Authentication Scheme for IoT of Power-Hungry Home Appliances in Smart Grid Environment

Samrat Acharya, Hoyin Wan, Ankita Manohar Narvekar, Susanna Xu, Maciej Becz

***Abstract*—The Internet of Things (IoT) in smart grid environment is increasingly evolving. Power-hungry home appliances like Air-conditioners (AC), water heaters, etc. have potentials to participate in providing grid-ancillary services or grid stability, by being remotely controlled by grid operator. However, secure communication between power-hungry devices and grid control center has been challenging, primarily because of the distributed nature of power-hungry devices. Moreover, large number of the power-hungry devices, needed for impactful grid-ancillary services, have imposed further challenge in security of IoT of power-hungry devices. This paper has explored authentication of communicating entities in IoT of power-hungry devices. Specifically, group authentication of power-hungry devices in Building Area Network Gateway (BANGW) is proposed for the sake of reducing overhead in BANGW, whereas Diffie-Helmen based one-to-one mutual authentication scheme is proposed for secure communication between BANGW and Control Center Gateway (CCGW). Furthermore, other techniques of authentication in the IoT environment is also outlined.**

***Index Terms*—Authentication, Power-hungry devices, Internet of things (IoT), Diffie-Helmen key exchange, Group authentication.**

I. Introduction

For the sake of three main pillars of sustainability; economics, environment, and society, power grids have been increasing the penetration of renewable energy integration in power generation portfolios. However, the expanding level of penetration is not free of challenges, particularly in terms of power grid reliability and security. Demand-side management has been envisioned as one of the promising avenues to contribute towards the solution of power grid reliability [1]. This new paradigm in power system environment give rises to Internet of Things (IoT) of power-hungry devices.

IoT of power-hungry devices can be anything from air conditioner (AC) units to electric vehicles (EVs), which consumes significant proportion of power, say in kilowatts (kWs), and are connected to the internet for their control. The number of these devices has been significantly increasing in smart grid environment. Moreover, these devices constitute a major portion of building energy consumption, especially in residential and commercial buildings, [2].

These devices operate under the principle of hysteresis control algorithms [1]. For instance, temperature range for AC units, state-of-charge (SoC) of battery for EVs. Due to this flexibility, these devices are encouraged to participate in providing grid ancillary services, like stability of the power grids. The grid ancillary service request is sent by grid control center, often called Supervisory Control and Data Acquisition (SCADA) system, to the power-hungry devices. Apparently, these power-hungry devices having pre-consent to participate in grid ancillary services are remotely controlled, by SCADA, on top of their local controller.

With devices now connected over the Internet and being remote controlled, pose new security threats as attackers can hack and control these devices remotely. They can use these hacked devices to create a botnet and cause a distributed denial-of-service (DDoS) attack which can lead to severe and widespread blackouts as the effects of the attack can trip breakers and cause a cascading grid failure. This is due to the fact that a small imbalance of power in the power grid system, for instance a 1% increase in demand in critical bus can create catastrophic results, with widespread line failures and take down 86% of the load [3].

Not only can attackers compromise home appliances, but also the utilities or SCADA who power and control these appliances. What makes these attacks more alarming is that the sources are hard to detect and disconnect by the grid operator due to the distributed nature of smart meters associated with power-hungry devices [3].

Proper authentication of these distributed smart meters at SCADA/ regional control center side, and the reverse is of crucial importance. Although authentication alone wont make the system secure on its own since lack of encryption is also a potential security flaw. However, in this paper we will investigate on authentication of power-hungry devices over different layers of area networks.

II. Background

IoT of power-hungry devices problem is only growing now as the number of detected attacks grew six times in 2017 [4]. Not a surprise when utilities increasingly encourage the installation of such devices in the form of smart meters so they can remotely control, like by turning them on and off, for power grid stability purposes [5]. According to [6] such devices are generally turned on, and mostly reside on residential networks which are not monitored for either incoming or outgoing attack traffic, and the networks where theyre deployed increasingly offer high-speed connections. This poses a major problem as with the high speed connection attackers can quickly bring down numerous networks as they are not monitored anyway. These attacks can also be done in quite a simple way, by generating a signal that is stronger than the ones the utilities repeaters send [5].

Even if the attacker is only in control of your smart meter, they can also potentially compromise the entire network of devices, from your computer to your washing machines, in your home. Compromised devices can quickly grow from one to many as each of these power devices or groups of them have a unique identification number that can be traced back to a specific household [5].

Manufacturers create IoT devices with as little processing power as possible in order to decrease cost[11]. This results

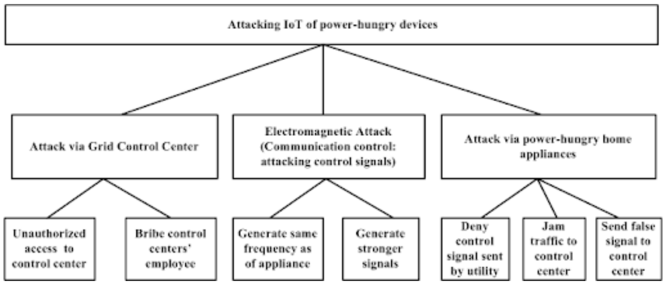
Attacking IoT of power-hungry devices
Attack via Grid Control Center
Electromagnetic Attack (Communication control: attacking control signals)
Attack via power-hungry home appliances
Unauthorized access to control center
Bribe control centers' employee
Generate same frequency as of appliance
Generate stronger signals
Deny control signal sent by utility
Jam traffic to control center
Send false signal to control center

Fig. 1. Attack tree for hacking IoT of power-hungry devices.

TABLE I
THREAT ANALYSIS TABLE

Threat	Solution Proposed
Remote smart meters accessed by attackers.	Create a backup power supply systems, eg. battery, to restore power quickly in case of blackouts.
Concentrated attack on one part of grid	Deregulation of power grids control center with strong mechanism of authentication, authorization and encryption. This solution has additional cost of deregulation but is more secure.
Repeaters which send out signals to control these power-hungry devices can be overpowered by stronger signals.	Make the communication channel secure and the electronic chips on all devices should have ways to identify and authorize correct signals and disregard incorrect ones.
Home routers can be compromised and they can be used to overrun DNS with bogus traffic	Create a system to identify Denial of Service attacks and block traffic coming from these spam devices.
Having same IDs for multiple power appliances.	Generate unique IDs and updating of IDs over time. This solution has advantage of minimizing the impact of attack

in our home appliances and the utility companies devices to have little to no security measures, for instance encryption, in place. This also means that if a major flaw is to found and exploited on these devices it will be arduous to recover from as these devices cant be patched or simply take a long time to do so [7]. Utilities must seek for manufacturers to put in place more security functionality in their devices for more secure communication throughout the network.

It is not enough to protect against these attacks by taking passive measures such as sectioning the grid to quarantine the attack to as small an area as possible or installing backup power generators. There is a desperate need for a more direct increase in security across the network. Policies are now being put in place to push for more security reinforcement on the power grids architecture. For instance, North American Electric Reliability Corporation has utilities not only observe the grid for potential attacks, but also use multi-factor user authentication to prevent unauthorized access. Authentication is crucial step in creating a more secure system as it can prevent attackers from gaining remote control access and sabotaging the network. This is extremely important since many of the devices are too simple to have their own interfaces so only admins can control it [7]. This makes it so that once attacker takes control it will be difficult to recover from or even detect [7].

III. THREAT MODELING

In the first part of assignment attack trees were used to show possible threats on the power grid with the use of IoT devices. To this day power-hungry IoT devices that are now commonplace in peoples homes, have very weak security. Manufacturers often overlook the security for these devices and make immature and crucial mistakes like assigning the same ID number to multiple devices or using weak and easily interpretable signals to contact them. Table I presents the different threats that have been identified as well as the proposed solutions for them.

This paper is focused on authentication of power-hungry devices with common IDs in home smart meters, and mutually authenticating signals exchanged between grid control center and smart meters.

IV. DESIGN

The general architecture of communication among entities in IoT of power-hungry devices in smart grid environment is depicated in Fig. 2. Primarily, the network can be divided into three layers.

1) Home Area Network (HAN)
   This network is present at the customers' end, and is at the lowest end of the hierarchical communication framework in smart grids. HAN can be seen as a network within a house or within an apartment in a building. Typical HAN network of power-hungry devices having IP address within an apartment is shown in Fig. 3. Smart meters installed at HAN, HANSM allows customers' to efficiently and economically manage their power-hungry appliances in real-time or ahead of time. Keeping in mind the reported use of common IDs of power-hungry home appliances in [5], it is assumed that those common IDs means the IP address of the power-hungry devices within HAN.
2) Building Area Network (BAN) The BAN is a combination of number of HANs. They can be viewed as a network within an building with number of apartments or a community of few houses. They smart meter at BAN manages the power consumption of a building or an area. It can be implied that this network is under single authority or a single group. Therefore, utility makes an demand-response agreement at BAN network level, rather than HAN level. Conventional WiFi or WiMax may be

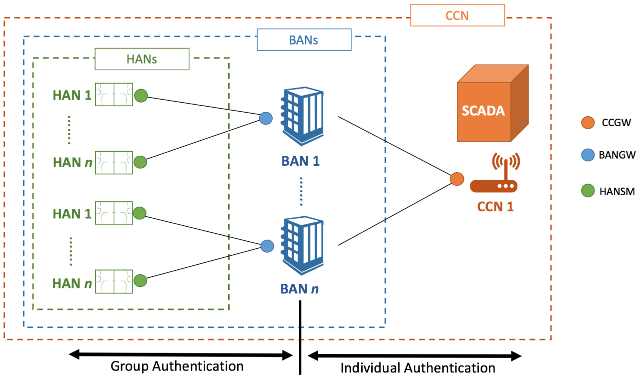

Fig. 2. General layout of communication from HAN to CCN.

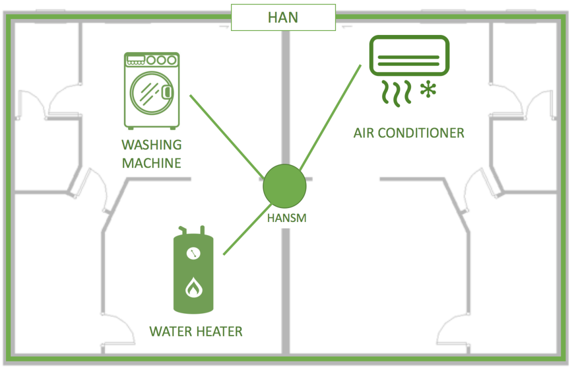

Fig. 3. Typical HAN structure.

employed at BAN based on its area covered.

3) Control Center Network (CAN)
This network can cover the main control center of grid, i.e. SCADA or regional control centers communicating with SCADA. Through the SCADA or Control Center Gateway (CCGW), the power-grid operator can control the power consumption of power-hungry home appliances in real-time. Since, the network coverage area is larger and crucial, WiMax or other relevant broadband wireless technologies can be employed for CAN.
The proposed authentication scheme should have the following properties to enhance security of IoT of power-hungry devices.
    a) Minimizing the computational overhead of BAN, i.e. increased efficiency.
    b) Isolation of malicious meters, i.e. minimizing the effect
    c) Scaleable solution
    d) Avoiding Replay attacks
    e) Secure Authentication

V. Implementation

The problem of authentication is divided into two folds; group authentication within BAN, and one-to-one mutual authentication between $BANGW$ and $CCGW$.

A. Group Authentication between $HANSM$ and $BANGW$

The group authentication of power-hungry home appliances like air-conditioners, water heaters, washing machines, etc within a BAN can be done as explained in [8]. The group authentication process primarily consist three phases, namely (i) Node Registration Phase, (ii) Group Authentication Phase, and (iii) Group Session Key Distribution Phase. In Node Registration Phase, $BANGW$ calculates a secret value, issues distributed secret values to each HAN smart meters, $HANSM$, using a threshold secret sharing scheme [8], [9]. In Group Authentication Phase, the each $HANSM$ generates authentication tokens using the secret values received from $BANGW$ at the Registration Phase, and sends them to $BANGW$. Then the $BANGW$ authenticates the group of $HANSM$ using the distributed secret values assigned to each $HANSM$ and and the tokens received from them. In the Group Session Key Distribution Phase, $BANGW$ generates a group session key, encrypts it and sends to $HANSM$. Then, $HANSM$ decrypt using the distributed secret value assigned at the first phase, and transmit data.

B. One-to-one Mutual Authentication between $BANGW$ and $CCGW$

Let us consider the private and public key pairs of i^{th} BAN gateway, $BANGW_i$ be $PubK_{SMGW_i}$ and $PrivK_{SMGW_i}$, respectively. Similarly, $PubK_{CCGW_j}$ and $PrivK_{CCGW_j}$ be the public key and private key pairs of j^{th} control center gateway $CCGW_j$, respectively. The Diffie-Hellman key establishing and sharing method is used for the initial handshake between $BANGW_i$ and $CCGW_j$.

Diffie-Helmen key establishment should hold Computational Diffie-Hellman (CDH) assumption. CDH assumption states that the computational problem is hard within a cyclic group. Let G be the cyclic set of large prime order q. Then, for $\{g, g^a, g^b\}$, where g be a generator randomly chosen from G and a, b are some unknown numbers, it is computationally complex to compute $g^{ab} \in G$. Based on the well established CDH, the proposed authentication method is explained further.

First, $BANGW_i$ chooses a random secret number $a_i \in Z_q$ and computes $A_i = g^{a_i} \bmod q$, and sends the A_i to $CCGW_j$. Similarly, $CCGW_j$ calculates $B_j = g^{b_j} \bmod q$, and sends to $BANGW_i$, where b_j is a secret number of $CCGW_j$. Then $BANGW_i$ and $CCGW_j$ calcutes $s_i = B_j^{a_i} \mod q$ and $s_j = A_i^{b_j}$, respectively. Fortunately, $s_i = s_j$, and hence is the shared secret key between $BANGW_i$ and $CCGW_j$.

In this mathematical framework, a_i and A_i are the $PrivK_{SMGW_i}$ and $PubK_{BANGW_i}$ of $BANGW_i$, respectively. Simillarly, b_j and B_j are the $PrivK_{CCGW_j}$ and $PubK_{CCGW_j}$ of $CCGW_j$, respectively. The shared key is then used for message authentication.

VI. Evaluation

The essence of group authentication is to reduce the computational overhead of the $BANGW$ to which numbers of power-hungry devices interact via $HANSM$. The evaluation of the proposed authentication scheme modified from [8], [10] is done under following headings.

A. Authentication

The $HANSMs$ are authenticated simultaneously by $BANGWs$, whereas the $BANGWs$ and $CCGWs$ are authenticated on an individual basis. Unlike one way authentication in group authentication protocol, $BANGWs$ and $CCGWs$ are also mutually authenticated. This mutual authentication is of high importance in case of communication between $BANGWs$ and $CCGWs$ compared to the communication between $HANSMs$ and $BANGWs$.

B. Efficiency

Computational overhead in $BANGWs$ are reduced during the group authentication of $HANSMs$. However, computational efficiency of Diffie-Helmen key exchange protocol has to be reasoned from the prospective of crucial nature of communication between $CCGWs$ and $BANGWs$.

C. Preventing Replay attacks

In case of proposed group authentication scheme, the secret value, distributed secret value, and master key of $BANGWs$ cannot be known even if intermidiate values of tokens generated by $HANSMs$ are attacked [8]. For the authentication between $BANGWs$ and $CCGWs$, authors in [10] have claimed resistance over replay attacks by using recorded time instance of sending message, i.e. the message will be sent with some validation time.

D. Identifying Malicious Participants

To prevent malicious participants from communicating, authors in [8] have proposed Chien scheme as presented in [11].

VII. Related Solutions

Authors in [12] have discussed about the communication between SMs in a NAN and how they are authenticated for communication of signals within themselves and thus authenticate with the HANs. The two-way secure authentication scheme described in the paper. When a smart meter wants to communicate with the gateway(GW), both parties new smart meter (SM) and GW can verify the authenticity of each other. The authenticity of GC is varied since the Authentication Request from the SM is encrypted using GWs key. It works as follows: SM will send an authentication request. The Network Operations Center(NOC) is a central authority which authenticates every node. NOC will validate data and send back an authentication response. This response contains the encrypted master key (MK) for the gateway which is handling that SM. The gateway will generate a random key(R) and send it to the new SM. Upon receiving, SM will send acknowledgement to the gateway. The gateway then multicasts the R to the group.

Once the SM is in the system, whenever it wants to communicate with the NOC, it sends the packet to one of its neighbours, through which it will eventually reach the NOC. Then, it sends the packet by applying a one way hash function on R and thus creating an encryption key, K. It then generates a MAC for the message using this key. The neighbour validates the message with the MAC and knowing what source it came from it generates the forwarding key of the source.

Authors in [13] focused on mutual communication between BANGW and SM in HAN. When a smart meter joins a smart grid, it first registers itself with the BANGW. This communication takes place with the help of a session key. Following is the process. The SM will first register iself in the BAN by submitting its ID and h(SN), which is modified secret number embedded by the manufacturer. Once this is done, the BANGW will compute a secret value for the SM and stores it. So the BANGW will have the ID and secret values. Once registration is done, the next step is to verify the SM and BANGW with each other and generate a session key which will be shared between them only. [4] also introduces two schemes to refresh the session keys. Finally, when the BANGW needs to send a command to a group of SMs, he Sm will receive a message containing the ID, key(Kg) and time stamp. Each SM will thus verify these details and check if the commands come from the valid BANGW. Once it verifies the message successfully, it will decrypt and send it back to the BANGW. The BANGW then adds the SM to its multi cast group and they communicate using key(Kg).

VIII. Conclusion

In this paper, authentication of power-hungry home appliances in smart grid environment is presented. The proposed scheme authenticates the entities in two layers; group authentication of power-hungry devices or HANSMs in BANGW, and one-to-one mutual authentication between BANGWs and CCGWs based on Diffie-Hellman key exchange protocol. The group authentication is proposed for the sake of reducing computational overhead in BANGWs. The proposed one-to-one mutual authentication between BANGWs and CCGWs are necessary so as to respect their crucial nature. In other words, a compromised BANGW with group authenticated power-hungry devices can be isolated if there is one-to-one authentication between BANGWs and CCGWs, and hence contain the attack within an smaller area only.

References

[1] S. Acharya, M. S. El Moursi, and A. Al-Hinai, "Coordinated frequency control strategy for an islanded microgrid with demand side management capability," *IEEE Transactions on Energy Conversion*, vol. 33, no. 2, pp. 639–651, 2018.

[2] "Use of energy in united states," https://www.eia.gov/energyexplained/index.php?page=us_energy_homes.

[3] "Madiot attacks on home appliances could take down power grids," https://www.welivesecurity.com/2018/09/06/madiot-home-appliances-power-grids/.

[4] "Utility companies: Rethink your iot information security strategy," https://chaione.com/blog/utility-company-iot-information-security-strategy/.

[5] "How to hack the power grid through home air conditioners," www.wired.com/2016/02/how-to-hack-the-power-grid-through-home-air-conditioners/.

[6] "Uk smart meters could be vulnerable to cyber attacks - gchq warns," https://www.information-age.com/smart-metres-vulnerable-cyber-attacks-123470837/.

[7] "Why you need timely patching and multi-factor authentication in the iot," https://arcticwolf.com/blog/why-you-need-timely-patching-and-multi-factor-authentication-in-the-iot/.

[8] D.-H. Lee and I.-Y. Lee, "Dynamic group authentication and key exchange scheme based on threshold secret sharing for iot smart metering environments," *Sensors*, vol. 18, no. 10, p. 3534, 2018.

[9] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

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

[11] H.-Y. Chien, "Group authentication with multiple trials and multiple authentications," *Security and Communication Networks*, vol. 2017, 2017.

[12] B. Alohali, K. Kifayat, Q. Shi, and W. Hurst, "Group authentication scheme for neighbourhood area networks (nans) in smart grids," *Journal of Sensor and Actuator Networks*, vol. 5, no. 2, p. 9, 2016.

[13] L. Yan, Y. Chang, and S. Zhang, "A lightweight authentication and key agreement scheme for smart grid," *International Journal of Distributed Sensor Networks*, vol. 13, no. 2, p. 1550147717694173, 2017.