Preprints of the 18th IFAC World Congress
Milano (Italy) August 28 - September 2, 2011

# Cyber Security and Information Protection in a Smart Grid Environment

**Shinn-Shyan Wu*. Chen-Ching Liu****
**Ahmed F.Shosha***. Pavel Gladyshev******

*,**School of Electrical, Electronic, and Mechanical Engineering, University College Dublin, Ireland
(e-mail: shinn-shyan.wu@ucdconnect.ie*, liu@ucd.ie**).
***,****School of Computer Science and Informatics, University College Dublin, Ireland
(e-mail: ahmed.shosha@ucdconnect.ie***, pavel.gladyshev@ucd.ie****)

Abstract: The concept of smart grid is built on both electrical and two-way information flow, which is intended to facilitate efficient usage of energy for the future. However, cyber security and information privacy issues have raised concerns as potential loopholes since large-scale communication networks will be needed to connect numerous devices from geographically dispersed sites to a control centre. Leakage or manipulation of sensitive operational data in a smart grid may result in serious financial losses as well as power system contingencies. Hence, for the interdependencies between the electric power infrastructure and networked computers, defence of the cyber network in a smart grid must be strengthened in order to avoid catastrophes that can be caused by electronic intrusions. The focus of this paper is to propose intrusion prevention systems to provide secure communications in a smart grid environment. Detailed functions of intrusion prevention systems are described and attack scenarios are developed to validate the effectiveness of the proposed methodology.

*Keywords:* smart grid, cyber security, information security, intrusion prevention system, information and communications technology

## 1. INTRODUCTION

### *1.1 Existing Electric Grid*

Although new controls have been developed and deployed on the electric power grids, the low level of investment and automation in the distribution level network is a bottleneck for further enhancement of power system reliability as most of power failures are due to incidents in distribution networks [Xu et al. 2007]. The Supervisory Control And Data Acquisition (SCADA) and Energy Management System (EMS) are centralised, primary control systems for monitoring and control of the power grid. They are principally focused on the transmission level networks. The lack of real-time information acquired from the distribution networks is a hurdle that needs to be overcome in order to achieve a step change in monitoring, control, and outage recovery of the distribution feeders.

### *1.2 Smart Grid Concepts*

Due to the lack of investment and aging of the power infrastructure, the future operating efficiency and system security become major challenges. Through modernisation of grid monitoring, automation and energy information management, the reliability and quality of power grid can be further improved. A major effort in modernisation is in the area of Smart Grid (SG). Background information on SG in different sectors can be found in [Amin et al. 2005].

### *1.3 Advanced Metering Infrastructure*

Forced power outages can be caused by the following incidents:

(1) Faults and accidents on power lines.

(2) Severe weather conditions.

(3) Intrusions and sabotage.

An important objective of SG is to create highly automated and sustainable distribution networks, including consumers on the demand side. In a research report, it is expected that the global Advanced Metering Infrastructure (AMI) market will be over $30 billion by 2030, and the goal of current US policy is to install 40 million smart meters by 2012 [Morgan Stanley Research 2009].

The renovation applied to the demand side is composed of automation and Distributed Energy Resource (DER) systems. The demand side automation includes a Home Area Network (HAN) that controls in-home appliances and Home Energy Management System (HEMS). The enabling technology to support these functions includes an AMI which is intended to realise the functional requirements stated in [Brockway N. 2008].

All functional requirements are meant to enhance the interaction between utilities and consumers to achieve an efficient electric power grid by real-time energy information gathering based on AMI.

### *1.4 Information and Communications Technology Networks*

Through the integration of information & communications technology (ICT) networks into existing electric power grids, monitoring and data acquisition devices will be networked to enable real-time operation and control at all levels. ICT networks which utilise available communication

technologies, such as ADSL, dedicated lines, GSM, GPRS, Wi-Fi, WiMax, Broadband over Power Line (BPL), provide two-way communication channels between the control centre and consumers. Data are transmitted through the ICT networks and processed to generate the necessary information for operation and control.

### *1.5 Prerequisites for Information and Communications Technology Networks*

As mentioned, power outages can be caused by natural disasters and severe weather conditions [Luan et al. 2010], ICT networks must have the following prerequisites to support the critical data acquisition and control functions:

(1) Heterogeneous medium: In case the communication medium malfunctions, ICT networks should have the backup capability.

(2) Low latency: Since the interconnectivity is extensive and widespread, ICT networks have to have a low latency to ensure reliability of the transmission for necessary energy data and control signals, especially in a time critical environment.

(3) High bandwidth: When power outages occur, ICT networks are highly critical due to the larger volume of data and information. ICT networks must have a high bandwidth to accommodate the critical information flow.

(4) High information security: As energy data are sensitive and essential for maintaining a normal power grid operating condition, the networks must meet a high information security requirement.

The key to success of a SG is the ICT networks at all levels in the electric power grid. In this paper, cyber security schemes are proposed to ensure the information security for both consumers and critical substations in a SG environment. Section 2 discusses the information security issues in a SG environment. Section 3 provides the proposed security schemes for both consumers and critical substations. The conclusion is given in Section 4.

## 2. INFORMATION SECURITY CHALLENGES IN SMART GRID

### *2.1 Cyber Network and Physical System*

As a result of the interdependencies between cyber and physical systems [Ten et al. 2008], power systems face challenges in data privacy and protection as they are transformed into a SG environment [NIST 2010]. In a SG, data need to be collected and transmitted through ICT networks. Analysis of the acquired data leads to appropriate operation and control actions. SG enhances efficiency of electric power grid operation by enabling consumer participation. However, there are also potential areas where security breaches of the cyber system can lead to intrusions into the electric power grid through ICT networks that are based on standardised technologies [Ericsson 2010]. If the energy data are tampered with, it could lead to thefts or billing problems. It may also affect the grid operation as incorrect controls. Information security incidents may cause major power outages and lower the overall system reliability. A survey based on 443 respondents indicates that an average financial loss of $234,444 is caused by information security incidents [CSI 2009]. In 2009, it was demonstrated that a smart meter can be hacked and the implemented malicious code can be spread from a meter to another [Davis 2009].

### *2.2 Privacy Concerns in Smart Grid*

ICT networks in an electric power grid are not publicly-accessible in the current environment. To implement a SG, communication channels are dedicated, SG will give end users the opportunities to participate in the market. Therefore, the access to ICT networks will be much expanded. Smart meters will be installed to numerous end consumers. As a result, there may be associated cyber vulnerabilities and intrusions [Boroomand et al. 2010, Clements et al. 2010]. If a smart meter is installed outside the premise, it could be hacked and reprogrammed by a hacker. Furthermore, if the hacked smart meter shares the same communication channel with the home personal computer (PC), it could become a rouge point to attack other devices and provides a direct link between consumers and the hacker.

### *2.3 Data Protection in Smart Grid*

SG is formed by networked devices from all levels of the power grid, and ICT networks are responsible for transmitting the necessary data to Energy Management System (EMS) and market applications. Hence, confidentiality, integrity, and availability are crucial for the grid operation. In [Metka et al. 2010], several security technologies are identified to address the SG security requirements, especially through the adaptation of Public Key Infrastructure (PKI) technologies.

## 3. PROPOSED SMART GRID SECURITY SCHEMES

The SG takes advantage of information technologies to add smartness to a traditional electric power grid and gives consumers and utilities more options to control over the energy usage. However, the increasing interconnectivity brings the threat of hacking that already trouble the Internet. In this section, two types of IPSs will be proposed to secure the SG from two aspects, consumer end and substation which serves as a critical cyber asset in a power grid.

### *3.1 Protection at Last Mile*

A Home Area Network (HAN) is a residential area network for communication between digital devices in the SG environment. Examples of devices in a SG HAN are In-Home Display (IHD), thermostat, hot water boiler, smart appliances, home PCs, and smart meters. The Home Energy Management System (HEMS) utilises HAN to integrate home digital devices and controls the connected devices. A Home Intrusion Prevention System (Home-IPS) is proposed to secure the HAN, the last mile in a SG. Fig. 1 depicts where a Home-IPS is deployed in a HAN.

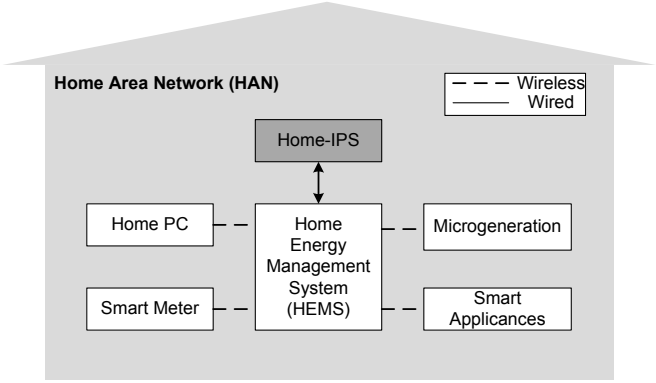


Fig. 1. Home-IPS in a HAN.

The main capabilities of the proposed Home-IPS are given below:

The Home-IPS is intended to protect the devices connected to HEMS from unauthorized access, modification, or disruption and guard upstream networks.

The Home-IPS sits in-line on the communication paths of HEMS and inspects all incoming and outgoing traffic.

The traffic on a Home-IPS can be categorized into 2 aspects:

(1) From User: Request to read data (e.g., real-time energy consumption).

(2) From Utility or Service Provider: (i) Request to read data (e.g., electricity usage pattern), (ii) Send notification (e.g., pricing signals), (iii) Demand response management, (iv) Software/firmware update.

The workflow of a Home-IPS is divided into 3 phases: Initialisation, Detection, and Decision Phase.

(1) Initialisation Phase: All traffic on HEMS will be captured by the HEMS Network Interface, and the traffic will be parsed by information stored in the packet header. The Initialisation phase is designed to facilitate the downstream phases.

(2) Detection Phase: After the traffic is parsed, packets that use different protocols will be decoded for signature matching which is conducted by comparing data packets with signatures stored in the Signature DB. The signatures can be customised to examine the data packets for various security requirements. Further details on how a signature is used to detect security violations are given in Section 3.3.

(3) Decision Phase: The main mitigation mechanisms are described in this phase. If an intrusion is detected, predefined mitigation plans will be taken in the Decision Phase which is generally classified into denial of malicious packets and sessions, alarm generation, and event logging.

*3.2 Home-IPS Examination Algorithm*

A HAN is similar to a local area network which is designed to be controlled under private administration. Base on this characteristic, a consumer is able to identify what assets are included and can be managed through HEMS. Hence, a trusted source set which described the in-home assets can be defined on Home-IPS to block unauthorized access and further cyber intrusions. Often the rules defined in Table 2 rely on the trusted source set definition which is the first line to stop the hacker at the earliest possible time. The other attributes used to complete the signature matching process are destination IP, command, file type, and limit. The notation for different attribute sets is listed in Table 1. The symbols $\alpha$, $\beta$, $\gamma$, $\theta$, $\mu$ and $\lambda$ indicate different conditions for various security levels. For example, $Y_1$ and $Y_2$ represent two command sets under different protocols.

| Attribute Sets for Home-IPS | |
|---|---|
| **Set** | **Attribute** |
| $W_\alpha$ | Trusted source |
| $X_\beta$ | Destination IP |
| $Y_\gamma$ | Command |
| $Z_\theta$ | File type |
| $L_\mu$ | Limit |
| $M_\lambda$ | Malicious data packet |
| $V_\lambda$ | Security violation indicator |

Table 1. Attributes for Home-IPS.

The trusted source can be formed by hostname (HN), IP and MAC address entries, and the corresponding attribute sets are constructed as follows:

$$W_\alpha := \{[\mathrm{HN_i}, \mathrm{IP_i}, \mathrm{MAC_i}], [\mathrm{HN_{i+1}}, \mathrm{IP_{i+1}}, \mathrm{MAC_{i+1}}], \cdots, [\mathrm{HN_j}, \mathrm{IP_j}, \mathrm{MAC_j}]\} \quad (1)$$

$$X_\beta := \{[\mathrm{Destination_i}], [\mathrm{Destination_{i+1}}], \cdots, [\mathrm{Destination_j}]\} \quad (2)$$

$$Y_\gamma := \{[\mathrm{Command_m}], [\mathrm{Command_{m+1}}], \cdots, [\mathrm{Command_n}]\} \quad (3)$$

$$Z_\theta := \{[\mathrm{File_p}], [\mathrm{File_{p+1}}], \cdots, [\mathrm{File_q}]\} \quad (4)$$

$$L_\mu := \{[\mathrm{Limit_f}], [\mathrm{Limit_{f+1}}], \cdots, [\mathrm{Limit_g}]\} \quad (5)$$

where i, m, p, and f denote the minimum entry, and j, n, q, and g denote the maximum entry for each attribute, respectively.

In the signature matching process, the proposed Home-IPS calculates the intersection of the overall attributes defined in the signature rule fields for each data packet and give a [0,1,2] output to demonstrate if there is a security violation against the data packet. Two functions are defined for the signature matching process on a Home-IPS:

$$\tau_{\mathrm{H1}} := W_\alpha' \cap X_\beta \cap Y_\gamma \cap (Z_\theta \wedge L_\mu) \rightarrow M_{H1} \quad (6)$$

$$\tau_{\mathrm{H2}} := W_\alpha \cap X_\beta \cap Y_\gamma \cap (Z_\theta \wedge L_\mu) \rightarrow M_{H2} \quad (7)$$

where $W_\alpha'$ is the complement of $W_\alpha$.

Eq. (6) is used to capture the unauthorised access with malicious behaviours while Eq. (7) detects the trusted devices with malicious behaviours. If Eq. (7) is valid for a data packet, it serves as a warning that a trusted source set is compromised.

After the signature matching process is completed, a home security violation indicator, $V_H$ is given in Eq. (8):

$$V_H = \begin{cases} 2, \text{if } \tau_{H1} \subseteq M_{H1} \\ 1, \text{if } \tau_{H2} \subseteq M_{H2} \\ 0, \text{otherwise} \end{cases} \quad (8)$$

where 2 and 1 indicate, respectively, that a data packet meets the rule set in a signature, and 0 shows no evidence of cyber intrusions.

The proposed Home-IPS examination algorithm, HIPSEA, describes the overall data packet examination process on a Home-IPS. The captured data packets will be inspected by the predefined signatures stored in the Signature DB. The result of HIPSEA is to determine if a security violation is detected.

HIPSEA:

1: $V_H$ =0; #Initialise home security violation indicator as zero
2: $I_1$= [*K* data packets] ; #Load *K* data packets captured from HEMS network interface
3: $I_1 \rightarrow I_{2,(Kx2)}$; #Parse the *J* data packets based on protocols used for non-trusted source set
4: $I_1 \rightarrow I_{3,((K-J)x2)}$; #Parse the *K-J* data packets based on protocols used for trusted source set
5: $I_{2,(Kx2)} \rightarrow I_{4,(5Jx3)}$; #Decode the *J* data packets to get the attributes for non-trusted source set
6: $I_{3,(Kx2)} \rightarrow I_{5,(5(K-J)x3)}$; #Decode the *(K-J)* data packets to get the attributes for trusted source set
7: $\tau_{H1} = I_{4,(5Jx3)}$ ; #Assign the attributes to $\tau_{H1}$
8: $\tau_{H2} = I_{5,(5(K-J)x3)}$ ; #Assign the attributes to $\tau_{H2}$
9: $\tau_{H1} := W_\alpha' \cap X_\beta \cap Y_\gamma \cap (Z_\theta \wedge L_\mu) \rightarrow M_{H1}$ # Calculate the home security violation for non-trusted source set
10: $\tau_{H2} := W_\alpha \cap X_\beta \cap Y_\gamma \cap (Z_\theta \wedge L_\mu) \rightarrow M_{H2}$ # Calculate the home security violation for trusted source set
11: if $\tau_{H1}$ is contained in $M_{H1}$
12: Set $V_H$ =2; # Detect an unauthorised access with malicious behaviours
13: if $\tau_{H2}$ is contained in $M_{H2}$
14: Set $V_H$ =1; # Detect malicious behaviours from a trusted source
15: return $V_H$

This algorithm is organised to clearly illustrate the Initialisation and Detection Phase on a Home-IPS. Lines 1 to 4 initialise the examination process. Lines 5 to 8 decode the data packet for signature matching. Lines 9 to 14 check the existence of home security violations. Finally, as Line 15 is reached, a conclusion is reached as to whether a malicious activity exists.

### *3.3 Home-IPS Framework Architecture*

In this section, a hybrid-type architecture for Home-IPS is proposed. The architecture contains two major components that are responsible for signature based detection and anomaly based detection. A current Intrusion Detection System (IDS) such as SNORT [Roesch 1999] detects the attacks based on prior knowledge of the attack signatures. However, these types of IDS could not detect the zero-day attacks. Anomaly based IDS could detect unknown attacks that do not conform to the normal behaviour. However, an anomaly based IDS has a high level of false alarms due to uncertainty associated with their detection decisions [Werlinger 2008] [Gates 2006].

Therefore, a hybrid architecture for Home-IPS is proposed that combines both advantages of signature based and anomaly based IDSs.

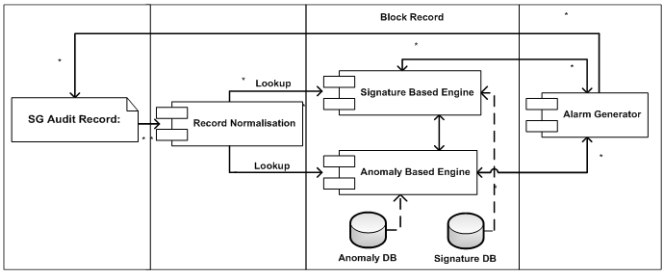


Fig. 2. Home-IPS framework architecture.

As illustrated in Fig. 2, the process of detection and prevention of anomalous packets is described by the following procedure:

(1) Extract the packet data and normalise the selected vector data using a standard data normalisation technique. The data items in each packet have been represented using the following features: time stamp, source IP, destination IP, used protocol and associated information such as window size, and packet sequence number.

| | | | |
|---|---|---|---|
| Signature ID | # A serial number used to identify a specific signature # | Severity | # Field used to indicate the severity of a signature # |
| Signature Name | #Name for a set of rules in a signature # | Protocol | # Field used to indicate which protocol is used in a signature # |
| Rules | # A series of rules to describe the signature matching process # | | |
| Detection Result | # A value that indicates the security condition of the protected network # | | |
| Mitigation Actions | Automatic<br># Predefined mitigation actions that will be performed automatically # | | Manual<br># Mitigation actions that needed to authorised # |

Table 2. Signature template for proposed security schemes.

(2) After extracting the packet data, Signature Based Engine component is in charge of the lookup process in the Signature DB and compares captured data to the known attack signatures. The Attack signatures are defined by the following feature: signature ID, severity, signature name, used protocol, rule which describes whether the action should be taken based on weights of data packets features, detection result, and, finally, the response describes the mitigation plan that mitigate the attack action. In Table 2, a signature template with explanation for each field is shown.

(3) After verifying the packet data, the component will generate an alarm and block the data packet and associated events if and only if the lookup process has indicated the identity of packet with the attack signature. If the lookup process fails to verify if the data packet contains attacks, it forwards the data packet for anomaly detection. A signature based IDS is not able to capture unknown attacks. So, the generalisation of the signature DB and discovery of unknown attacks is performed by Anomaly Detection Engine (ADE).

ADE has been trained using labelled data to detect and classify the coming data packet into normal and abnormal data. If ADE has classified the data packet as an attack, the component generates a signature for the attack and updates the Signature DB. After updating the Signature DB, an alarm signal is sent to alarm generator component that blocks the packet data and prevents the associated events from execution.

The above procedure has to be taken for each audit record to ensure that all data packets are free from malicious activities and attacks.

*3.3 Scenarios for Home-IPS*

In this section, three scenarios have been developed to verify the effectiveness of the proposed Home-IPS. The scenarios are A: Attack within HAN, B: Attack from HAN to substation C: Attack from the Internet to HAN. Different signatures are created for these scenarios.

**(1) Scenario A: Attack within HAN**

A knowledgeable hacker (IP: 10.0.0.5/24) knows how to crack the wireless connection password and penetrates into the HAN as shown in Fig. 3. The Hacker intends to retrieve the consumer's electricity usage pattern from the smart meter (IP: 10.0.0.7/24) to plan when to break into the premise. The Home-IPS captured the data packets sent from the hacker in the HAN. The hacker intends to retrieve the /SmartMeter_SecZone/usage.info file on the smart meter which reveals the consumer's activities at home, and has been detected as the behaviour of data packet matches a predefined signature in Table 4. The data packet has been flagged as anomalous, and so the mitigation actions will be taken to stop the attack.

**(2) Scenario B: Attack from HAN to Substation**

In Fig. 4, the hacker (10.0.0.5/24) intrudes into a HAN and launches a Denial of Service (DoS) attack against Human Machine Interface (HMI) (IP:10.1.0.8/24) in a substation during peak hours. The DoS attack will cause the target substation to lose its availability to intended users. If a necessary change of power system topology needs to be implemented when a contingency occurs, a substation which suffers from DoS attack will not be able to perform the task. This may result in cascading events that can bring down the entire power grid.

The signature shown in Table 5 developed in Scenario B is to prevent substations from receiving excessive Ping requests. When a large volume of data packets contain Ping requests sent from a hacker, the Home-IPS stops the traffic from going any further as the Ping requests come from a non-trusted source, and the repeating rate is larger than a predefined threshold.

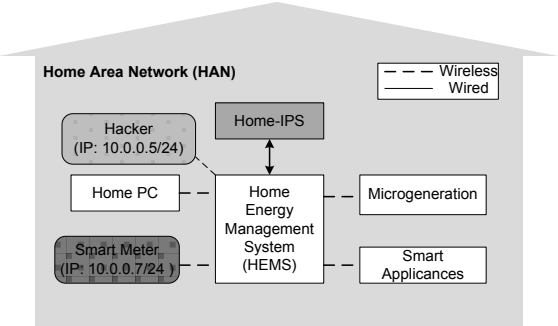


Fig. 3. Scenario A: Attack within HAN.

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| * | * | * | * | * | * |
| 6 | 30.3511 | 10.0.0.5 | 10.0.0.7 | TCP | 8484 > http [SYN] Seq=0 Win=8192 |
| 7 | 30.3527 | 10.0.0.5 | 10.0.0.7 | TCP | 8484 > http [ACK] Seq=0 Win=8192 |
| * | * | * | * | * | * |
| 9 | 30.3578 | 10.0.0.5 | 10.0.0.7 | HTTP | GET /SmartMeter_SecZone/ usage.info |

Table 3. Captured packets sent from hacker.

| Signature ID | HAN-001 | Severity | High |
|---|---|---|---|
| Signature Name | Critical Privacy Related Files | Protocol | HTTP |
| Rules | $W_1'$ : Source IP & MAC $\neq$ Trusted source set<br>&<br>$X_1$ : **Destination IP == 10.0.0.7**<br>&<br>$Y_1$ : Command == GET<br>&<br>$Z_1$ : File Type == /SmartMeter_SecZone/ *.info | | |
| Detection Result | $V_H = 2$ | | |
| Mitigation Plans | Automatic<br>Deny Attack Inline<br>Reset TCP Connection<br>Produce Alarm<br>Produce Log | Manual<br>Request to unblock host | |

Table 4. Signature ID: HAN-001 for Scenario A.

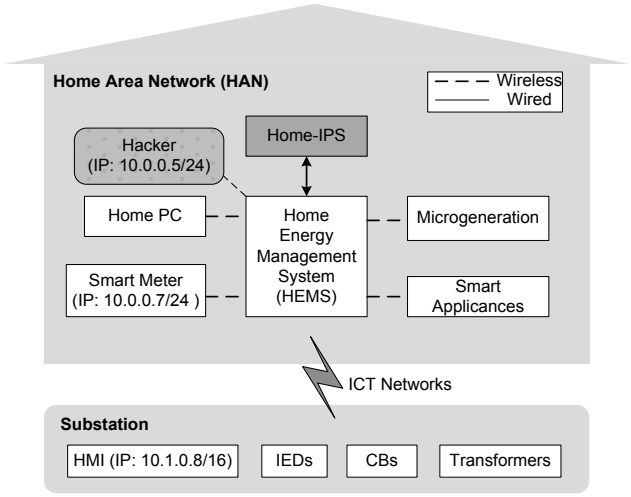


Fig. 4. Scenario B: Attack from HAN to Substation.

| Signature ID | HAN-002 | Severity | High |
|---|---|---|---|
| Signature Name | Rouge Point | Protocol | ICMP |
| Rules | $W_2'$ : Source IP & MAC Address $\neq$ Trusted source set<br>&<br>$X_2$ : **Destination IP == 10.1.0.8 (Hostname: HMI)**<br>&<br>$Y_2$ : Command == ECHO Reply<br>&<br>$L_2$ : Ping Request Repeating Rate > Threshold % | | |
| Detection Result | $V_H = 2$ | | |
| Mitigation Plans | Automatic<br>Deny Attack Inline<br>Reset TCP Connection<br>Produce Alarm<br>Produce Log | Manual<br>Request to unlock host | |

Table 5. Signature ID: HAN-002 for Scenario B.

**(3) Scenario C: Attack from the Internet to HAN**

As illustrated in Fig. 5, the home PC (IP: 10.0.0.6/24) with an Internet connection is compromised by malware which is designed to receive control commands from an unknown hacker on the Internet. The hacker (IP: 10.5.0.9/16) can exploit this comprised home PC as an intermediary machine to hack the smart meter by replacing the original configuration file in the smart meter (IP: 10.0.0.7/24) with a malicious one. It may cause a disruption of energy markets as incorrect meter readings can be sent.

The source IP & MAC address comes from the hacker is not trusted, and the packet is meant to replace the critical system file, /SmartMeter_SecZone/*.sys. Hence, this anomaly is captured by Home-IPS as the data packet is examined with the signature defined in Table 6. The Home-IPS secures the traffic that goes through the HEMS which acts as a central point for the HAN. By inspecting all the traffic granularly, various signatures can be customised to stop different attacks.

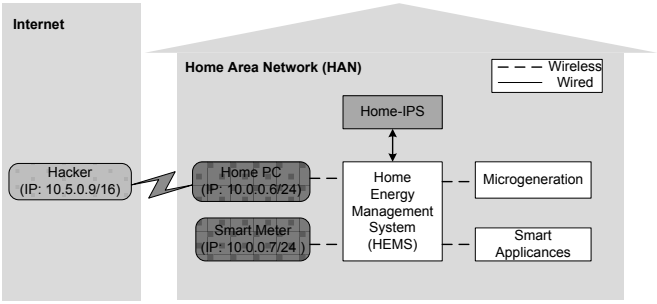


Fig. 5. Scenario C: Attack from the Internet to HAN.

| Signature ID | HAN-003 | Severity | High |
|---|---|---|---|
| Signature Name | Smart Meter Critical File Access | Protocol | HTTP |
| Rules | $W_3$ : Source IP & MAC Address == Trust source set<br>&<br>$X_3$ **: Destination IP == 10.0.0.7 (Hostname: Smart_Meter)**<br>&<br>$Y_3$ : Command == POST<br>&<br>$Z_3$ : File Type == /SmartMeter_SecZone/*.sys | | |
| Detection Result | $V_H = 1$ | | |
| Mitigation Plans | Automatic<br>Deny Attack Inline<br>Reset TCP Connection<br>Produce Alarm<br>Produce Log | Manual<br>Request to unblock host | |

Table 6. Signature ID: HAN-003 for Scenario C.

*3.4 Substation-IPS Examination Algorithm*

The power substations are critical nodes in an electric power grid. In a SG environment, if a hacker successfully penetrates into one or more substations, the damage can be significant due to the interdependencies between cyber network and physical systems as mention in Section 2.1. A Substation-IPS is proposed to mitigate possible cyber intrusions into a substation. It acts similarly to Home-IPS but takes one step further by having the ability to reconfigure other security devices and distribute new security rules within the protected network.

In a substation, the connected device must be predefined on HMI for centralised control. Hence, a site engineer can identify the number of substation devices through HMI. This is analogous to the HAN described earlier. Generally, the attributes used on proposed Substation-IPS to capture the anomalies are similar to Home-IPS. However, due to the different operating conditions that exist in a substation, time attribute is introduced to further address the security needs. The time attribute set is defined as follows:

$$C_\pi := \{[\text{Time}_u],[\text{Time}_{u+1}],\cdots,[\text{Time}_v]\} \quad (9)$$

where u and v denote the confined time intervals.

The signature matching process on Substation-IPS is given by Eq. (10) and (11).

$$\tau_{S1} \coloneqq C_\pi \cap W_\alpha' \cap X_\beta \cap Y_\gamma \cap \left(Z_\theta \wedge L_\mu\right) \rightarrow M_{S1} \quad (10)$$

$$\tau_{S2} \coloneqq C_\pi \cap W_\alpha \cap X_\beta \cap Y_\gamma \cap \left(Z_\theta \wedge L_\mu\right) \rightarrow M_{S2} \quad (11)$$

Once the signature matching process is completed, a substation security violation indicator, $V_S$ in Eq. (12) will be calculated to give the site engineer a quick understanding of signs of cyber intrusions.

$$V_S = \begin{cases} 2, \text{if } \tau_{S1} \subseteq \mathrm{M}_{S1} \\ 1, \text{if } \tau_{S2} \subseteq \mathrm{M}_{S2} \\ 0, \text{otherwise} \end{cases} \quad (12)$$

The Substation-IPS examination algorithm, SIPSEA, has the same logic as HIPSEA except that an added time attribute set is included in the examination process.

SIPSEA:

1: $V_S$=0; #Initialise substation security violation indicator as zero
2: $\mathrm{I_a}$= [*K* data packets] ; #Load *K* data packets captured from substation communication bus
3: $\mathrm{I_a} \rightarrow \mathrm{I_{b,\,(}}_{J\mathrm{x2)}}$; #Parse the *J* data packets based on protocols used for non-trusted source set
4: $\mathrm{I_a} \rightarrow \mathrm{I_{c,\,((}}_{K\text{-}J\mathrm{)x2)}}$; #Parse the *K*-*J* data packets based on protocols used for trusted source set
5: $\mathrm{I_{b,\,(}}_{K\mathrm{x2)}} \rightarrow \mathrm{I_{d,\,(}}_{6J\mathrm{x3)}}$; #Decode the *J* data packets to get the attributes for non-trusted source set
6: $\mathrm{I_{c,\,(}}_{K\mathrm{x2)}} \rightarrow \mathrm{I_{e,\,(}}_{6(K\text{-}J)\mathrm{x3)}}$; #Decode the *K*-*J* data packets to get the attributes for trusted source set
7: $\tau_{S1} = \mathrm{I_{d,\,(}}_{6J\mathrm{x3)}}$ ; #Assign the attributes to $\tau_{S1}$
8: $\tau_{S2} = \mathrm{I_{e,\,(}}_{6(K\text{-}J)\mathrm{x3)}}$ ; #Assign the attributes to $\tau_{S2}$
9: $\tau_{S1} \coloneqq C_\pi \cap W_\alpha' \cap X_\beta \cap Y_\gamma \cap \left(Z_\theta \wedge L_\mu\right) \rightarrow M_{S1}$ # Calculate the substation security violation for non-trusted source set
10: $\tau_{S2} \coloneqq C_\pi \cap W_\alpha \cap X_\beta \cap Y_\gamma \cap \left(Z_\theta \wedge L_\mu\right) \rightarrow M_{S2}$ # Calculate the substation security violation for trusted source set
11: if $\tau_{S1}$ is contained in $M_{S1}$
12: Set $V_S$=2; # Detect an unauthorised access with malicious behaviours
13: if $\tau_{S2}$ is contained in $M_{S2}$
14: Set $V_S$=1; # Detect malicious behaviours from a trusted source
15: return $V_S$

SIPSEA is organised to illustrate the Initialisation and Detection Phase on a Substation-IPS. Lines 1 to 4 initialise the overall examination process. Lines 5 to 8 decode the data packet for signature matching process. Lines 9 to 14 check the existence of substation security violations with the added time attribute. Finally, at Line 15, a conclusion is reached as to whether a cyber intrusion exists.

*3.5 Scenarios Development and Study for Substation-IPS*

In this section, three scenarios are developed to explain how the Substation-IPSs secure a critical substation. An example substation network is illustrated in Fig. 6. The devices in the substation network are HMI, Intelligent Electronic Devices (IEDs), merging units, actuators, sensors, and circuit breakers (CBs). The station bus and process bus are used to separate the substation network into different operation zones. A perimeter firewall (P_FW) is placed on the electronic perimeter of the substation network. In Fig. 7, the firewalls (FWs) and IPSs are deployed to partition the substation into different security zones.

**(1) Scenario D: Hacker on HMI**

The hacker (IP: 10.1.0.9/16) uses the correct user credentials to log in the HMI (IP: 10.0.1.214/24) via the web browser, and tries to retrieve the Substation Configuration Description file (*.SCD) to understand the substation layout and enumerate the devices in the substation.

In Fig. 7, IPS_1 notices this attack as the data packet meets the conditions described in the signature defined in Table 7. After the security violation is detected on IPS_1, the anomalous data packets will be blocked, and the hacker will not be able to retrieve the SCD file. A further action taken by IPS_1 is to log this event, generate the new security rule and distribute it to other security devices within the substation. The advantage of security rule generation-distribution mechanism is that it can be used to eradicate the hacker-related connections as the source IP and MAC addresses are reported as malicious in every substation security device.

**(2) Scenario E: Hacker on station bus**

The hacker penetrates into a station bus during maintenance hours, and tries to send commands to IEDs (IP: 10.0.2.215/24) in order to open CBs (IP: 10.0.3.0) controlled by the IED. However, the content of maintenance does not include an open command for any CBs.

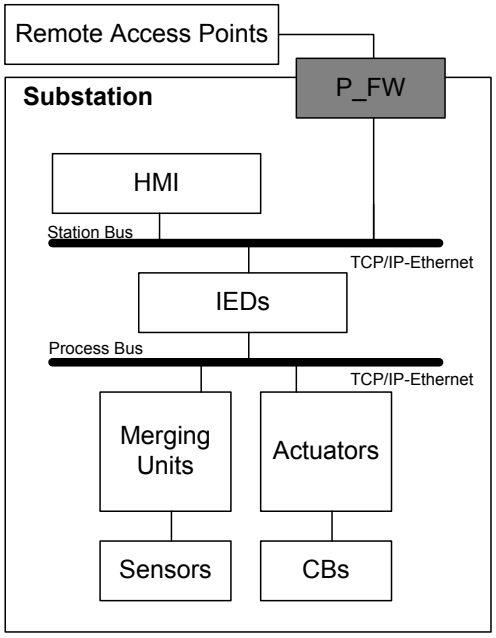


Fig. 6. Substation network.

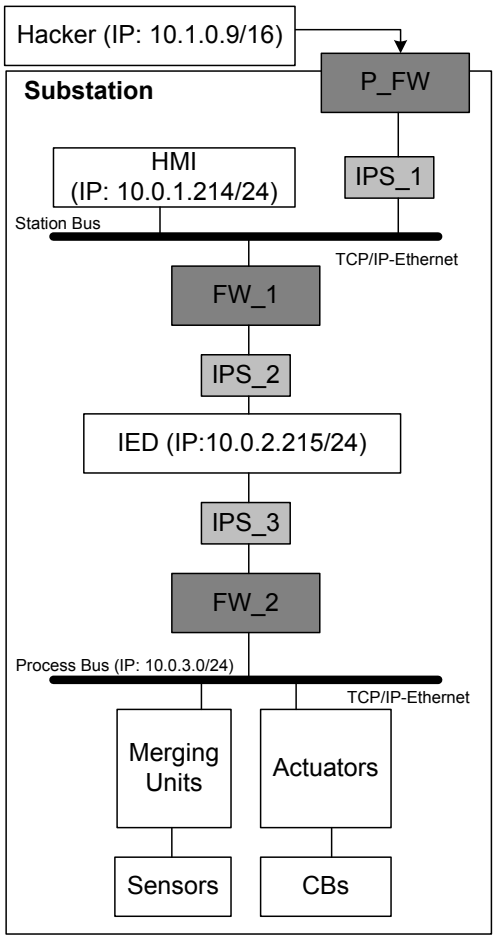


Fig. 7. Proposed security scheme in a substation.

IPS_2 shown in Fig. 7 detects the CB open command by inspecting the data packets sent from HMI to the IED, and IPS_2 with a predefined signature listed in Table 8 stops this anomalous traffic from reaching its destination.

| Signature ID | SIPS-01-001 | Severity | High |
|---|---|---|---|
| Signature Name | Substation Critical System Files | Protocol | HTTP |
| Rules | $C_4$ : Time ≠ Maintenance hours<br>&<br>$W_4'$ : Source IP & MAC ≠ Trust Set<br>&<br>$X_4$ **: Destination IP == 10.0.1.214 (Hostname: HMI)**<br>&<br>$Y_4$ : Command == GET<br>&<br>$Z_4$ : File Type == *.SCD | | |
| Detection Result | $V_S = 2$ | | |
| Mitigation Plans | Automatic<br>Deny Attack Inline<br>► Create New Security Rule on P_FW<br>► Distribute New Security Rule<br>Produce Alarm<br>Produce Log | Manual<br>Request to unblock host | |

Table 7. Signature ID: SIPS-01-001 for Scenario D.

| Signature ID | SIPS-02-001 | Severity | High |
|---|---|---|---|
| Signature Name | Unauthorised CB Commands During Maintenance Hours | Protocol | IEC 61850 based |
| Rules | $C_5$ : Time == Maintenance hours<br>&<br>$W_5'$ : Source IP & MAC ≠ Trust Set<br>&<br>$X_5$ **: Destination IP == 10.0.2.215 (Hostname: IED)**<br>&<br>$Y_5$ : Command == CB Open<br>&<br>$L_5$ : Number of CB open command > Threshold% per second | | |
| Detection Result | $V_S = 2$ | | |
| Mitigation Plans | Automatic<br>Deny Attack Inline<br>► Create New Security Rule on FW_1<br>► Distribute New Security Rule<br>Produce Alarm<br>Produce Log | Manual<br>Request to unblock host | |

Table 8. Signature ID: SIPS-02-001 for Scenario E.

**(3) Scenario F: Hacker on IED**

The hacker has compromised a PC in the utility corporate office and uses it to log in IED through direct access during non-maintenance hours, and tries to open all CBs controlled by the IED on the process bus network, 10.0.3.0. In Fig. 7, IPS_3 sits between the IED and the process bus. Hence, the commands destined to process bus that is aimed to change the power system topology will be inspected by IPS_3 with a signature defined in Table 9. IPS_3 stops the attack initialised by hacker who has the IED direct access privilege.

| Signature ID | SIPS-03-001 | Severity | High |
|---|---|---|---|
| Signature Name | Unauthorised CB Commands During Non-Maintenance Hours | Protocol | IEC 61850 based |
| Rules | $C_6$ : Time ≠ Maintenance hours<br>&<br>$W_6$ : Source IP & MAC == Trust Set<br>&<br>$X_6$ **: Destination IP == 10.0.3.0**<br>&<br>$Y_6$ : Command == CB Open<br>$L_6$ : Number of CB open command > Threshold% per second | | |
| Detection Result | $V_S = 1$ | | |
| Mitigation Plans | Automatic<br>Deny Attack Inline<br>► Create New Security Rule on FW_2<br>► Distribute New Security Rule<br>Produce Alarm<br>Produce Log | Manual<br>Request to unlock host | |

Table 9. Signature ID: SIPS-03-001 for Scenario F.

Since the substation has been partitioned into different security zones, and the new security rule is distributed within the substation to all security devices, the connections established for the hacker will be terminated. As a result, the hacker can no longer stay on HMI, IED, or any of the buses to sniff the traffic and modify the packets.

## 4. CONCLUSIONS

Cyber security is an important aspect in the smart grid design. This paper proposes a methodology for security design to protect a smart grid from cyber intrusions. Attack scenarios are developed to verify the efficacy the Home- and Substation-IPSs. Major implementation issues need to be addressed, such as whether the HEMS, IEDs and computer networks have the capabilities and computational resources to support intrusion prevention systems in a time critical environment. The severity field in the signature is designed to give the administrator a quick understanding of the severity of security threats when alarms are generated. According to different severity levels (high, medium, and low), the administrator is able to determine what threats should be focused on first. To set a proper severity level for each signature, a comprehensive study will be needed. Otherwise, the administrator may be flooded by an excessive number of urgent alarms. Classification of intruders from legitimate users is not a straightforward task. An accurate definition for members of the TRUSTED SOURCE SET is important. It will require a better clarification procedure and algorithm. As new security rules can be distributed between security devices, how to secure the rule during the distribution process is also an important area of research. The future work will include the implementation of the proposed IPSs on the cyber security test bed available to the research team.

## REFERENCES

Amin, S.M. and Wollenberg, B.F. (2005). Toward a Smart Grid: Power Delivery for the 21st Century. *IEEE Power and Energy Magazine,* vol. 3, no. 5, pp.34-41.

Boroomand, F., Fereidunian, A., et al. (2010). Cyber Security for Smart Grid: A Human-Automation Interaction Framework. *2010 IEEE PES Innovative Smart Grid Technologies Conference Europe*, pp. 1-6.

Brockway, N. (2008). *Advanced Metering Infrastructure: What Regulators Need to Know Its Value to Residential Customers,* National Regulatory Research Institute, Columbus, OH, USA.

Clements, S. and Kirkham, H. (2010). Cyber-security Considerations for Smart Grid. *2010 IEEE Power and Energy Society General Meeting*, pp. 1-5

Computer Security Institute, CSI (2009). *14th Annual Computer Crime and Security Survey Executive Summary*, CSI.

Davis, M. (2009). *Recoverable Advanced Metering Infrastructure.* Black Hat Conference, Las Vegas, OH, USA.

Ericsson, G.N. (2010). Cyber Security and Power System Communication-Essential Parts of a Smart Grid Infrastructure. *IEEE Trans. on Power Delivery*, vol. 25, no. 3, pp. 1501-1507.

Gates, C. and Taylor, C. (2006). Challenging the Anomaly Detection Paradigm: A Provocative Discussion. *Proceedings of the 2006 Workshop on New Security Paradigms*, pp. 21-29.

Luan, W.P., Sharp, D., and Lancashire S. (2010). Smart Grid Communication Network Capacity Planning for Power Utilities. *2010 IEEE PES Transmission and Distribution Conference and Distribution Exposition,* pp. 1-4.

Metke, A.R. and Ekl, R.L. (2010). Smart Grid Technology. *2010 IEEE PES Innovative Smart Grid Technologies Conference Europe,* pp. 1-7.

Morgan Stanley Research (2009). *Clean Energy*, Morgan Stanley Research.

National Institute of Standards and Technology, NIST (2010). *Smart Grid Cyber Security Strategies and Requirements*, NISTIR 7628.

Roesch, M. (1999). Snort-Lightweight Intrusion Detection for Networks. *Proceedings of LISA '99: 13th System Administration Conference*, pp. 229-238.

Ten, C.-W., Liu, C.-C., and Govindarasu M. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Trans. on Power Systems,* vol. 23, no. 4 pp. 1836-1846.

Werlinger, R., Hawkey, K., et al. (2008). The Challenges of Using an Intrusion Detection System: Is It Worth the Effort? *Proceedings of the 4th Symposium on Usable Privacy and Security*, vol. 337, pp. 107-118.

Xu L., Chow M.-Y., and Taylor, L.S. (2007). Power Distribution Fault Cause Identification with Imbalanced Data Using the Data Mining-Based Fuzzy Classification E-Algorithm. *IEEE Trans. on Power Systems,* vol. 22, no. 1, pp. 164-171.

## ACKNOWLEDGEMENT

The authors would like to acknowledge Science Foundation Ireland (SFI) for the support through a Principal Investigator Award. Useful suggestions from the reviewers are greatly appreciated.

## BIOGRAPHIES

**Shinn-Shyan Wu** received his BSEE degree from National Sun Yat-Sen University, Kaohsiung, Taiwan, and MSEE degree from National Cheng-Kung University, Tainan, Taiwan, in 2006 and 2008, respectively. He is currently pursuing his Ph.D. at the University College Dublin, Ireland.

**Chen-Ching Liu (F'94)** received his Ph.D. degree from the University of California, Berkeley. Dr. Liu is currently Professor of Power Systems and Deputy Principal, College of Engineering, Mathematical and Physical Sciences, at the University College Dublin.

**Ahmed F. Shosha** received his B.A. degree from Cairo University, Egypt, and M.Sc degree in Software Engineering from Nile University, Egypt, in 2007 to 2009, respectively. He is pursuing his Ph.D. in School of Computer Science and Informatics at University College Dublin, Ireland.

**Pavel Gladyshev** is a College Lecturer at the UCD School of Computer Science and Informatics, where he is directing the GDip/MSc programme in Forensic Computing and Cybercrime Investigation.