A Privacy and Security Preservation Framework for D2D Communication Based Smart Grid Services

Lebogang P. Bopape
Department of Electronic & Computer Engineering
Faculty of Engineering, DUT
Durban, RSA
lebobopape@gmail.com

Bakhe Nleya, P. Khumalo
Department of Electronic & Computer Engineering
Faculty of Engineering, DUT
Durban, RSA
bmnleya@ieeee.org

Abstract— **Long-Term-Evolution (LTE) based Device-to-Device (D2D) communication in future generation networks are envisaged to become the basis for deployment of various applications and services in Smart Grids (SGs). However related privacy and security aspects are also under serious consideration especially when dealing with large-scale deployment of services and applications related D2D groups. Current and legacy related algorithms cannot be applied directly to this new paradigm shift (i.e D2D communication and group formations). Using the IoT as the pillar communication subsystem for SGs, the service providers can deploy several applications and services some of which may include the acquisition and storage of personal information of individual SG users. However, the challenge will always be in the strict preservation of privacy and security of their personal data and thus a necessity in eliminating such concerns. In this paper we propose a general framework that employs a Group Key Management (GKM) mechanism to ensure enhanced privacy and security especially during the discovery and communication phases. We further mitigate on the impact of enhanced privacy and security in SG services and applications.**

Keywords— IoT (Internet of Things), privacy, security, group authentication, D2D communications

I. IOT ENABLED SMART GRID COMMUNICATION SUBSYSTEMS

The introduction of next generation power grid systems commonly referred to as SGs, has brought about improved operational efficiencies in terms of demand, supply and marketing within them. The incorporation of distributed control and management infrastructures has further brought about new and innovative applications and services [1], [2]. However, this latter development has resulted in heightened concerns about various privacy as well as various security issues which need to be addressed adequately. Security threats such as semantic attacks, physical attacks as well as nature related disasters are prominent examples threats with regards to SGs deployment which if not addressed can ultimately lead to a complete infrastructural collapse, increased revenue losses due to energy theft, power blackouts, SG user privacy breaches, as well as safety compromise to of operating and maintenance personnel. It is therefore imperative that privacy and security issues in the SGs be critically addressed so as to minimize as well as avoid possible failures or threats [3], [4].

Key to the successful operation of future generation SGs would be an enabling secured communication subsystem to interconnect the various distributed computing systems. Harnessing the already available IoT as the pillar communication subsystem for SGs has added advantages. The International Telecommunications Union (ITU) defines an IoT enabled network as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [4].

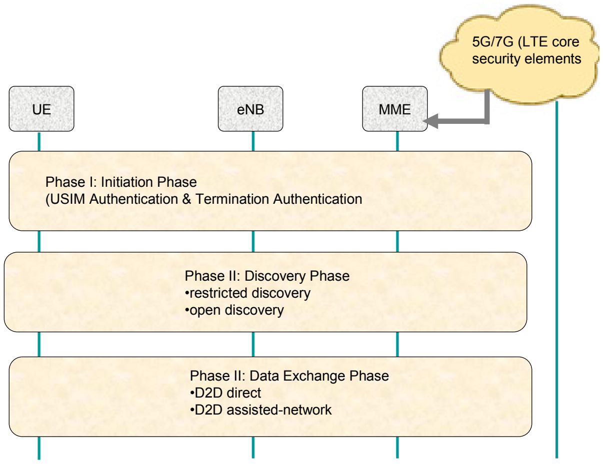

Fig. 1. Summary D2D communication phases

The diversity in terms of dimensions and the scopes of an IoT enabled network has prompted standardization in order to establish interoperability among interconnected things in SGs. In this regard, several standardization authorities are currently working or wrapping up relevant standards. To provide a common seamless SG communication subsystem platform for the envisaged multitudes of services and applications, a D2D group communication standard is being defined. Most individual applications or services in the SG in-

ISBN 978-1-7281-3770-4/19/$31.00 ©2020 IEEE

volve the interaction of devices in a group. A typical example service would be the multicasting of targeted users for power usage regulation purposes or billing data acquisition from smart meters in a particular residential area. In this regard D2D group communication has the potential to afford high data rates, minimal end to end latencies, as well as matured peer discovery mechanisms. A D2D communication is normally characterized by three distinct phases namely, initialization, discovery and data exchanges as illustrated in Fig. 1. Privacy and security issues are considered key milestones in such communications and thus the required authentication as well other security requirements for Phase I are provided by the core network itself whereas additional security requirements are needed for the other two phases. Most services and applications deployment will involve the cooperation and interaction of devices within a particular area forming a group. Thus, efficient device discovery mechanisms are required for detecting the proximity of such D2D communication-enabled devices. When initiating a service targeted device are expected to detect peers within proximity to potentially establish the required D2D communication session [5].

In this paper, we will restrict ourselves to addressing the problem of designing a group-based authentication and key agreement (AKA) scheme that ensures secure end-to-end communications in an automated metering infrastructure (AMI) in the SG. Specifically, our solution provides an efficient approach to managing keys as well as a strong authentication mechanism.

II. EXISTING D2D GROUP COMMUNICATIONS AKA PROTOCOLS

Quite a number of group privacy and security protocols specifically relating to groups AKA continue to be explored. Security requirements such as confidentiality, mutual authentication, privacy preservation, integrity and most importantly utilizing a common and single security (encryption) key during the communication sessions in the IoT network is preferred. Such protocols need to inherently achieve efficacy in maintaining the group key unlink ability as well as generate minimal overheads that otherwise may lead to network congestion [6]. To alleviate signaling related congestion the authors in [7] proposed a congestion avoidance approach in which a group of devices delegate a leader to handle the communications on behalf of the rest of the group members. In this way the volumes of aggregated signaling overheads is significantly lowered and so is the congestion.

The same approach was revisited by the authors in [8] in which they propose a group AKA (G-AKA) protocol. In this case a single device from the group is authenticated by the AKA authority in the SG, after which the same device is now delegated to authenticate the remaining devices of the group. In that way the authentication process becomes relatively simplified for the rest of the devices in the group. One disadvantage with such a protocol is that of the possibility of high levels of signaling overhead being generated should several devices wish to gain access to the SG network simultaneously. It has also been shown that the protocol is so secure in preventing to potential threats such, as DoS and redirection attacks.

A symmetric key based AKA (SE-AKA) protocol that enhances both data integrity and confidentiality was investigated in [9]. Whereas the protocol shows improvements in security, it however generates massive signaling overheads that ultimately lead to network signaling congestion.

In [10] an enhanced group AKA (EG-AKA) protocol is proposed to authenticate a targeted group of devices. The protocol is quite computationally intensive and hence generates high computation overheads in the network due to asymmetric key operations. The authors in [11] propose a Group-AKA protocol that mitigates the problem of excessive signaling overheads by way of authenticating grouped devices simultaneously. The protocol maintains the unlink-ability in the group key whenever an individual device vacates or joins the group. One of its short comings is that of preserving the privacy of participating devices as well as susceptibility to identity catching attacks while authenticating any additional new device(s) into the group.

To address the shortcomings of privacy preservation failures in previous AKA protocols, the authors in [12] proposed a elliptic curve cryptography based privacy preserving group authentication AKA (PRIVACY-AKA). Initially a pseudo identity by way of elliptic curve cryptography is generated and thereafter each device in the group transfers its message authentication code to the designated group leader. The group leader then in turn compiles each code into an aggregate MAC which will subsequently be used by the network to authenticate the rest of the devices in the group. Whereas, the protocol provides acceptable security, it however generates high computational overhead due to the asymmetric key cryptosystem. It also fails to take into consideration the group key secrecy in terms of when a device joins or vacates the group.

The proposed approach overcomes the security problems of the network and generates relatively less overhead compared to the existing group-based AKA protocols. It accomplishes all the security requirements for D2D communication with moderate levels of both signaling as well as computational overhead.

III. IOT ENABLED COMMUNICATION SUBYSTEM AND AMI INFRATSRUCTURE

In order to provide privacy as well as security in an AMI service, secure authentication and key exchange among the D2D communication compliant smart meters (SMs) is necessary. A third-generation partnership project (3GPP) IoT enabled network architecture is assumed as illustrated in Fig. 2. Key security related blocks defining the SG communication subsystem include the D2D communication server, (D2D), home subscriber server (HSS) and mobility management entity (MME). The HSS retains attributes information of the SM devices and relies on the MME to verify the SMs by way of granting a set of authentication tokens. The billing entity (which is part of the service provider control authority) can be regarded as a D2D user and as such remains outside the core SG communication network domain. To facilitate SM data reading in a particular area the D2D server connects to both the billing center (BC) as well as SMs and upon successful authentication among the parties the data read from the SMs can now be furnished to the BC.

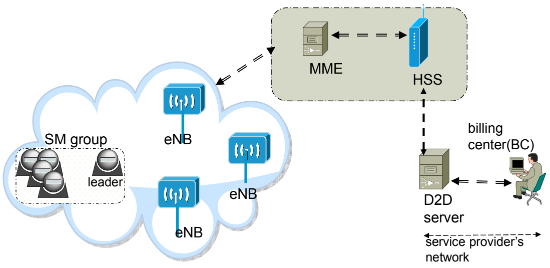

Fig. 2. SG IoT Enabled Communication Subsystem Architecture [5].

In this paper, the AMI service infrastructure is assumed to abstractly comprises: the BC, neighborhood located data collectors (DCs) and the SMs. The required communication link is provided by the available IoT enabled network. This is illustrated in Fig. 3.

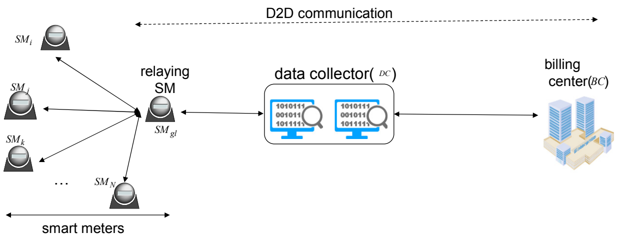

Fig. 3. Abstracted AMI service

The data exchanges between the various entities constituting the AMI traverse one or multiple collectors and possibly through other SMs acting as relay points. D2D communications is assumed between the BC and DCs. As such all SMs deployed in the SG are assumed to be D2D communication compliant and physically unclonable. Data load handling in SMs is addressed by way of data aggregation in which the data from various remote SMs is combined together before being relayed across the network via a designated relaying SM. The same relaying SM becomes a group leader (SM_{gl}). In that way both the bandwidth as well as links are utilized more efficiently.

IV. MODEL APPROACH

In this section we briefly describe the security framework that we will refer to as the Group Authentication and Key agreement scheme (Gr-AKA). We assume that each approved SM is preloaded with a private (A^-) as well as a public key (A^+) on a long term basis. Similarly both the DC and authorized billing center (BC) are also preloaded with their own private/public key pairs on a long term basis. For shared key establishment, SMs, DCs and BC commonly make use of Diffie-Hellman (DH) parameters g and p [13]. The all agree on the use of the following elementary cryptographic operations:

i. public encryption key on message;

$M \rightarrow Public\_key(K,M)$.

ii. Symmetric key encryption on the same message using the key in step;

$i \rightarrow symmetric\_key(K,M)$.

iii. Signature of the message by A a derivative of (A^-);

$signature)\_(A,M)$.

iv. computing of the hash key of the message using the same key;

$hash\_(k,M)$.

v. We assume a centralized key generation center (KGC) and is available for use within the SG by authorize parties.

Our security objective is to ensure that the data read from SMs can only be read by an authorized BC and thus it is necessary to efficiently encrypt the data exchanged between a designated DC and BC. In practice the entire data collection procedure has a tree like formation. The DC then collects the data from all the targeted SM group members via the designated group's leader (SM_{gl}). The collected data is then forwarded to the BC via the available network.

The detailed descriptions are as follows [1], [18];

A. *Session Request and SM Group Registration*

A BC is routinely requested to acquire data from SMs within the SG and as such registers for the AMI service with the service provider (SP).

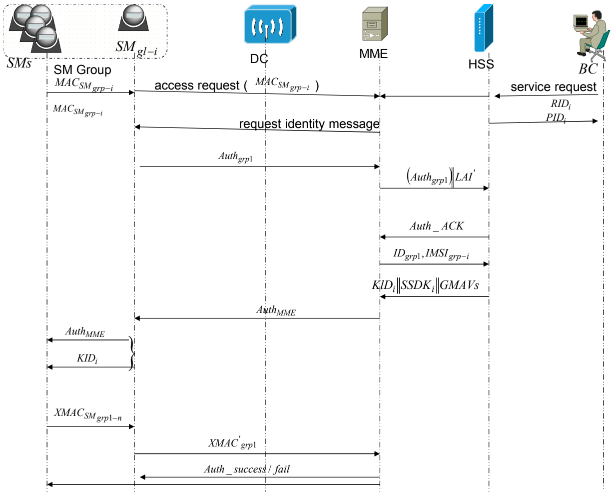

Fig. 4. Sequence events for the proposed framework

As an authorized user with a real and valid identifier (RID_i) the BC completes the necessary registration formalities with the local HSS. If access is granted the HSS acknowledges by generating and issuing a pseudonym ID ($pseudo\_PID_i$) to the BC.

$$pseudo\_PID_i \overset{\text{def}}{=} (pseudoID, ExpiryTime) \tag{1}$$

The already generated RID_i will further be used in the SM group discovery (formation) as well as initialization process. All members of the SM group (SM_{grp-i}) must be authenticated as well by the HSS. In this regard the latter generates a set of random numbers $\mathbf{R_z} \in \mathbf{Z_p^*}(z = 1,2,...i)$ that will be used to compute a set of temporary identities $TID_{SM_{i-j}}$ to each SM in that group:

$$TID_z = h_1(ID_{MTCD} \| \mathbf{R_z} * x) \tag{2}$$

where,
$h_1(.)$ is a secure hash function with parameters p and q;
x is HSS's own secret authentication key.
The HSS further computes the newly formed group's authentication key as follows:

$$GK_i = h_3(\sec_{i-1} \oplus \sec_{i-2} \oplus ..., \oplus \sec_{i-j} \oplus g * x) \tag{3}$$

where $h_3(.)$ is a hash key and g – is a random integer.

B. Group Authentication and Key Agreement

In order to maintain group privacy as well as security individual SMs in the group must mutually authenticate as belonging to the group, SM_{grp-i}. The SP then assigns a key (K_{grpi-j}) to each group member, as well as generating a group key which will be used for mutual authentication as well as privacy protection between the group's members and SP. This is done mainly by the group's leader (SM_{gl-i}) and the HSS. This is carried out is sequence as follows:

1. Each group member shares a fresh temporary identifier ($TID_{SM_{i-j}}$) and associated token $f\left(TID_{SM_{i-j}}\right)$ with the group's leader.

$$SM_{i-j} \rightarrow \lfloor TID_{SM_{i-j}}, f(TID_{SM_{i-j}} \rfloor \Rightarrow SM_{gl} \tag{4}$$

2. This is followed by the group's leader calculating the Lagrange component (LC) vector for the group. For it to do so, it will first acquire $TID_{SM_{i-j}}$ and $f\left(TID_{SM_{i-j}}\right)$ values from the KGC.

   The general formula it uses for the LC computation is;

$$LC_{grp-i} = f(TID_{SM_{1-i}}) \prod_{q=1, q \neq j}^{\frac{n}{m}} \frac{-TID_{SM_{1-q}}}{TID_{SM_{i-j}} - TID_{SM_{i-q}}} \bmod p \tag{5}$$

   This computed component is shared with all group members for mutual authentication purposes within the group. This step is necessary in order to ensure that unauthorized SMs or other devices may not have access to the data being collected.

3. Upon successful completion of the previous step, the group leader further authenticates with the core network (MME) on behalf of the entire group. It does by furnishing both the group's MAC_{grp-i} and $Auth_{grp-i}$ computed values.

$$MAC_{grp-i} = h_2(GK \| ID_{grp-i} \| LAI \| S') \tag{6}$$

$$Auth_{grp-i} = (TID_{grp-i} \| MAC_{grp-i}) \tag{7}$$

$$SM_{gl-i} \underrightarrow{Auth_{grp-i}, TID_{SM_{i-1}}, ...TID_{SM_{i-j}}} \rightarrow MME \tag{8}$$

4. MME will then confirm the legitimacy of the group's existence with HSS.

$$MME \rightarrow \underrightarrow{Auth_{grp-i}, LAI} \rightarrow HSS \tag{9}$$

5. The HSS authenticates the group by recalculating the group's MAC_{grp-i} based on values furnished by the MME

$$MAC'_{grp-i} = h_2(GK \| ID_{grp-i} \| LAI \| S) \tag{10}$$

   If authentication is successful at this stage, HSS further generates a temporary group key (TGK) for the group as follows:

$$TGK_{grp-i} = h_3(GK \| r_{HSS}) \tag{11}$$

   where, r_{HSS} is a random integer.

6. HSS confirms the successful authentication with the MME in which case the latter further computes its own LC (LC_{MME}) and corresponding $Auth_{MME}$ before sending them to the group's leader(SM_{gl-i}). These are:

$$LC_{MME} = f(ID_{MME}) \prod_{q=1}^{\frac{n}{m}} \frac{-TID_{SM_{i-q}}}{ID_{MME} - TID_{SM_{i-q}}} \times \bmod p \tag{12}$$

$$Auth_{MME} = (LC_{MME} \| r_{MME} \oplus GTK \| r_{HSS} \| ID_{MME}) \tag{13}$$

   Upon receiving $Auth_{MME}$, and encrypted KID_i the group leader broadcasts them to the rest of the group members.

7. Once the group members receive the values in (12) and (13) above, each in turn updates its LC accordingly;

$$LC\_new_{SM_{i-j}} = LC_{SM_{i-j}} * \frac{-ID_{MME}}{TID_{SM_{i-j}} - ID_{MME}} \tag{14}$$

Each SM further calculates its own , integrity and cipher keys TGK using the received r_{HSS} as follows:

$$TGK_{grp_i} = h_3(GK \| r_{HSS}) \tag{15}$$

$$IK'_{grp_{i-j}} = h_4(ID_{grp_i} \| r_{HSS}) K_{grp_{i-j}} \tag{16}$$

$$CK'_{grp_{i-j}} = h_5(ID_{grp_i} \| r_{HSS}) K_{grp_{i-j}} \tag{17}$$

$$\begin{aligned} K_{asme}^{'MTCDgrpi} = KDF(GTK_{grp-i} \| IK'_{grp_{i-j}} \| CK'_{grp_{i-j}} \\ \| ID_{grp-i} \| IMSI_{grp_{i-j}} \end{aligned} \tag{18}$$

Each member further computes its response using (15) to (18) before furnishing it to the group leader.

$$XMAC_{SM'_{grp_{i-j}}} = h_1(ID_{grp-i} \| r_{HSS} \| IMSI_{grp_{i-j}})_{GTK_{grp-i}} \tag{19}$$

The group leader finally computes the group response.

$$\begin{aligned} XMAC_{grp-i} = h_1(XMAC_{MTCD_{grp1}} \oplus XMAC_{MTCD_{grp1-2}} \oplus \\ \oplus, \ldots . XMAC_{MTCD_{grpn}})_{GRPK_1} \end{aligned} \tag{20}$$

The response is sent back to the MME for final authentication.

V. SECURITY DISCUSSION

In the proposed security framework, the privacy of the data is ensured by way of using DH keys which are themselves exchanged in encrypted form. Signatures are also used to further enhance information exchanges from the root to leaves, while data is authenticated hashes on a hop by hop basis.

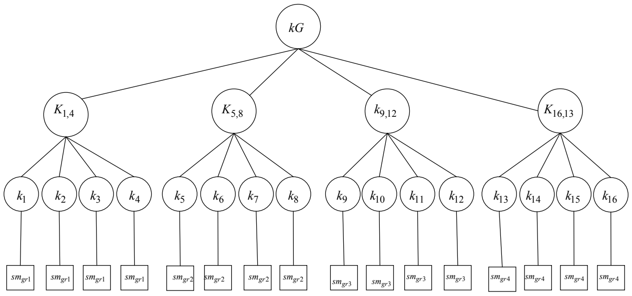

Fig. 5. Multilevel (4) key tree for group formation during data collection

In this part, we present the performance evaluation obtained in the security of D2D group device communications implementation. The general level of security requirements for the proposed framework is to prevent any forms of malicious attacks as well as guarantee several security requirements. Examples of such requirements include integrity and protection, privacy in group communication (GK), anonymity in GK, non-repudiation as well as identity disclosure.

An analytical evaluation of the proposed framework protocol with others discussed in the review section was performed with respect to three performance measures namely; (1) computational complexity, (2) number of signaling messages exchanged during authentication and (3) communication cost (which is an indicator of the volumes of data exchanged in executing the authentication processes.

Table 1. parameters for computing computational loads

field	size(bytes)
Message Authentication Code	8
IMSI	8
GK	16
LAI	5
temporary Id	16
pseudo ID	40

As per the proposed hierarchical architecture and aggregation is performed by group leader, the size of groups is 4 SMs a single group. One of them is designated as a group leader and aggregates the messages/signals from the other three.

Table 2 Computational parameters (SM side)

operation	*duration (ms))*
ciphering	0.2
decyphering	5
digital signature	5
hashing (h)	0.04
pairing	40
point multiplication	1.5

The main security aspects of the protocol is tested using the GUROBI Solver tool [16] . To evaluate the total computational overheads, we compare the protocol with PPAKA-HMAC [17], G-AKA [16], and GBS-AKA [16]. The analytical evaluation relied mostly on the values in tables 1,2 and 3 adapted from [18].

Table 3. Computational parameters (core network)

operation	Duration (ms))
digital signature	5
hashing (h)	0.02
pairing	20.1
point multiplication	0.5
LC calculation	0.5

We further explore the proposed protocol's execution time and compare the same protocols cited earlier.

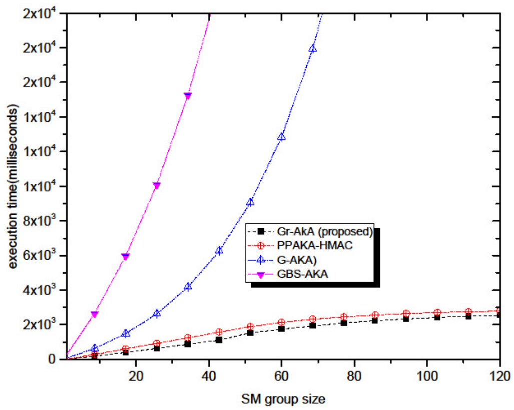

Figure 5: Execution time comparisons

The execution time more less increases linearly with increase in the number of *SM* devices in the group for the proposed scheme as well as PRAKA-HMAC [17]. However, execution times more less grow exponentially with both G-AKA, and GBS-AKA.

We also evaluate the protocol in terms of the signaling overheads generated during the AKA phases.

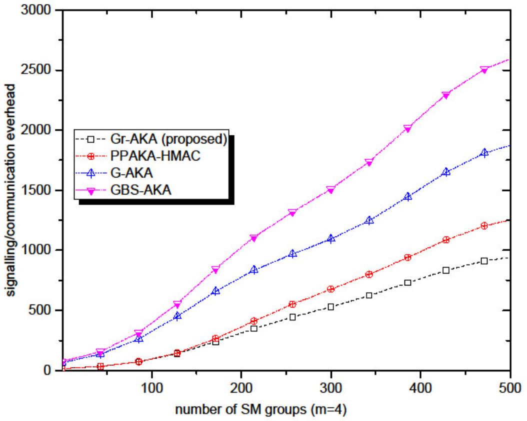

Figure 6: Signaling overhead

The plot in Fig. 7 plots the magnitude communication overhead a function of the number of *SM* groups, each comprising 4 members. Overall both the proposed protocol and PPAKA-HMAC generate more or less the same levels of signaling data, moderate enough not to cause congestion.

VI. CONCLUSION

The paper presents a privacy and security preservation framework for data acquisitions and transfer in an SG environment where all devices are D2D communication compliant. This includes the smart meters. Specifically, we propose a general framework that employs a Group Key Management (GKM) mechanism to ensure enhanced privacy and security especially during the discovery and communication phases. The proposed Gr-AKA underlying protocol's performance is compared with that of similar ones. By comparison, analytical results show the proposed protocol outperforming the other comparable ones significantly. In particular the low overhead computational loads is attributed to by the group authentication approach in which the designated group leader handles all the authentication on behalf of the rest of group members.

REFERENCES

[1] P. Khumalo, B.Nleya, A. Gomba, A Mutsvangwa. "Services and Applications Security in IoT Enabled Networks", International Conference on Intelligent and Innovative Computing Applications (ICONIC),2018.

[2] W. Wang and Y. Xu and M. Khanna, "A survey on the communication architectures in smart grid", Computer Networks, (2011) July, pp. 3604-3629.

[3] X. Fan and G.ang Gong., "Security Challenges in Smart-Grid Metering and Control Systems", Technology Innovation Management Review, July 2013.

[4] S. Ruj, A. Nayak and I. Stojmenovi, "A Security Architecture for Data Aggregation and Access Control in Smart Grids", arXiv:1111.2619v1,[cs.NI],10 Nov 2011.

[5] Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Aspects of Non-3GPP Accesses (Release 11), document 3GPP TS 33.402 V11.4.0, 3GPP, Jun. 2012.

[6] S. M. R. Islam, D. Kwak, M. Humaun and K.-S. Kwak, ''The Internet of Things for health care: A comprehensive survey,'' IEEE Access, vol. 3, pp. 678–708, Jun. 2015.

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

[8] Y.-W. Chen, J.-T. Wang, K.-H. Chi, and C.-C. Tseng, ''Group-based authentication and key agreement,'' Wireless Personal. Communications., vol. 62, no. 4, pp. 965–979, 2012.

[9] C. Lai, H. Li, R. Lu, and X. S. Shen, ''SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks,'' Computer. Networks., vol. 57, no. 17, pp. 3492–3510, 2013.

[10] R. Jiang, C. Lai, J. Luo, X. Wang, and H. Wang, ''EAP-based group authentication and key agreement protocol for machine-type communications,'' Int. Journal of.Distributed Sensor Networks., vol. 9, no. 11, p. 304601, 2013.

[11] D. Choi, H.-K. Choi, and S.-Y. Lee, "A group-based security protocol for machine-type communications in LTE-advanced,'' Wireless Networks., vol. 21, no. 2, pp. 405–419, 2015.

[12] 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., vol. 9, no. 13, pp. 2002–2014, 2016.

[13] C. Lai, R. Lu, D. Zheng, H. Li, and X. S. Shen, ''GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications,'' Computer. Networks., vol. 99, pp. 66–81, Apr. 2016.

[14] "Wash.. de data set", 20154, [online]; http://data.octo.dc.gov/

[15] "GUROBI solver", 2014, [Online];: http//www.gurobi.com/

[16] Y.-W. Chen, J.-T. Wang, K.-H. Chi, and C.-C. Tseng, ``Group-based authentication and key agreement,' Wireless Personal. Communications., vol.62, no. 4,pp. 965_979, 2012.

[17] J. Yao, T. Wang, M. Chen, L. Wang, and G. Chen, ``GBS-AKA: Group based secure authentication and key agreement for M2M in 4G network,'' in Proc. IEEE Int. Conf. Cloud Computing. Research. Innovations. (ICCCRI), May 2016, pp. 42_48.

[18] P. Roychoudhury, B. Roychoudhuryand D. K. Saikia, "Hierarchical Group Based Mutual Authentication and Key Agreement for Machine Type Communication in LTE and Future 5G Networks, Security and Communication Networks", Volume 2017, Article ID 1701243, 21 pages.