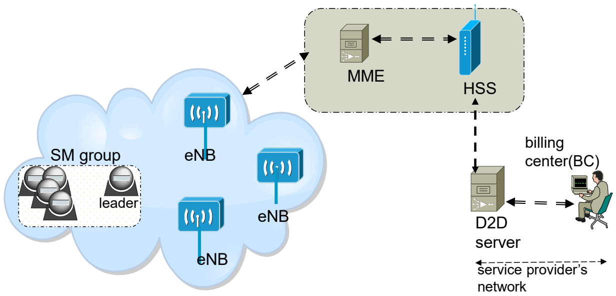

Fig. 2, 3GPP coverage in an SG network[8]

By default attributes information of the various elements, devices and objects are retained by the HSS. It also relies on the MME to verify each unit by way of granting a set of authentication tokens [10,11]].

Our model framework will focus on both security and privacy preservations in the SG. Hence three components of the framework providing for data security, data aggregation, and privacy authentications will together provide complete security in the SG. We discuss and evaluate each of these in the next three sections.

II. RELATED WORKS

Security: In [12] the authors analyzed general security challenges in various parts of SGS. Case studies are carried out herein regarding the key components such as renewable generation, low and high-frequency transmission of power, distribution as well as billing in the customer side networks. Also discussed herein are cryptographic-based countermeasures that include, authentication, key distribution, and management in different sections of an SG.

Likewise, in [152 the authors focus on SG and smart home security, and in particular the interactions between the SG and HANs. After categorizing various security threats, they also evaluate theoretical impacts. Furthermore, key security countermeasures are suggested. These include authentication and general physical security. However, the work did not provide any critical comparative analysis of the then existing schemes.

Security in respect of data-driven approaches is discussed in [13] The data-driven approaches include, data acquisition, data storage, data generation, and data processing security. Various security analytics techniques, such as data mining, statistical methods, and visualization are discussed. Whereas the work sounded quite extensive, it however falls short of further evaluating adverse implications and other complexities in terms of deployment in existing SG . SMs and data intelligence techniques for future energy systems are discussed in [14]. Intelligence tools such as support vector machines and fuzzy logic are explored. The whole idea was to elevate intelligence in SMs to detect any abnormalities in real-time. Typical examples explored herein included end-user profiling and load forecasting.

However, the authors fall short of relating the detection of abnormalities, end-user profiling, and load forecasting to the enhancement of security.

Cyber-physical attacks are discussed in [15,16]. In particular attack scenarios on various sections and entities of SGs are exemplified. Counter measures such as protection, detection, and mitigation are considered. However, no comparative analysis of the various counter measures is carried out hence extending this work would be a key step. The authors in [16] discuss cyber-attacks in IoT-enabled networks and related environments. They exemplify as well as model a threat vector that can be utilized by adversaries in attacking various IoT devices and elements. In this same work, the authors point out at hidden IoT-enabled attack paths. The work, however, falls short of providing in-depth mitigation of would-be feasible counter measures.

III. PROPOSED SECURITY AGGREGATION MODEL

The scheme takes into cognizance the fact that some of the elements involved are resource-constrained hence a lightweight form approach is chosen. In that way-SG messages will be delivered with absolute security guarantees, at low computational complexities and loads since most of the devices are constrained in terms of both power and computational memory.

Preliminaries

In this subsection, we define a few parameters that would be utilized in modeling the scheme as follows:
N – the number of plaintext vectors.
r – a value characterizing the ring of vectors.
l – the total number of operations.
n – non-hard disturbed matrices of a public key'

Next, we generate $l_o = n \times N \times \varepsilon_{\max} + (N-1) \times r$, and $q = 2 \times l_o \times (2l+1)$, subject to $p = q \times r \times \varepsilon$ being prime and $\varepsilon < l_o$.

We further generate two matrices $\mathbf{A}$ and $\mathbf{B}$ of size $N * N$ over $GF(p)$ such that $\mathbf{M} = [\mathbf{A}|\mathbf{B}]$. This is followed by defining a scrambler matrix Δ of size $N * N$ over the same $GF(p)$.

By generating a noise matrix $\mathbf{D}_i$ for $i \in 1,2,...n$, we can subsequently compute a distributed matrix

$$M_i = [A_o|B_i + D_i\Delta] \quad (1)$$

Like wise we can compute a hard noise matrix;

$$M_o = [A_o|B_o + D_o\Delta] \quad (2)$$

By selecting a permutation $P(.)$, we can compute;

$$M_i = P(M_i),\ i \in \{1,2,..., n\} \quad (3)$$

From all this, we can deduce that the public key is defined by the $n+1$ matrices $\{M_o, M_1,..., M_n\}$ alongside Δ .
We can now define both ciphering and deciphering as follows:

Cyphering

Let a message be defined vectorially as $m \in Z_r^N$ and noise as M_o . If we and a scrambling sequence mM_o to a set of n noise vectors $\sum_i r_i * M_i$, where $r_i < \varepsilon_{\max}$ and $n <_{\max}$

$$c = mM_o + \sum_{i=1}^{n} r_i * M_i \quad (4)$$

Deciphering

This is achieved by way of filtering the previously added noise sequences. In short, the permutation is reciprocated as :

JOURNAL OF OPTOELECTRONICS LASER ISSN: 1005-0086
Volume 41 Issue 8, 2022

$$\dot{c} = P^{-1}(c),\ c \in GF(p)^{2N} \qquad (5)$$

The targeted destination computes the scrambled noise as:

$$e = \dot{c}_D - \dot{c}_U\ A^{-1}B \qquad (6)$$

In the last equation $\dot{c}_D, \dot{c}_U$ are non disturbed and disturbed halves of $\dot{c}$ respectively

$$\dot{e} = e\Delta - 1 \qquad (7)$$

We also have;

$$\ddot{e}_j = \dot{e}_j - \mu \quad \forall\ \dot{e} = \left[\dot{e}_1{}', \dot{e}_2, ..., \dot{e}_N\right] \qquad (8)$$

For;

$$\mu = \begin{cases} \dot{e}_j \bmod q & \dot{e}_j \bmod q < \frac{q}{2} \\ \left(\left(\dot{e}_j \bmod q\right) - q\right) & \text{otherwise} \end{cases} \qquad (9)$$

Subject to $m_j = \ddot{e}_j q^{-1}$ and $i \in \{1, 2, ..., N\}$, $m = (m_1, m_2, ... m_N)$

Process Scheme Model

For simplicity's sake, in the interim, we will first assume that a dedicated secured connection is established between the control canter (CC) and APs via SMs and BSs.

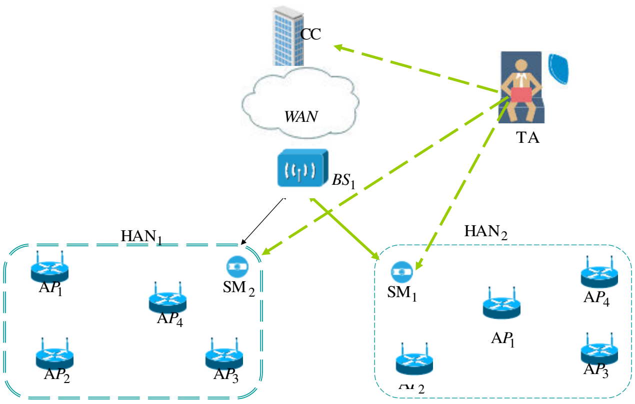

Fig. 3, Model configuration

We can thus elaborate on two distinct phases characterizing the operation, initialization and actual data aggregation.

Initialization

As is similar to the procedure, followed in chapter 3, the TA assigns public and private keys to all parties

For the CC, if M_{cc0} is the scrambling noise, and $\{M_{c1}, M_{cc2}, ..., M_{ccn}\}$ a set of n softened noise sequences, then public keys are:

$$\{M_{cc0}, M_{cc1}, ..., M_{ccn}\} \qquad (10)$$

The private keys will be;

$$P_{cc}(\bullet), M_{cc}, \Delta_{cc} \qquad (11)$$

For the BS similarly we have;

M_{bs0} is the scrambling noise , whilst $\{M_{bs1}, M_{bs2}, ..., M_{bsn}\}$ is a set of n softened noise sequences, then public keys are:

$P_{bs}(\bullet), M_{bs}, \Delta_{bs}$ (12)

For an individual SM

M_{sm0} is the scrambling noise, whilst $\{M_{sm1}, M_{sm2}, ..., M_{smn}\}$ a set of n softened noise sequences, then the private keys will be;

$P_{sm}(\bullet), M_{sm}, \Delta_{sm}$ (13)

Each AP has its own ID (AP_i) and it encrypts it before safely storing it:

$$ID_{j-enc} = ID_j * M_{sm0} + \sum_i r_i * M_{sm_i} \quad (14)$$

Data Aggregation : *(*At HAN level)

As already stated, each household has a HAN ., thus each AP ciphers its read data $m_j = (m_1, m_2, ..., m_w)$ according to;

$$c_j = m_j M_{cco} + \sum_{i=1} r_i * Mcc_i \quad (15)$$

It now dispatches it to the AP for the current reading cycle. The receiving AP aggregates the read data homomorphically;

$$c = \sum_j c_j \quad (16)$$

Ultimately it encrypts the aggregated data and relays it to the SM

$$AP_s \xrightarrow{c, ID_{s-enc}} SM \text{ .} \quad (17)$$

The SM will in turn validate and time stamp before sending it off to a BS . E.g this proceeds as follows:

The timestamp is T_v and nonce comprises $\mathbf{f}$ vectors.

$$x = c \| \mathbf{T_v} \| \mathbf{f} \quad (18)$$

$$\dot{x} = P_{sm}^{-1}(x) \quad (19)$$

$$e = \dot{x}_D - \dot{x}_U \mathbf{A}_{sm}^{\mathbf{-1}} \mathbf{B_{sm}} \quad (20)$$

$$\dot{e} = e \Delta_{sm}^{-1} = \left[\dot{e}_1 ', \dot{e}_2 ,..., \dot{e}_N \right] \quad (21)$$

For each $\dot{e}_j , i \in \{1,2,..., N\}$ the SM must calculate;

$$\mu = \begin{cases} \dot{e}_j \bmod q & \dot{e}_j \bmod q < \frac{q}{2} \\ \left(\dot{e}_j \bmod q \right) - q & \text{otherwise} \end{cases} \quad (22)$$

Subject to;

$$y_j = \ddot{e}_j q^{-1}, i \in \{1,2,..., N\} \quad (23)$$

and,

$$Y = (y_1, y_2, \ldots y_N) \quad (24)$$

Once accomplished the relaying is completed thus:

$$SM_s \xrightarrow{c, ID_{s-enc}} BS \quad (25)$$

Data Aggregation : *(*At BS level)
The SM's signature is validated by checking both T_v and $\mathbf{f}$ before extracting the message;

$$x = Y * M_{smo} + \sum_{i=1} r_i * Msm_i \quad (26)$$

It now aggregates the read data coming from various SMs homomorphically;

$$C = \sum_k c_k \quad (27)$$

Next it ciphers the aggregated power consumption of the area using its private key;

$$P_{bs}(*), M_{bs}, \Delta_{bs} \quad (28)$$

$$g = c \| \mathbf{T}_w \| q \quad (29)$$

$$\dot{g} = P_{bs}^{-1}(g) \quad (30)$$

$$w = \dot{g}_D - \dot{g}_U \mathbf{A}_{bs}^{-\mathbf{1}} \mathbf{B}_{bs} \quad (31)$$

$$\dot{w} = e\Delta_{bs}^{-1} = \left[\dot{w}_1', \dot{w}_2, \ldots, \dot{w}_N \right] \quad (32)$$

For each $\dot{e}_j, i \in \{1, 2, \ldots, N\}$ the SM must calculate;

$$\mu = \begin{cases} \dot{w}_j \bmod q & \dot{w}_j \bmod q < \frac{q}{2} \\ \left(\dot{w}_j \bmod q \right) - q & \text{otherwise} \end{cases} \quad (33)$$

Subject to ;

$$d_j = \ddot{w}_j q^{-1}, i \in \{1, 2, \ldots, N\} \quad (34)$$

and;

$$Y = (y_1, y_2, \ldots y_N) \quad (35)$$

Once accomplished it relays the encrypted data to the CC

$$BS_s \xrightarrow{c, ID_{bsenc}} CC \quad (36)$$

The CC ultimately receives the aggregated power consumption data from BS and likewise validates it;

$$\dot{c} = P^{-1}(c) \quad (37)$$

$$s = \dot{c}_D - \dot{c}_U A_{cc}^{-1} B_{cc} \quad (38)$$

$$\dot{s} = s\Delta_{cc}^{-1} = \left[\dot{s}_1', \dot{s}_2, ..., s_N\right] \quad (39)$$

Once again for each $\dot{s}_k$, $k \in \{1,2,..., N\}$ the CC calculates;

$$\mu_o = \begin{cases} \dot{s}_k \bmod q & \dot{s}_k \bmod q < \frac{q}{2} \\ \left(\dot{s}_{kj} \bmod q\right) - q & \text{otherwise} \end{cases} \quad (40)$$

Subject to;

$$m_k = \ddot{s}_k q^{-1}, k \in \{1,2,..., N\} \quad (41)$$

and,

$$m = (m_1, m_2, ... m_N) \quad (42)$$

Requests for power reallocations

For security purposes, consumption for each defined domain is approximated in advance, and only when demand exceeds this projected value, will a AP request additional power. This is done via the SM and BS. The following are the secured procedures that the AP_j takes in sending this request R to the CC;

It encrypts its ID by time stamping it with value T_d and nonce L;

$$n_j = R \| ID_{j-enc} \| T_d \| L. \quad (43)$$

It further encrypts n_j using the control canter's a public key;

$$z_j = n_j * M_{cco} + \sum_{i=1} r_i * Mcc_i \quad (44)$$

The message will in turn be signed by the BS en route to the CC.

IV. ANALYSIS

The analysis of the efficacy of this framework's lightweight aggregation schemes is determined by both its security and performance. We thus will commence this section with a security analysis.

Security Analysis

During the data aggregation analysis, the scheme has the objective of satisfying both security as well as privacy. In summary, it must ensure data security as well as preserve confidentiality and message integrity.

Privacy: The scheme conceals the finer details of power consumption from units such as $HANs$, SMs and BSs. By this, we mean that each end user's daily power consumption is concealed from all these units, such that even if attackers intercepted the message(s), they will not be able to extract the semantics as they are encrypted. The same applies to APs as they receive the individual readings in ciphered form. Subsequently, the use of encrypted IDs also means that APs and other entities would not find it easy to decipher the real identities of end-users. Peer APs will are only restricted to knowing the aggregated reading of each other, but not the finer detail. It is also important to point out that the aggregated data relayed by APs is encrypted and only CC has the decryption keys. As already outlined earlier $HANs$, SMs and BSs are relaying agents and not capable of extracting the semantics of the aggregated messages.

JOURNAL OF OPTOELECTRONICS LASER ISSN: 1005-0086

Volume 41 Issue 8, 2022

Authenticity and Messages' Confidentiality and Integrity

The nature and manner in which encryption/decryption keys are assigned is such that only authorized parties can decrypt (decipher) messages. E.g as earlier alluded to, $HANs$, SMs and BSs act as relay agents and only the CC has decryption keys that were provided(generated) TA from the onset. In that way, authenticity, confidentiality as well as integrity are maintained. Note that the use of time stamping together with signatures also makes it impossible for attackers to forge signatures to intercept the data messages.

Data Security

Over and above, measures already discussed, the framework utilizes a crypto-system based on the hidden lattice problem, thus considered to be hard. With this cryptosystem, no entity can extract the semantics of the original lattice from its disturbed version.

Performance Analysis

Communication loads

During a single data aggregation process, a minimal number of messages is exchanged. Moreover, cognizance is taken of the fact that APs and SM units are general computational resource-constrained and hence the minimized number of messages.

For every data reading and aggregation cycle, an AP sends a single message Overall, it is generally noted that the total communication loads for BS, SM and each AP is one message for each reading and aggregation cycle. Fig. 4. shows the communication load at HAN level during a data reading and aggregation round. As expected, as we increase the number of household appliances, the communication load also increases. For the SM load remains stagnant.

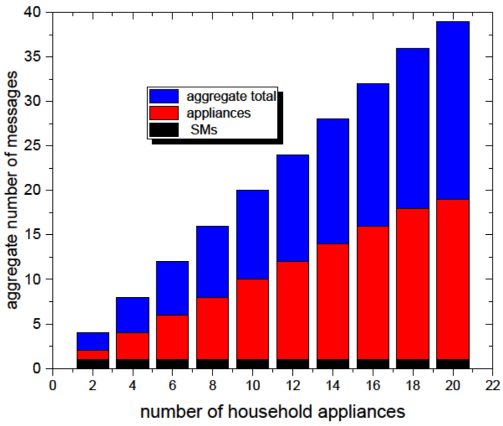

Fig. 4, Communication loads per data reading cycle

Shown in Fig. 5, is the total communication loads per day for a particular area (domain). In this case, we gradually increase the number of APs corresponding to the increase in the number of households, appliances, or expansion of the domain.

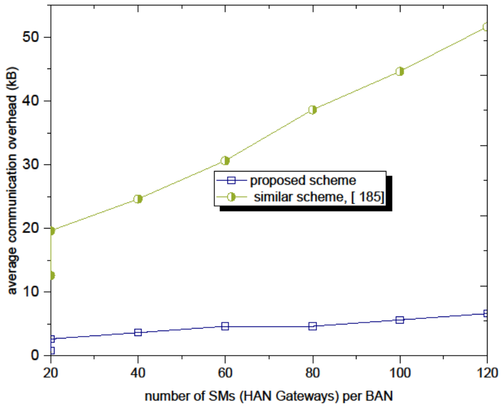

Fig.5, Communication loads per 24 hour cycle

Whereas the number of APs increase, each AP, SM or BS will still send a single message per reading and aggregation cycle. It can be observed that an increase in the number of $HANs$ also leads to communication load moderately increases.

Computational overhead

According to the proposed scheme, each AP performs a single encryption run per each data reading and aggregation cycle. The same applies to each HAN if it houses a single AP. However, if it houses n of them, then the number of encryption operations will also correspondingly increase to n. By nature, the encryption is lightweight enough as it involves basic arithmetic operations.

$$C_{total} = [m*(n*T_e + T_s + T_v)] + T_d + T_v + T_s \quad (45)$$

In the previous equation, m is the number of BS in the area. T_e is the computation.

time for one encryption process, T_d is the time for one decryption process, T_s is the time for one signing process, and T_v is the time for one verification process. The provided table (Table 1) summarises the number of operations.

Table 1, Summary of cryptographic operations

No. of operations	per cycle	per day
$AP_s(Group-1\&2)$	T_e	$h*T_e$
$AP_s(Group-3\&4)$	T_e	$(h+2)*T_e$
SM	T_e	$(h+6)*T_e$

A plot of the computational loads versus the number of appliances is provided in Fig. 6 .for each data reading and aggregation cycle.

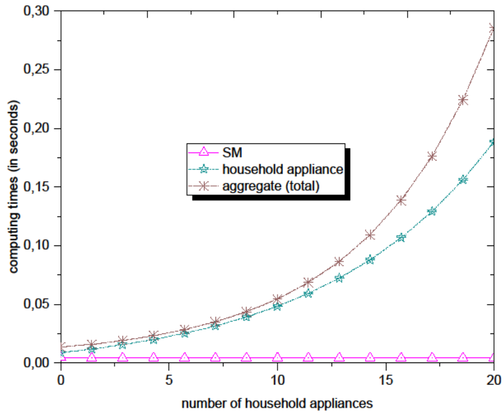

Fig. 6, Plot of computational delay times

It can be observed that the computational load of the individual APs is independent of the number in a household. Once again a SM's load is stagnant as it only is required to perform a single signing process regardless of the number of messages included.

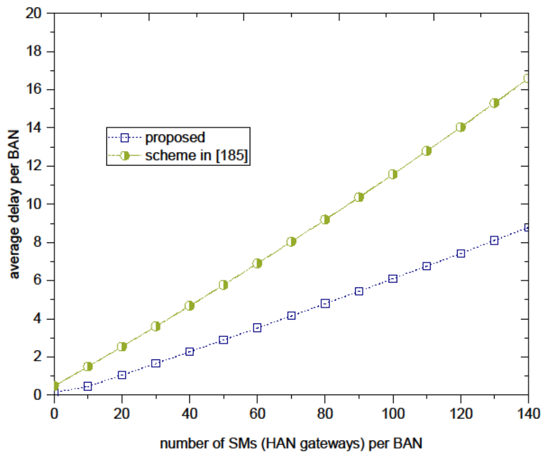

Fig. 7, Computational delays

In Fig. 7, the aggregated daily computation load for a single cluster is plotted for varying numbers of both $HANs$ and APs e. As indicated, the computation overhead increases with the increase of APs and HANs' numbers, but still within a bounded limit; the total computation delay for a cluster of 100 HANs that each one of them has 20 APs is around 90 seconds per day.

V. CONCLUSION

A D2D Lightweight Customer Side data Aggregation Scheme takes into cognizance the fact that some of the elements involved are resource-constrained hence a lightweight form approach is chosen. In this way-SG messages will be delivered with absolute security guarantees, at low computational complexities and loads since most of the devices are constrained in terms of both power and computational memory.

Conflicts of Interest

None of the authors has a financial relationship with a commercial entity that has an interest in the subject of this manuscript.

Funding Statement

The work was partly funded by the Faculty of Engineering jointly with the Research Office as part of support to my PhD studies.

Acknowledgments

We acknowledge the support we got from colleagues in the Department.. The work was equally contributed by the two authors

REFERENCES

[1] R. Lu, X. Liang, X. Li, X. Lin and X. Shen, EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid C. Ji, P. Yu, W. Li, P. Zhao and X. Qiu, Comprehensive vulnerability assessment and optimization method for smart grid communication transmission systems, IFIP/IEEE Symposium on Integrated Network and Service Management (IM), (2017), 75-978.

[2] P. McDaniel and S. McLaughlin, Security and Privacy Challenges in the Smart Grid, IEEE Security & Privacy, 7 (3),(2009), 75-77.

[3] S. Han, S. Zhao, Q. Li, C. Ju and W. Zhou, PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation With Fault Tolerance, IEEE Transactions on Information Forensics and Security, !! (9), (2016), 1940-1955.

[4] S. Li, K. Xue, Q. Yang and P. Hong, PPMA: Privacy-Preserving Multisubset Data Aggregation in Smart Grid, IEEE Transactions on Industrial Informatics, 14(2),(2018),462-471,

[5] M. Yang, T. Zhu, B. Liu, Y. Xiang and W. Zhou, Machine Learning Differential Privacy With Multifunctional Aggregation in a Fog Computing Architecture, IEEE Access, 16,(2018), 17119-17129.

[6] H. Wu, L. Wang and G. Xue, Privacy-Aware Task Allocation and Data Aggregation in Fog-Assisted Spatial Crowdsourcing,n IEEE Transactions on Network Science and Engineering, 7(1), (2020), 589-602.

[7] Wang M, Yan Z, Niemi V. UAKA-D2D: Universal Authentication and Key Agreement Protocol in D2D Communications. *Mob Netw Appl,* 22(3), (2017),510–25.

[8] N. Maskey, S. Horsmanheimo and L. Tuomimäki, Analysis of latency for cellular networks for smart grid in suburban area, IEEE PES Innovative Smart Grid Technologies, (2014), 1-4.

[9] J. Cao et al., A Survey on Security Aspects for 3GPP 5G Networks, IEEE Communications Surveys & Tutorials, 22(1), (2020),70-195.

[10] Y. Sun, J. Cao, M. Ma, Y. Zhang, H. Li and B. Niu, EAP-DDBA: Efficient Anonymity Proximity Device Discovery and Batch Authentication Mechanism for Massive D2D Communication Devices in 3GPP 5G HetNet, IEEE Transactions on Dependable and Secure Computing, 19(1), (2022), 370-387.

[11] J. G. Panicker, A. S. Salehi and C. Rudolph, Authentication and Access Control in 5G Device-to-Device Communication, IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, (2021), 1575-1582.

[12] L. Wei, L. P. Rondon, A. Moghadasi and A. I. Sarwat, Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid, IEEE/PES Transmission and Distribution Conference and Exposition (T&D), (2018), 1-9.

[13] H. Zhang, B. Liu and H. Wu, Smart Grid Cyber-Physical Attack and Defense: A Review, IEEE Access, 9, (2021), 29641-29659.

[14] S. Ruj, A. Nayak, and I. Stojmenovic, A security architecture for data aggregation and access control in smart grids, (2011).

[15] A. Fu, J. Song, S. Li, G. Zhang, and Y. Zhang, A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks, Security Communication. Networks., 9(13), (2016), 2002–2014.

[16] K.-R. Jung, A. Park, and S. Lee, Machine-type-communication (MTC) device grouping algorithm for congestion avoidance of MTC oriented LTE network, Security-Enriched Urban Computing and Smart Grid. Berlin, Germany: Springer,(2010) 167–178.