This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2014.2332095, IEEE Journal on Selected Areas in Communications

A Game Theoretical Analysis of Data Confidentiality Attacks on Smart Grid AMI

Ziad Ismail, Jean Leneutre, David Bateman and Lin Chen

***Abstract*—The widespread deployment of smart meters in the Advanced Metering Infrastructure (AMI) raises privacy concerns. Analyzing data collected from smart meters can expose habits and potentially be used to predict consumers' behaviors. In this paper, we analyze the confidentiality of information in the AMI consisting of nodes with interdependent correlated security assets. On each node, the defender can choose one of several security modes available. We try to answer the following questions: What is the expected behavior of a rational attacker? What is the optimal strategy of the defender? Can we configure security modes on each node so as to discourage the attacker from launching any attacks?**

In this paper, we formulate the problem as a non-cooperative game and analyze the behavior of the attacker and the defender at the Nash equilibrium. The attacker chooses his targets in order to collect the maximum amount of data on consumers, and the defender chooses the encryption level of outbound data on each device in the AMI. Using our model, we derive the minimum defense resources required and the optimal strategy of the defender. Finally, we show how our framework can be applied in a real world scenario via a case study.

***Index Terms*—Advanced Metering Infrastructure, Smart Meters, Security, Privacy, Non-Cooperative Game Theory, Nash Equilibrium.**

I. Introduction

According to the last report of the U.S. Energy Information Administration on the international energy outlook, they predict that the world energy consumption will grow by 56 % between 2010 and 2040 [1]. To meet the increasing demand for energy, the power utilities need to produce energy more efficiently, and consumers to manage and control their power consumptions. The Advanced Metering Infrastructure (AMI) is an integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers. In the AMI, smart meters are electronic devices installed at the consumers' premises. These devices send users power consumptions to the utility. The power utility uses this data to (i) bill the user for the power consumed, (ii) enable demand response, (iii) predict power consumptions curves for each area or neighborhood, and (iv) update energy prices in real time.

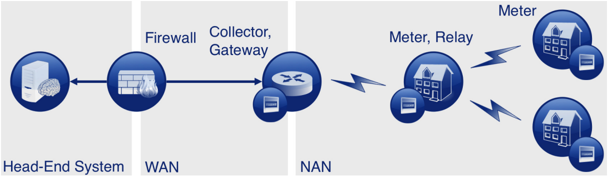

Fig. 1: AMI hierarchy and network components

The AMI is mainly composed of three hierarchical areas (Figure 1). The Neighborhood Area Network (NAN) is a network of meters and collectors in the same geographical area [2]. Each collector in the NAN is responsible of collecting data from a set of smart meters. The WAN network includes gateways and routers that are responsible of connecting the utility Head-End system to devices in NANs. The utility Head-End system analyzes data collected from smart meters. In addition, it communicates with smart meters through collectors to request data or to send control commands.

The security of the smart grid, and in particular the AMI, is an active research topic. Due to the nature of industrial infrastructures, they were long been viewed as isolated, and therefore partially secured from external attacks. In fact, devices in this type of infrastructures used to communicate at the local level, or through dedicated private connections. Most of these devices were not connected to the internet. However, the smart grid is envisioned to provide new services, further relying on the communication infrastructure. This increased number of connections with the telecommunication infrastructure, and in particular with the internet, has the potential to increase the attack surface of the smart grid.

In the context of smart metering, security objectives are different from other smart grid operations where priority is often given to guarantee data availability [3]. Data sent by smart meters is sensitive and need to be protected from attackers. Therefore, a number of smart meters can be configured to operate in different security modes. Each mode protects a set of information sent to the utility. In this paper, we refer to the security mode as the encryption rate of data sent by a device to the power utility. The large number of devices deployed in the AMI renders the management of the overall security a challenging task. Constrained with a strict defense budget, the defender often prioritizes the protection of assets. In addition to protecting assets that are important to the utility, the defender should protect targets that are identified as attractive to attackers. Therefore, the security strategy of the defender should take into account in addition to the value of the assets, the possible actions of attackers. In this paper, we investigate this problem and propose a security game with two players, an attacker and a defender. The attacker's objective is to attack devices in the AMI in order to compromise data sent

Z. Ismail and D. Bateman are with the Department SINETICS (SImulation NEutronique, Technologies de l'Information et Calcul Scientifique), EDF R&D, 1 avenue Général de Gaulle, 92141 Clamart, France. E-mail: ziad.ismail@edf.fr, david.bateman@edf.fr

J. Leneutre is with the Department of Computer Science and Networks, Telecom ParisTech, CNRS LTCI-UMR 5141 laboratory, 46, Rue Barrault, 75013, Paris, France. E-mail: jean.leneutre@telecom-paristech.fr

L. Chen is with the Department of Computer Science and Networks, LRI (Laboratoire de Recherche en Informatique), University of Paris-Sud 11, 15 Rue Georges Clemenceau, 91400 Orsay, France. E-mail: lin.chen@lri.fr

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2014.2332095, IEEE Journal on Selected Areas in Communications

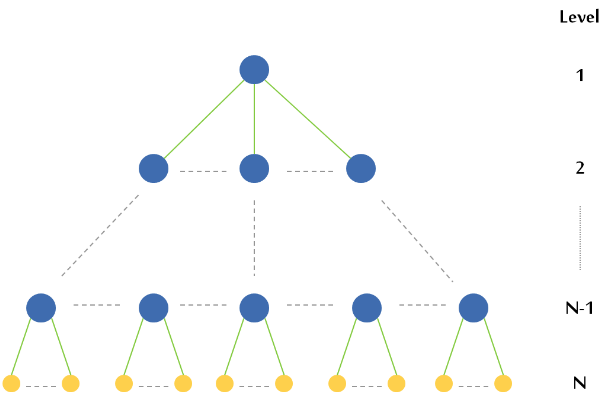

Fig. 2: AMI communication architecture

from these devices to the utility company. On the other hand, the defender has to choose which security mode to enable on each device in order to protect the maximum amount of data from the attacker. Our main contributions are as follows:

- We provide a game theoretical framework of data confidentiality in the AMI where nodes have different security assets.
- We derive the expected behavior of both the attacker and the defender, the optimal defense strategy that discourages the attacker of launching any attack and the minimum defense resources required to deploy that strategy.
- We provide a case study to demonstrate how the game theoretical framework can be implemented to optimize the defense resources in the AMI.

The paper proceeds as follows. We introduce our game model in section II. In section III and IV, we analyze two types of interactions between players and analyze the behavior of both players at the Nash equilibrium. In section V, we show via a case study, how our framework can be applied to configure security modes in the AMI. Section VI discusses related work. Finally, we conclude the paper in section VII.

II. System Model and Game Formulation

A. System Model

We consider a tree like communication architecture $\mathcal{T}$ for the AMI with one root node as in Figure 2. In this architecture, nodes represent equipment in the AMI. Each node collects data from its children, aggregates it, and finally sends it to its parent node. We consider that there exists N aggregation levels. Let $\mathcal{V} = \{1, 2, ..., Y\}$ be the set of nodes in the tree $\mathcal{T}$, where Y is the total number of nodes. Let L_i be the set of nodes that belong to the i^{th} aggregation level. We consider that each node can only belong to one aggregation level. We refer by 1, the root node of $\mathcal{T}$. Smart meters devices are represented by nodes that belong to the N^{th} aggregation level.

Table I lists the main symbols used throughout the paper.

We define the following functions:

$f : \mathcal{V}\backslash\{1\} \rightarrow \mathcal{V}$, function that returns for each node $i \in \mathcal{V}\backslash\{1\}$, its parent node.

$Ch : \mathcal{V} \times [\![1; N]\!] \rightarrow 2^{\mathcal{V}}$ (where $2^{\mathcal{V}}$ denotes the power set of $\mathcal{V}$), function such that for a particular node i and an aggregation level k, $Ch(i, k)$ returns the set containing the children of $i \in L_m$ at level $k > m$. To simplify notations, we will refer by $Ch(i)$ the set containing the children of node i at level $m + 1$.

TABLE I: List of main symbols

$\mathcal{T}$	a tree (a connected graph without cycles)
$\mathcal{L}(\mathcal{T})$	set of leaves of tree $\mathcal{T}$
$\mathcal{V}$	set of nodes in the tree $\mathcal{T}$
$\mathcal{V}_S$	set of sensible target nodes in $\mathcal{T}$
$\mathcal{T}_S$	a subtree of $\mathcal{T}$ consisting of nodes $i \in \mathcal{V}_S$
N	number of aggregation levels in $\mathcal{T}$
Y	total number of nodes in the tree $\mathcal{T}$
$N_S(i)$	maximum aggregation level of the leaves of the subtree $\mathcal{T}_i$ of $\mathcal{T}_S$ that has i as root node
L_i	set of nodes that belong to the i^{th} aggregation level
W_i	security asset of node i
W_i^k	security asset of the parent of node $i \in L_m$ at level $k < m$
∇_i^k	number of children of node $i \in L_m$ at level $k > m$
Δ_i^k	number of children of node $i \in L_m$ at level $k > m$ that belong to the sensible target set $\mathcal{V}_S$
$f(i)$	parent of node i
$Ch(i, k)$	set of the children of node $i \in L_m$ at level $k > m$
$Ch(i)$	set of the children of node $i \in L_m$ at level $m + 1$
$Ch_S(i, k)$	set of the children of node $i \in L_m$ at level $k > m$ that belong to the sensible target set $\mathcal{V}_S$
$Ch_S(i)$	set of the children of node $i \in L_m$ at level $m + 1$ that belong to the sensible target set $\mathcal{V}_S$
$\overline{Ch_S(i, k)}$	$Ch(i, k)\backslash Ch_S(i, k)$
$\mathbb{1}_{expr}$	equals 1 if $expr$ is true, 0 otherwise
p_i	probability of attacking node i
s_i	encryption rate of outbound data on node i
P	total attack resources
S	total encryption resources

Data on each node i has a value or security asset W_i. W_i quantifies the loss in data confidentiality if the attack on node i is successful. We suppose that these values have been quantified as a result of the application of a security risk assessment method (e.g. [4]). The parent node i collects data from all its children $Ch(i)$. A node could be responsible of processing and analyzing a set of the data collected from its children. The result of this analysis is then sent with the aggregated data from children nodes to the parent node. Therefore, we consider that $W_i \geq \sum_{j \in Ch(i)} W_j$. The value of data on node i is the sum of the value of data generated by the node in addition to the value of data collected from its children.

For presentation reasons, we first consider that the tree $\mathcal{T}$ has N aggregation levels such that $\forall j \in L_{N-1}$, $Ch(j) \cap L_N \neq \emptyset$. However, we will show throughout the paper that our framework can be applied to any types of trees.

Finally, let $\mathcal{L}(\mathcal{T})$ be the set of leaves of the tree $\mathcal{T}$. We refer by ∇_i^k, the number of children of node $i \in L_m$ at level $k > m$, and W_i^r the security asset of the parent of node $i \in L_m$ at level $r < m$. As notations, let $\nabla_i^k = 1$ and $W_i^k = W_i \; \forall i \in L_k$.

B. Game Formulation

We consider a game with two players, an attacker and a defender. On each node, the defender can choose one of a set of security modes available on that node. In our case, we consider that the defender chooses an encryption level of outbound data on each node. For example, if 100 packets

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2014.2332095, IEEE Journal on Selected Areas in Communications

are sent from the node, the defender chooses how many packets need to be encrypted. We consider that data on each communication link is encrypted with different encryption keys or using different encryption algorithms. At the root node, data is encrypted for storage after being analyzed.

The objective of the attacker is to intercept data by attacking the nodes without being detected. If the attacker wants to intercept data sent by node i, he can either attack node i or attack the parent node of i. We consider that encryption keys are stored in a cryptoprocessor that cannot be accessed by the attacker. The inbound data arrive at a device and is decrypted using the appropriate cryptographic key, processed and then encrypted using a different key. The attacker has no access or control on the decryption and encryption processes. We consider that on each node, an Intrusion Detection System (IDS) is installed with a detection rate of a. The IDS can be a combination of hardware and software detection capabilities. Let p_i be the probability of attacking node i. The attacker's strategy is subject to a budget constraint $\sum_i p_i \leq P \leq 1$ ($0 \leq p_i \leq 1\ \forall i$). We consider that the attacker can attack only one particular device at any given time. Let s_i be the encryption rate of the packets at node i. The defender's strategy is subject to a budget constraint $\sum_i s_i \leq S \leq Y$ ($0 \leq s_i \leq 1\ \forall i$). In general, defense mechanisms deployed to protect a device depend on the value of data generated, stored, or processed by that device. The efficiency, robustness and therefore the cost of the countermeasures deployed by administrators to protect devices are often proportional to the value of the assets on these devices. The attacker's effort to compromise data on a device increases with defense measures deployed to protect that device which depend on the value of its assets. Therefore, we consider that the cost of attacking and encrypting data on node i are proportional to the value of the data W_i and are given by C_aW_i and C_eW_i respectively, where $0 \leq C_a, C_e \leq 1$.

To intercept data sent by node i, the attacker can choose either to attack node i or its parent node $f(i)$. Therefore, the probability of compromising unencrypted data sent by i with an encryption level of s_i for W_i without being detected is given by $W_i(p_i + p_{f(i)})(1-a)(1-s_i)$. We assume that $1-a > C_a$. Otherwise, the attacker has no incentive to attack since the cost to attack is greater than the payoff when the attack is successful and undetected.

The utility functions U_A and U_D of the attacker and the defender respectively are as follows:

$$\begin{aligned} U_A(p,s) &= \sum_{i\in\mathcal{V}} (W_i(p_i + p_{f(i)})(1-a)(1-s_i) - p_iC_aW_i) \\ &= \sum_{i\in\mathcal{V}} (W_ip_i(1-a)(1-s_i) - p_iC_aW_i) \\ &\quad + \sum_{\substack{i\in\mathcal{V}\\ i\notin L_N}} \sum_{j\in Ch(i)} p_iW_j(1-a)(1-s_j) \\ U_D(p,s) &= -\sum_{i\in\mathcal{V}} (W_ip_i(1-a)(1-s_i) + s_iC_eW_i) \\ &\quad - \sum_{\substack{i\in\mathcal{V}\\ i\notin L_N}} \sum_{j\in Ch(i)} p_iW_j(1-a)(1-s_j) \end{aligned}$$

III. Solving the Game

We study the interactions between the attacker and the defender as a non-cooperative game. The attacker and the defender have complete knowledge of the architecture of the system. In the context of non-cooperative games, we are interested in the concept of Nash equilibrium, in which none of the players has an incentive to deviate unilaterally [5]. The Nash equilibrium is considered as the most profitable strategy profile that gives each player the maximum utility given the actions of other players. Let $p = (p_1, ..., p_Y) \in \mathscr{P}$ and $s = (s_1, ..., s_Y) \in \mathscr{S}$ be the strategy profiles of the attacker and the defender respectively, where $\mathscr{P}$ and $\mathscr{S}$ refer to the strategy spaces of each player. We define the Nash equilibrium of our game as follows:

Definition 1. *A* ***Nash equilibrium*** *is a strategy profile (****p*,s****) in which each player cannot improve his utility by altering his decision unilaterally.*

More precisely, we have:

$$\begin{aligned} &U_A(p^*,s^*) \geq U_A(p,s^*)\ for\ all\ p \in \mathscr{P} \\ and\quad &U_D(p^*,s^*) \geq U_D(p^*,s)\ for\ all\ s \in \mathscr{S} \end{aligned}$$

A. Sensible Target Set

In section II, we considered that the attacker and the defender have limited attack and defense resources respectively. With a strict budget, it is rational to assume that both players will try to intelligently distribute their resources to maximize their utilities. Therefore, we can predict that the attacker will try to identify targets that yield the maximum profit, and then allocate resources to compromise data on these devices. On the other hand, the objective of the defender is then to identify the targets that are most likely to be attacked, and protect the confidentiality of data by increasing data encryption rates on these devices.

Let $\mathcal{R}$ be a subset of the set of nodes $\mathcal{V}$. We refer by $\mathcal{M}(\mathcal{R})$, the set of nodes $i \in \mathcal{R}$ such that there are no node $j \in L_k \cap \mathcal{R}$ with $j \in Ch(i,k)$. For each node $i \in \mathcal{R}$, let $N_S(i)$ be the highest aggregation level of any node $j \in \mathcal{R}$ that is a child of i. Therefore, $N_S(i) = \max_k \{j \in L_k \cap \mathcal{M}(\mathcal{R}) \cap Ch(i,k)\}$. In the case where nodes in the set $\mathcal{R}$ form a tree $\mathcal{T}_R$, we have $\mathcal{M}(\mathcal{R}) = \mathcal{L}(\mathcal{T}_R)$.

We define the sensible target set $\mathcal{V}_S$ as a subset of $\mathcal{V}$ as follows:

Definition 2. *The* ***sensible target set*** *$\mathcal{V}_S$ is a subset of $\mathcal{V}$ consisting of $Y_A = |\mathcal{V}_S|$ nodes and defined such that for every node $i \in \mathcal{V}_S$, we have:*

$$\begin{cases} W_i > & \frac{1}{\alpha(1-\frac{C_a}{1-a})}(Y_A(1-\frac{C_a}{1-a}) + \beta - S)\ if\ N_S(i) = N \\ W_i > & \frac{1}{\alpha(1-\frac{C_a}{1-a})}(Y_A(1-\frac{C_a}{1-a}) + \beta - S \\ & \qquad -\alpha \sum\limits_{\substack{k\in Ch(j)\\ j\in Ch_S(i,N_S(i))}} W_k) \qquad if\ N_S(i) \neq N \end{cases}$$

$$where\ \alpha = \sum_{i\in\mathcal{V}_S} \frac{1}{W_i} + \sum_{r=1}^{N-1} \sum_{i\in L_r \cap (\mathcal{V}_S \setminus \mathcal{M}(\mathcal{V}_S))} \frac{\sum\limits_{j=r+1}^{N_S(i)} (-1)^{j-r} \Delta_i^j}{W_i}$$

$$\begin{aligned}\beta \quad &= -\frac{C_a}{1-a}\sum_{r=1}^{N-1}\sum_{i\in L_r\cap(\mathcal{V}_S\backslash\mathcal{M}(\mathcal{V}_S))}\sum_{j=r+1}^{N_S(i)}\sum_{m\in Ch_S(i,j)}\frac{(-1)^{j-r}W_m}{W_i}\\ &-\sum_{r=1}^{N-1}\sum_{i\in L_r\cap(\mathcal{V}_S\backslash\mathcal{M}(\mathcal{V}_S))}\sum_{j=r+1}^{N_S(i)}\sum_{\substack{m\in\overline{Ch_S(i,j)}\\ f(m)\in\mathcal{V}_S\backslash\mathcal{M}(\mathcal{V}_S)}}\frac{(-1)^{j-r}W_m}{W_i}\\ &+\sum_{r=1}^{N-1}\sum_{i\in L_r\cap\mathcal{M}(\mathcal{V}_S)}\sum_{j\in Ch(i)}W_j\sum_{l=1}^{r}\frac{(-1)^{r-l}}{W_i^l}\end{aligned}$$

From Definition 2, it follows that if a node $i \in \mathcal{V}_S$, $f(i) \in \mathcal{V}_S$ since $W_{f(i)} \geq \sum_{j\in Ch(f(i))} W_j \geq W_i$. For the rest of the paper, we refer by $\mathcal{T}_S$, the tree with root node 1 formed by nodes in $\mathcal{V}_S$. Therefore, we have $\mathcal{M}(\mathcal{V}_S) = \mathcal{L}(\mathcal{T}_S)$. Let $Ch_S(i,j)$ refers to the set of the children of node i at level j that belong to $\mathcal{V}_S$. The intuition behind the sensible target set is to have a set of targets whose security assets' compromise yields the maximum payoff for the attacker. In our context, the security asset refers to the confidentiality of data processed by nodes. Analyzing certain types of information such as customers' data or power billing information can have severe impacts on both the customers and the utility company. The analysis can provide the attacker with necessary information to predict a customer's behavior and habits, or even impact the utility's corporate image by exposing customer's credentials and power consumptions.

Algorithm 1: FindSensibleTargetSet

```
Data: Tree $\mathcal{T}$ and the set of nodes $\mathcal{V}$.
Result: The sensible target set $\mathcal{V}_S$
begin
    for $x \in \mathcal{V}$ do
        if $x \in \mathcal{V}\backslash\mathcal{L}(\mathcal{T})$ then
            $W_{t_i} \leftarrow W_i + \frac{1}{(1-\frac{C_a}{1-a})}\sum_{j\in Ch(i)} W_j$
        else
            $W_{t_i} \leftarrow W_i$
        end
    end
    $W_i' \leftarrow$ SortInDescendingOrder($W_{t_{\sigma(i)}}$)
    initialization: $Y_A = Y$, $\alpha$, $\beta$
    while $(Y_A \geq 1)$ &
    $(W_{Y_A}' \leq \frac{1}{\alpha(1-\frac{C_a}{1-a})}(Y_A(1-\frac{C_a}{1-a})+\beta-S))$ do
        $Y_A \leftarrow Y_A - 1$
        update($\alpha$)
        update($\beta$)
    end
    $\mathcal{V}_S = \{\sigma(i) \in \mathcal{V},\ s.t.\ i \in [\![1;Y_A]\!]\}$
end
```

The sensible target set $\mathcal{V}_S$ is determined using Algorithm 1. We start by considering all elements in the set $\mathcal{V}$ and computing for each node i, a new value W_{t_i} depending on the position of node i in the tree $\mathcal{T}$. Then, we sort these new values in descending order. In the new sorted set, we have $W_1' \geq W_2' \geq ... \geq W_Y'$. We start with the lowest value of W' and proceed by removing any node that does not belong to the sensible target set. We note that from Definition 2, the parent of any node that belongs to the sensible target set $\mathcal{V}_S$ is also a member of $\mathcal{V}_S$.

Lemma 1. *α is a positive real number.*

Proof. For presentation reasons, we will prove that $\alpha > 0$ in the special case where $\mathcal{V}_S = \mathcal{V}$. The general case can be proved in a similar way. We prove the result by dividing α into disjoint sets and analyzing each set individually. Refer to Appendix A for full proof. □

Lemma 2. *Data on all nodes will be encrypted with non-zero encryption rates if the defender has at least S_{min} encryption resources, where S_{min} is given by:*

$$S_{min} = Y(1-\tfrac{C_a}{1-a})+\beta$$

Proof. Follows directly from Definition 2. □

For the rest of the paper, we consider that encryption resources are limited s.t. $S \leq S_{min}$.

Theorem 1. *A rational attacker attacks only nodes in the sensible target set $\mathcal{V}_S$.*

Proof. We consider the vector $s^0 = (s_1^0, ..., s_Y^0)$ where:

$$s_i^0\begin{cases} = 1-\frac{C_a}{1-a}-\frac{1}{\alpha W_i}(Y_A(1- \quad \frac{C_a}{1-a})+\beta-S) & \\ \quad +\frac{\mathbb{1}_{(N_S(i)\neq N)}}{W_i}\sum_{j\in Ch(i)} W_j & \forall i\in\mathcal{L}(\mathcal{T}_S)\\ = 1-\frac{C_a}{1-a}-\frac{A_i}{(1-a)W_i} & \forall i\in L_k\cap(\mathcal{V}_S\backslash\mathcal{L}(\mathcal{T}_S))\\ = 0 & \forall i\in\mathcal{V}\backslash\mathcal{V}_S\end{cases}$$

where A_i is given in Appendix B.

First, we use Lemma 1 and Lemma 2 to prove that the choice of s^0 is valid s.t. $s_i^0 \geq 0\ \forall i$.

We have $\sum_{i\in\mathcal{V}_S} s_i^0 = S$. Let $s = (s_1, ..., s_Y)$ be the strategy of the defender. By the pigeonhole principle, $\sum_{i\in\mathcal{V}_S} s_i \leq S$, thus $\exists m \in \mathcal{V}_S$ s.t. $s_m \leq s_m^0$.

We consider the attacker strategy satisfying $\sum_{i\in\mathcal{V}\backslash\mathcal{V}_S} p_i > 0$. We construct the attacker strategy profile $p^{'}$ s.t.:

$$p_i^{'} = \begin{cases} p_i & i\in\mathcal{V}_S \text{ and } i\neq m\\ p_m+\sum_{j\in\mathcal{V}\backslash\mathcal{V}_S} p_j & i=m\\ 0 & i\in\mathcal{V}\backslash\mathcal{V}_S\end{cases}$$

We prove that, $U_A(p,s) - U_A(p',s) < 0$. The payoff of the attacker is greater when operating on $p^{'}$ instead of p. The attacker attacks only nodes in $\mathcal{V}_S$.

Refer to Appendix A for full proof. □

While proving that the choice of s^0 is valid in Theorem 1, we proved that if data on a node j is encrypted with a certain rate, all data handled by each one of its parent nodes will be encrypted with non-zero encryption rates. As a result, we cannot expect all data to be sent in clear between nodes if one of the children of these nodes has encrypted a set of its data.

The sensible target set $\mathcal{V}_S$ is a set of nodes whose security assets are the most attractive to the attacker. To maximize his payoff, the attacker only needs to compromise data processed by these nodes. Any node that does not belong to the sensible target set is not attractive enough for the attacker, and therefore will not be attacked. In this case, from the point of view of the defender, data processed by these nodes do not need to be encrypted. An important security implication of this result is that the defender only needs to secure data processed by nodes in the sensible target set $\mathcal{V}_S$.

B. Nash Equilibrium Analysis

In this section, we investigate the case where both the attacker and the defender take the decisions at the same time while taking into account each other's strategies. This type of interactions falls under the one-shot game category [5]. Let p^* and s^* denote the attacker and the defender strategies at the Nash equilibrium respectively. Therefore, we have:

$$U_A(p^*,s^*) > U_A(p,s^*)\ \forall p \in \mathscr{P}\ s.t.\ \sum_i p_i \leq P$$
$$U_D(p^*,s^*) > U_A(p^*,s)\ \forall s \in \mathscr{S}\ s.t.\ \sum_i s_i \leq S$$

Theorem 2. *Under the assumption that $\sum_i p_i = P$ and $\sum_i s_i = S$, a Nash equilibrium exists and is given by:*

$$\begin{cases} s_i = 1 - \frac{C_a}{1-a} - \frac{1}{\alpha W_i}(Y_A(1-\frac{C_a}{1-a}) + \quad \beta - S) \\ \qquad + \frac{\mathbb{1}_{(N_S(i)\neq N)}}{W_i} \sum\limits_{j \in Ch(i)} W_j \quad \forall i \in \mathcal{L}(\mathcal{T}_S) \\ s_i = 1 - \frac{C_a}{1-a} - \frac{A_i}{(1-a)W_i} \qquad \forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)) \end{cases}$$

$$\begin{cases} p_1^* = \frac{1}{\gamma}(P - \frac{C_e}{1-a} \sum\limits_{r=2}^{N} \sum\limits_{i \in L_r \cap \mathcal{V}_S} \frac{(1+(-1)^r)}{2} \\ \qquad - \frac{W_1 C_e}{1-a} \sum\limits_{r=2}^{N} \sum\limits_{i \in L_r \cap \mathcal{V}_S} (-\frac{1}{W_i} + \mathbb{1}_{(r>2)} \sum\limits_{j=2}^{r-1} \frac{(-1)^{r-j+1}}{W_i^j})) \\ p_i^* = \frac{C_e}{1-a}(\frac{1+(-1)^k}{2}) + p_1^* W_1 (\frac{1}{W_i} + \sum\limits_{j=1}^{k-1} \frac{(-1)^{k-j}}{W_i^j}) \\ \qquad + \frac{W_1 C_e}{1-a}(-\frac{1}{W_i} + \mathbb{1}_{(k>2)} \sum\limits_{j=2}^{k-1} \frac{(-1)^{k-j+1}}{W_i^j}) \\ \qquad\qquad \forall i \in L_k \cap \mathcal{V}_S, k \geq 2 \end{cases}$$

where A_i and γ are given in Appendix B.

and $\mathbb{1}_{expr} = \begin{cases} 1 & if\ expr\ is\ true \\ 0 & otherwise \end{cases}$

Proof. The attacker needs to solve the following optimization problem:

$$\max_p U_A(p,s)\ s.t. \sum_i p_i = P$$

The Lagrangian of this optimization problem is given by: $\mathcal{L}_1(p,s,\lambda) = U_A(p,s) + \lambda(P - \sum_i p_i)$ s.t $\lambda > 0$

We prove that $\forall i \in \mathcal{L}(\mathcal{T}_S)$,
$W_i(1-a)(1-s_i) - C_a W_i + \mathbb{1}_{(N_S(i)\neq N)} \sum\limits_{j \in Ch(i)} (1-a)W_j = \lambda$

And we prove that $\forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S))$:

$$\begin{aligned} & W_i(1-a)(1-s_i) - C_a W_i \\ & = - \sum_{j=k+1}^{N_S(i)} \sum_{\substack{m \in L_j \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(i,j)}} \mathbb{1}_{(j\neq N)} (-1)^{j-k} \sum_{t \in Ch(m)} (1-a)W_t \\ & \quad + (1-a) \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \sum_{\substack{\underline{m \in Ch_S(i,j)} \\ f(m) \in \mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)}} W_m \\ & \quad + C_a \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \sum_{m \in Ch_S(i,j)} W_m \\ & \quad + \lambda(1 + \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \Delta_i^j) \end{aligned}$$

$$\Rightarrow \begin{cases} s_i = 1 - \frac{C_a}{1-a} - \frac{\lambda}{(1-a)W_i} \\ \qquad + \frac{\mathbb{1}_{(N_S(i)\neq N)}}{W_i} \sum\limits_{j \in Ch(i)} W_j \quad \forall i \in \mathcal{L}(\mathcal{T}_S) \\ s_i = 1 - \frac{C_a}{1-a} - \frac{A_i}{(1-a)W_i} \qquad \forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)) \end{cases}$$

We have $\sum_i s_i = S$.

Therefore, we find that $\lambda = \frac{(1-a)}{\alpha}(Y_A(1-\frac{C_a}{1-a}) + \beta - S)$. By substituting λ in the equations of s_i, we find the results in Theorem 2.

Similarly, we find the attacker's strategy at equilibrium by solving the defender's optimization problem, $\max\limits_s U_D(p,s)\ s.t. \sum_i s_i = S$.

Refer to Appendix A for full proof. □

At the Nash equilibrium (NE), the attacker and the defender have no incentive to deviate from their strategies unilaterally. The NE consists of the optimal acceptable strategies for both players. In the worst case where the attacker has sufficient attack resources, the defender's NE strategy is his best response to the attacker's strategy. As we proved earlier, once the defender chooses to encrypt a set of data on a certain node, he needs to guarantee that the data transiting from this node to the root node is not sent in clear (without encryption). Therefore, the defender's strategy to encrypt data on node i does not only depend on the security asset W_i and the attacker's strategy, but on the number and security assets of nodes along the path from node i to the root node.

IV. Stackelberg Game

In most cases, the attacker chooses his attack strategy based on the deployed security measures in the system. In this section, we analyze the interactions between players as a Stackelberg game [5]. In this type of games, a leader chooses his strategy first. Afterwards, the follower, notified by the leader's choice, chooses his strategy. The leader tries to anticipate the follower's response and chooses the strategy that yields the maximum payoff knowing what will be the reaction of the follower. In our case, the defender is the leader who tries to configure encryption rates on each device in order to protect the confidentiality of the maximum amount of data transiting in the AMI.

Stackelberg games are generally solved by backward induction. The solution is known as Stackelberg Equilibrium (SE) or Stackelberg-Nash Equilibrium (SNE). We start by computing the best response strategy of the follower as a function of the leaders strategy. Then, according to the follower's best response, we derive the optimal strategy of the leader.

The attacker solves the following optimization problem:

$$p(s) = \underset{p \in [0;1]^Y}{\text{argmax}}\, U_A(p,s)$$

On the other hand, the defender solves the following optimization problem:

$$s(p) = \underset{s \in [0;1]^Y}{\text{argmax}}\, U_D(p(s),s)$$

Theorem 3. *The game admits a Stackelberg Nash equilibrium (p^S, s^S) given by:*

$$\begin{cases} p_i^S = 0 & \forall i \in \mathcal{V} \\ s_i^S = 1 - \frac{C_a}{1-a} & \forall i \in L_N \\ s_i^S = 1 - \frac{C_a}{1-a} & \\ \quad - \frac{C_a \sum\limits_{j=k+1}^{N} (-1)^{j-k} \sum\limits_{m \in Ch(i,j)} W_m}{W_i(1-a)} & \forall i \in L_k, k \leq N-1 \end{cases}$$

Proof. Solving the system by backward induction, we get the best response of the follower given by:

$$p_i \begin{cases} = 1 & if \ (1-a)(1-s_i) - C_a > 0 \\ \in [0;1] & if \ (1-a)(1-s_i) - C_a = 0 \\ = 0 & if \ (1-a)(1-s_i) - C_a < 0 \end{cases} \quad \forall i \in L_N$$

and $\forall i \in L_k, k \leq N-1$,

$$p_i \begin{cases} = 1 & if \sum\limits_{j \in Ch(i)} W_j(1-a)(1-s_j) \\ & \quad + W_i(1-a)(1-s_i) - C_a W_i > 0 \\ \in [0;1] & if \sum\limits_{j \in Ch(i)} W_j(1-a)(1-s_j) \\ & \quad + W_i(1-a)(1-s_i) - C_a W_i = 0 \\ = 0 & if \sum\limits_{j \in Ch(i)} W_j(1-a)(1-s_j) \\ & \quad + W_i(1-a)(1-s_i) - C_a W_i < 0 \end{cases}$$

The payoff of the defender is given by:

$$U_D(p,s) = -\sum_i (p_i W_i(1-a)(1-s_i) + s_i C_e W_i) - \sum_{i \notin L_N} \sum_{j \in Ch(i)} p_i W_j (1-a)(1-s_j)$$

We find the results in Theorem 3 by noticing that the defender's payoff is a decreasing function with respect to the attaker's strategy p. Therefore, the defender will choose his strategy in order to push the attacker to set his strategy p to 0. Therefore, $\forall i \in L_N$,

$$(1-a)(1-s_i) - C_a = 0 \Rightarrow s_i = 1 - \frac{C_a}{1-a}$$

and $\forall i \in L_k, k \leq N-1$, we prove that:

$$W_i(1-a)(1-s_i) = C_a W_i + C_a \sum_{j=k+1}^{N} (-1)^{j-k} \sum_{m \in Ch(i,j)} W_m$$

Therefore, we find the results in Theorem 3.

□

Operating exactly at s^S, the defender is not certain that the attacker will operate at $p^S = 0$. Therefore, in order to push the attacker to choose $p^S = 0$, the defender will operate at a strategy $s_i^{S'}$ slightly higher that s_i^S. In this case, when the defender operates at $s^{S'}$, the attacker will be better off not attacking at all. Otherwise, the attacker will get a negative payoff. The defender strategy $s^{S'}$ is given by:

$$\begin{cases} s_i^{S'} = 1 + \epsilon - \frac{C_a}{1-a} & \forall i \in L_N \\ s_i^{S'} = 1 + \epsilon - \frac{C_a}{1-a} & \\ \quad - \frac{C_a \sum\limits_{j=k+1}^{N} (-1)^{j-k} \sum\limits_{m \in Ch(i,j)} W_m}{W_i(1-a)} & \forall i \in L_k, k \leq N-1 \end{cases}$$

where ϵ is a small positive number.

The defender needs additional encryption resources to maintain the Stackelberg equilibrium. However, the gain of adding the additional encryption resources on each node is greater than the possible cost of operating exactly at s^S. Otherwise, the attacker can significantly decrease the payoff of the defender by launching attacks. At the SE, the choice of the encryption rates discourages the attacker of launching any attacks against any node in the system.

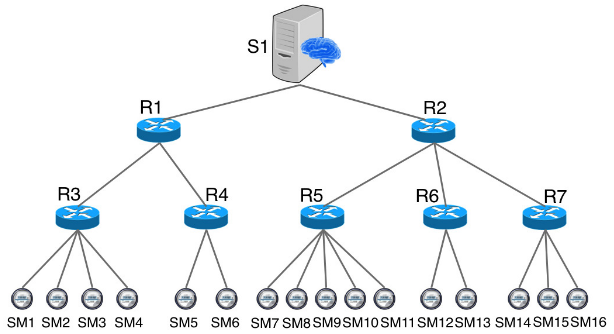

Fig. 3: Example of an AMI architecture

Theorem 4. *The defender needs at least* $Y(1 - \frac{C_a}{1-a}) - \frac{C_a}{1-a} \sum_{i \in L_k} W_i \sum_{j=1}^{k-1} \frac{(-1)^{k-j}}{W_i^j}$ *encryption resources to discourage the attacker of launching any attacks.*

Proof. Follows directly from Theorem 3. □

Theorem 4 shows that with sufficient defense resources, the defender is capable of preventing any attack. In fact, from the point of view of the attacker, the cost of attacking in this case outweighs the payoff of potential attacks.

V. Case Study

In this section, we apply our game theoretical framework on an AMI topology as shown in Figure 3. In this case study, the number of aggregation levels as defined in our model is 4. Smart meters send consumers' data to the head-end system S_1 to be analyzed. Along the path, data from several smart meters are aggregated at two intermediate levels. On each communication link, different encryption keys or algorithms are used to encrypt outbound data. We consider that on each device in the AMI, we have an IDS with a detection rate a of 0.6. The cost weights C_a and C_e of attacking and encrypting data on a node i are set to 0.2 and 0.05 respectively. The attacker disposes an attack budget P of 1, and the defender a total budget to encrypt data S of 8. We analyze the behavior of the attacker and the defender in the cases of one-shot and Stackelberg games. Results are depicted in Table II.

1) One-Shot game: In this type of games, both players choose their strategies at the same time. Nodes with security assets that are not attractive to the attacker are "self-protected". The defender does not need to encrypt data on these nodes (SM1, SM2, etc.) since they will not be attacked.

We notice that most of the time, the defender's deployed defense resources on a node is an increasing function with respect to the security asset of that node. In addition to the value of the security asset, the topology of the network affects the strategy of the defender. For example, the security asset of router R2 is double than R1. However, the defender does not allocate twice as much resources to encrypt data on R2. At the smart meters level, we notice that the defender chooses the same data encryption rates on nodes with the same values for their security assets. However, in addition to security assets values, the attacker takes into account interconnections between devices and whether smart meters share the same parent node at level $N-1$ (3^{rd} level). For example, SM11

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2014.2332095, IEEE Journal on Selected Areas in Communications

and SM14 have the same security asset value of 3 but do not share the same parent node at the 3^{rd} level. We notice that the attacker does not deploy the same amount of attack resources on SM11 and SM14 even though data encryption rates chosen by the defender at the NE are the same. Finally, both players do not evaluate nodes that belong to different aggregation levels but with the same security assets values in the same way. For example, R4 and SM9 have the same security asset value of 4, however both players treat each node differently.

2) Stackelberg game: In the Stackelberg game, we have a leader and a follower. First, the leader chooses his strategy. Then, the follower, informed by the leader's choice, chooses his strategy accordingly. In our case, the defender is the leader who tries to anticipate attacker's actions and configure encryption rates on each device to reduce the amount of data that can be accessed by the attacker. In addition to the security asset, the cost of attacking and the network topology play an important role in the choice of encryption rates in this case. For example, interestingly, encryption rates for data sent from nodes in the 3^{rd} aggregation level to R1 and R2 are higher than encryption rates for data sent from R1 and R2 to S1. Moreover, encryption rates are not proportional with respect to the security assets of the nodes ($s_{R2} \neq 2 \times s_{R1}$). Smart meters are treated in the same way regardless of their security assets. However, this choice of encryption rates is sufficient to discourage the attacker of launching any attacks. Finally, we note that in order to maintain this Stackelberg equilibrium, the defender needs at least a budget of 14.297.

TABLE II: Nash Equilibrium

	$\mathbf{W_i}$	**One-Shot game**		**Stackelberg game**	
		p^*	s^*	p^S	s^S
S1	65	0.1267	0.9316	0	0.7731
R1	20	0.0039	0.4618	0	0.6625
R2	40	0.0011	0.5361	0	0.725
R3	14	0.1291	0.9643	0	0.8214
R4	6	0.1398	1	0	0.875
R5	29	0.1278	0.9583	0	0.8103
R6	4	0.1519	0.809	0	0.8125
R7	15	0.1314	0.9509	0	0.8167
SM1	1	0	0	0	0.5
SM2	2	0	0	0	0.5
SM3	1	0	0	0	0.5
SM4	5	0.0183	0.2472	0	0.5
SM5	3	0.0225	0.0787	0	0.5
SM6	1.5	0	0	0	0.5
SM7	1	0	0	0	0.5
SM8	4	0.0251	0.184	0	0.5
SM9	6	0.0159	0.2894	0	0.5
SM10	4	0.0251	0.184	0	0.5
SM11	3	0.0345	0.0787	0	0.5
SM12	1	0	0	0	0.5
SM13	1.5	0	0	0	0.5
SM14	3	0.0309	0.0787	0	0.5
SM15	5	0.016	0.2472	0	0.5
SM16	1.5	0	0	0	0.5

VI. Related Work

In general, a large number of devices in the smart grid have constrained computational resources. Therefore, cryptographic mechanisms and security protocols need to be adapted to this constrained environment [6]. In addition, security resources should be intelligently allocated to best protect both the utility and consumers' data. The security solution should protect consumers' data along the communication path to the utility company [7]. A possible solution based on homomorphic encryption is proposed by Li et al. [8]. The authors propose a distributed incremental smart meter data aggregation approach using homomorphic encryption. This type of encryption allows certain algebraic operations on the plaintext to be performed directly on the cyphertext without the need to decrypt the data. In this system, each node is responsible of aggregating its own data with the data collected from its children. Therefore, user data is protected and intermediate results remain secure. However, to gurantee that consumer's data is not manipulated, the authors' solution assumes that intermediate nodes are not compromised.

Data stored on smart meters and sent to utility companies is sensitive and need to be protected. By compromising this data, attackers could leverage information that could be used to threaten a customer's physical security. In addition, monitoring the behavior of customers through insecure AMI communications could help attackers commit crimes, or perform robberies. In fact, the behavior of consumers could be predicted using Nonintrusive load monitoring (NILM) technology [9]. NILM can determine the operating schedule of electrical loads from measurements stored in a centralized location. To protect the privacy of consumers' energy consumption metering data, approaches based on aggregating power consumptions of multiple consumers [10] or smart metering data anonymization [11] were proposed. Another approach, the Load Signature Moderation (LSM) technique [12], changes appliances load signatures which makes it harder to distinguish the timing and the nature of appliances being used. In addition, multiple protocols were proposed to protect the confidentiality of consumers' data. Rial et al. [13] propose a privacy-preserving protocol that allows consumers to perform calculations on meter readings without disclosing any consumption data. Rottondi et al. [14] propose an infrastructure and a communication protocol to protect consumers' smart meters data. Special nodes, referred to as Privacy Preserving Nodes (PPN), are responsible of collecting consumer's data. The authors assume the integrity of PPNs. However, these nodes can be attractive targets to attackers for their potential value and importance in the system. Therefore, assuming the integrity of PPNs cannot be totally guaranteed.

In the security domain, the defenders often deploy defense countermeasures based on the value of the assets they try to protect and potential threats from attackers. Often with a strict defense budget, defenders should intelligently allocate defense resources while taking into account the possible actions of attackers. To analyze this type of interactions between attackers and defenders, and eventually find the optimal defense strategy, game theory has been used [15]. Game theory studies interactions between different players with the same or conflicting interests. This theory has also been used to analyze problems in the smart grid [16] that include microgrids, demand-side management and communications.

In our model, we rely on an intrusion detection system installed on each device to detect attacks. Designing intrusion

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2014.2332095, IEEE Journal on Selected Areas in Communications

detection systems for the AMI is an active research field. One of the promising IDS solutions is proposed by Berthier el al. [17]. The authors' solution is a specification-based intrusion detection system for AMIs. In a specification-based intrusion detection system, any sequence of operations executed outside the systems specifications is considered to be a security violation. Therefore, this type of IDSs is capable of detecting unknown attacks.

A security solution for the AMI should take into account potential threats from adversaries. Attackers can take advantage of vulnerable points in the system to disrupt the service or compromise system equipment. Defenders often deploy security solutions with a limited defense budget. Our work contributes to the existing literature by providing a game model to protect the confidentiality of consumers' data in the AMI. We derived the minimum encryption resources required to thwart attacks in the AMI. Finally, we illustrated how our model can be used to configure data encryption rates in real scenarios via a case study.

VII. Conclusion

In this paper, we analyzed data confidentiality attacks on smart grid Advanced Metering Infrastructure (AMI) network components. We modeled the interaction between an attacker and a defender as a non-cooperative game. The objective of the attacker is to collect the maximum amount of data about consumers by attacking devices in the AMI, whereas the defender tries to protect data from attacker's eavesdropping by encrypting it using different encryption keys or encryption algorithms for each network link. We were able to derive the expected behavior of the attacker and the defender for two types of interactions between the players. Based on our analysis, we identified the set of devices which when compromised will be the most profitable for the attacker. In a leader and follower game where the defender anticipates attacker's actions, we derived the minimum defense budget required and the optimal encryption rates on each device in the AMI in order to thwart attacks. Finally, we showed via a case study how to apply our game framework to configure encryption rates on network devices in the AMI.

As future work, we plan to investigate the impact of false alarm rates for the detection of attacks on players' behaviors. Another research direction will be to extend the model to include additional players' actions. For example, the defender can choose between different possible encryption algorithms on each device where each algorithm is characterized by its robustness and cost, or the possibility to reconfigure network connections when the system is under attack.

Appendix A

Proof of Lemma 1*:*

We assumed that $W_i \geq \sum_{j \in Ch(i)} W_j$. Therefore, $W_i \geq W_j \; \forall j \in Ch(i)$.

We start by dividing α into three disjoint parts.

Let $\alpha = \sum_i \frac{1}{W_i} + \sum_{r=1}^{N-1} \sum_{i \in L_r} \frac{\sum_{j=r+1}^{N} (-1)^{j-r} \nabla_i^j}{W_i}$ = I + II + III

I: $\sum_{i \in L_N} \frac{1}{W_i} + \sum_{j \in L_{N-1}} \frac{-\nabla_j^N}{W_j}$

We have, $Wi \geq W_j, \; \forall j \in Ch(i)$

$$\Rightarrow \frac{1}{W_i} \leq \frac{1}{W_j}$$

$$\Rightarrow \frac{Ch(i)}{W_i} \leq \sum_{j \in Ch(i)} \frac{1}{W_j}$$

$$\Rightarrow \text{I} \geq 0$$

II:

$$\sum_{p=1}^{\lfloor \frac{N}{2} - 1 \rfloor} \Bigg\{ \sum_{i \in L_{N-2p+1}} \frac{1}{W_i} + \sum_{i \in L_{N-2p}} \frac{1}{W_i} + \sum_{m \in L_{N-2p}} \frac{1}{W_m} \sum_{j=N-2p+1}^{N} (-1)^{j-N+2p} \nabla_m^j + \sum_{l \in L_{N-2p-1}} \frac{1}{W_l} \sum_{j=N-2p}^{N} (-1)^{j-N+2p+1} \nabla_l^j \Bigg\}$$

$$= \sum_{p=1}^{\lfloor \frac{N}{2} - 1 \rfloor} \Bigg\{ \sum_{i \in L_{N-2p+1}} \frac{1}{W_i} + \Bigg(\sum_{i \in L_{N-2p}} \frac{1}{W_i} - \sum_{l \in L_{N-2p-1}} \frac{\nabla_l^{N-2p}}{W_l} \Bigg) + \Bigg(\sum_{m \in L_{N-2p}} \frac{1}{W_m} \sum_{j=N-2p+1}^{N} (-1)^{j-N+2p} \nabla_m^j - \sum_{l \in L_{N-2p-1}} \frac{1}{W_l} \sum_{j=N-2p+1}^{N} (-1)^{j-N+2p} \nabla_l^j \Bigg) \Bigg\}$$

$$= \sum_{p=1}^{\lfloor \frac{N}{2} - 1 \rfloor} \Bigg\{ \sum_{i \in L_{N-2p+1}} \frac{1}{W_i} + \sum_{i \in L_{N-2p}} \underbrace{\Big(\frac{1}{W_i} - \frac{1}{W_i^{N-2p-1}}\Big)}_{\geq 0} + \sum_{m \in L_{N-2p}} \underbrace{\Big(\sum_{j=N-2p+1}^{N} (-1)^{j-N+2p} \nabla_m^j \Big)}_{>0} \Big(\frac{1}{W_m} - \frac{1}{W_m^{N-2p-1}} \Big) \Bigg\}$$

However, $\frac{1}{W_m} - \frac{1}{W_m^{N-2p-1}} \geq 0, \; \forall m \in L_{N-2p}$

$\Rightarrow$ II ≥ 0

III:

$$\underbrace{\Bigg(\frac{1-(-1)^N}{2} \Bigg) \Bigg(\sum_{i \in L_2} \frac{1}{W_i} + \sum_{m \in L_1} \frac{1}{W_m} \sum_{j=2}^{N} (-1)^{j-1} \nabla_m^j \Bigg)}_{\geq 0} + \sum_{i \in L_1} \frac{1}{W_i}$$

$\Rightarrow$ III > 0

Therefore, we conclude that $\alpha > 0$ for any tree $\mathcal{T}$ s.t. $\forall i \in \mathcal{T}, \exists k \in L_N$ s.t. $k \in \nabla_i^N$.

We can verify that the lemma is valid for any types of trees with one root node.

Proof of Theorem 1*:*

We consider the vector $s^0 = (s_1^0, ..., s_Y^0)$ where:

$$s_i^0 \begin{cases} = 1 - \frac{C_a}{1-a} - \frac{1}{\alpha W_i} (Y_A (1 - \frac{C_a}{1-a}) + \beta - S) + \frac{\mathbb{1}_{(N_S(i) \neq N)}}{W_i} \sum_{j \in Ch(i)} W_j & \forall i \in \mathcal{L}(\mathcal{T}_S) \\ = 1 - \frac{C_a}{1-a} - \frac{A_i}{(1-a) W_i} & \forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)) \\ = 0 & \forall i \in \mathcal{V} \backslash \mathcal{V}_S \end{cases}$$

where A_i is given in Appendix B.

First, we prove that the choice of s^0 is valid s.t. $s_i^0 \geq 0 \; \forall i$. It is straightforward to show that $\forall i \in L_k \cap \mathcal{V}_S$ s.t $k \leq N-1$, we have $\frac{C_a}{(1-a)W_i} \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \sum_{m \in Ch_S(i,j)} W_m \leq 0$.

This is done by grouping elements of the sum $\{k+1, k+2\}$, $\{k+3, k+4\}$, etc. and realizing that $-\sum_{m \in Ch_S(i,j)} W_m + \sum_{m \in Ch_S(i,j+1)} W_m \leq 0, \forall j \in \llbracket 1; N-1 \rrbracket$.

Similarly, we prove that:

$$\frac{1}{W_i} \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \sum_{\substack{m \in Ch_S(i,j) \\ f(m) \in \mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)}} W_m \leq 0, \; \forall i \in L_k \cap \mathcal{V}_S$$

s.t $k \leq N-1$.

Let $\phi = \frac{1}{\alpha}(Y_A(1 - \frac{C_a}{1-a}) + \beta - S)$.

ϕ is a positive real number since we have from Lemma 1 that $\alpha > 0$ and we supposed that $S \leq S_{min}$ where S_{min} is given in Lemma 2.

We know that $\forall i \in \mathcal{L}(\mathcal{T}_S)$, we have:

$$\begin{aligned} W_i > \; & \frac{1}{\alpha(1-\frac{C_a}{1-a})}(Y_A(1 - \frac{C_a}{1-a}) + \beta - S \\ & \qquad -\alpha \mathbb{1}_{N_S(i) \neq N} \sum_{j \in Ch(i)} W_j) \end{aligned}$$

$\forall i \in L_{N_S(i)-1} \cap (\mathcal{V_S} \backslash \mathcal{L}(\mathcal{T}_S))$, we have:

$$\begin{aligned} W_i & \geq \sum_{j \in Ch(i)} W_j \geq \sum_{j \in Ch_S(i)} W_j \\ & > \frac{\Delta_i^{N_S(i)} \phi}{1-\frac{C_a}{1-a}} - \frac{1}{(1-\frac{C_a}{1-a})} \sum_{j \in Ch_S(i)} \mathbb{1}_{N_S(j) \neq N} \sum_{k \in Ch(j)} W_k \\ & > \frac{(1-\Delta_i^{N_S(i)})\phi}{1-\frac{C_a}{1-a}} - \frac{1}{1-\frac{C_a}{1-a}} \sum_{j \in Ch_S(i)} \mathbb{1}_{N_S(j) \neq N} \sum_{k \in Ch(j)} W_k \end{aligned}$$

Let us suppose that,

$$\begin{aligned} W_i > & \frac{\phi}{1-\frac{C_a}{1-a}}(1 + \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \Delta_i^j) \\ & - \frac{1}{1-\frac{C_a}{1-a}} \sum_{j=k+1}^{N_S(i)} \sum_{\substack{m \in L_j \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(i,j)}} \mathbb{1}_{(j \neq N)} (-1)^{j-k} \sum_{t \in Ch(m)} W_t \end{aligned}$$

is true $\forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)), k \leq N-1$.

Therefore, $\forall m \in L_{k'}$ s.t $k' = k-1$ we have:

$$\begin{aligned} W_m & \geq \sum_{j \in Ch(m)} W_j \geq \sum_{j \in Ch_S(m)} W_j \geq \sum_{l \in Ch_S(m,k+1)} W_l \\ & > \sum_{l \in Ch_S(m,k+1)} \frac{\phi}{1-\frac{C_a}{1-a}}(1 + \sum_{r=k+2}^{N_S(l)} (-1)^{r-k-1} \Delta_j^r) \\ & - \frac{1}{1-\frac{C_a}{1-a}} \sum_{j \in Ch_S(i)} \mathbb{1}_{N_S(j) \neq N} \sum_{k \in Ch(j)} W_k \\ & - \sum_{j \in Ch_S(i)} \frac{1}{1-\frac{C_a}{1-a}} \sum_{r=k'+2}^{N_S(j)} \\ & \qquad \sum_{m \in L_r \cap \mathcal{L}(\mathcal{T}_S) \cap Ch_S(j,r)} \mathbb{1}_{(r \neq N)} (-1)^{r-k'-1} \sum_{t \in Ch(m)} W_t \\ & > \frac{\phi}{1-\frac{C_a}{1-a}}(\Delta_m^{k'+2} + \sum_{r=k'+3}^{N_S(i)} (-1)^{r-k'} \Delta_m^r) \\ & - \frac{1}{1-\frac{C_a}{1-a}} \sum_{j \in Ch_S(i)} \mathbb{1}_{N_S(j) \neq N} \sum_{k \in Ch(j)} W_k \\ & + \frac{1}{1-\frac{C_a}{1-a}} \sum_{j \in Ch_S(i)} \sum_{r=k'+2}^{N_S(j)} \\ & \qquad \sum_{m \in L_r \cap \mathcal{L}(\mathcal{T}_S) \cap Ch_S(j,r)} \mathbb{1}_{(r \neq N)} (-1)^{r-k'} \sum_{t \in Ch(m)} W_t \\ & > \frac{\phi}{1-\frac{C_a}{1-a}}(1 - \Delta_m^{k'+1} + \Delta_m^{k'+2} + \sum_{r=k'+3}^{N_S(i)} (-1)^{r-k'} \Delta_m^r) \\ & - \frac{1}{1-\frac{C_a}{1-a}} \sum_{r=k'+1}^{N_S(i)} \sum_{\substack{m \in L_r \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(i,r)}} \mathbb{1}_{(r \neq N)} (-1)^{r-k'} \sum_{t \in Ch(m)} W_t \\ & = \frac{\phi}{1-\frac{C_a}{1-a}}(1 + \sum_{r=k'+1}^{N_S(i)} (-1)^{r-k'} \Delta_i^r) \\ & - \frac{1}{1-\frac{C_a}{1-a}} \sum_{r=k'+1}^{N_S(i)} \sum_{\substack{m \in L_r \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(i,r)}} \mathbb{1}_{(r \neq N)} (-1)^{r-k'} \sum_{t \in Ch(m)} W_t \end{aligned}$$

Therefore, $1 - \frac{C_a}{1-a} - \frac{A_i}{(1-a)W_i} > 0 \; \forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S))$. As a result, we proved that $s_i^0 > 0 \; \forall i$.

We have $\sum_{i \in \mathcal{V}_S} s_i^0 = S$. Let $s = (s_1, ..., s_Y)$ be the strategy of the defender. By the pigeonhole principle, $\sum_{i \in \mathcal{V}_S} s_i \leq S$, thus $\exists m \in \mathcal{V}_S$ s.t. $s_m \leq s_m^0$.

We consider the attacker strategy satisfying $\sum_{i \in \mathcal{V} \backslash \mathcal{V}_S} p_i > 0$.

We construct the attacker strategy profile $p^{'}$ s.t.:

$$p_i^{'} = \begin{cases} p_i & i \in \mathcal{V}_S \text{ and } i \neq m \\ p_m + \sum_{j \in \mathcal{V} \backslash \mathcal{V}_S} p_j & i = m \\ 0 & i \in \mathcal{V} \backslash \mathcal{V}_S \end{cases}$$

$$\begin{aligned} U_A(p^{'}, s) = & \sum_{i \in \mathcal{V}_S} (W_i p_i^{'} (1-a)(1-s_i) - p_i^{'} C_a W_i) \\ & + \sum_{\substack{i \in \mathcal{V}_S \\ i \notin \mathcal{L}(\mathcal{T})}} \sum_{j \in Ch(i)} p_i^{'} W_j (1-a)(1-s_j) \\ = & \sum_{i \in \mathcal{V}_S, i \neq m} (W_i p_i (1-a)(1-s_i) - p_i C_a W_i) \\ & +(p_m + \sum_{j \in \mathcal{V} \backslash \mathcal{V}_S} p_j) W_m ((1-a)(1-s_m) - C_a) \\ & + \sum_{\substack{i \in \mathcal{V}_S, i \neq m \\ i \notin \mathcal{L}(\mathcal{T})}} \sum_{j \in Ch(i)} p_i W_j (1-a)(1-s_j) \\ & + \mathbb{1}_{(N_S(m) \neq N)} (p_m + \sum_{j \in \mathcal{V} \backslash \mathcal{V}_S} p_j) \sum_{k \in Ch(m)} (1-a) W_k \end{aligned}$$

Therefore,

$$\begin{aligned} & U_A(p, s) - U_A(p^{'}, s) \\ & = \sum_{i \in \mathcal{V} \backslash \mathcal{V}_S} (W_i p_i (1-a)(1-s_i) - p_i C_a W_i) \\ & \quad + \sum_{\substack{i \in \mathcal{V} \backslash \mathcal{V}_S \\ i \notin L_N}} p_i \sum_{j \in Ch(i)} W_j (1-a)(1-s_j) \\ & \quad - \sum_{i \in \mathcal{V} \backslash \mathcal{V}_S} p_i W_m ((1-a)(1-s_m) - C_a) \\ & \quad - \mathbb{1}_{N_S(m) \neq N} \sum_{i \in \mathcal{V} \backslash \mathcal{V}_S} p_i \sum_{k \in Ch(m)} (1-a) W_k \end{aligned}$$

$$\begin{aligned} & U_A(p, s) - U_A(p', s) \\ & \leq \sum_{i \in \mathcal{V} \backslash \mathcal{V}_S} (W_i p_i (1-a)(1-s_i) - p_i C_a W_i) \\ & \quad + \sum_{\substack{i \in \mathcal{V} \backslash \mathcal{V}_S \\ i \notin L_N}} p_i \sum_{j \in Ch(i)} W_j (1-a)(1-s_j) \\ & \quad - \sum_{i \in \mathcal{V} \backslash \mathcal{V}_S} p_i W_m ((1-a)(1-s_m^0) - C_a) \\ & \quad - \mathbb{1}_{N_S(m) \neq N} \sum_{i \in \mathcal{V} \backslash \mathcal{V}_S} p_i \sum_{k \in Ch(m)} (1-a) W_k \end{aligned}$$

$$\begin{aligned}
&U_A(p,s)-U_A(p',s)\\
&\le \sum_{i\in\mathcal{V}\setminus\mathcal{V}_S}(W_ip_i(1-a)-p_iC_aW_i)\\
&\quad+\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\notin L_N}} p_i \sum_{j\in Ch(i)} W_j(1-a)\\
&\quad-\sum_{i\in\mathcal{V}\setminus\mathcal{V}_S} p_iW_m((1-a)(1-s_m^0)-C_a)\\
&\quad-\mathbb{1}_{N_S(m)\neq N}\sum_{i\in\mathcal{V}\setminus\mathcal{V}_S} p_i\sum_{k\in Ch(m)}(1-a)W_k
\end{aligned}$$

However,

$$\begin{aligned}
&-\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\in L_N}} p_iW_m((1-a)(1-s_m^0)-C_a)\\
&-\mathbb{1}_{N_S(m)\neq N}\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\in L_N}} p_i\sum_{k\in Ch(m)}(1-a)W_k\\
&+\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\in L_N}}(W_ip_i(1-a)-p_iC_aW_i)\\
=&-\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\in L_N}} p_i\tfrac{(1-a)}{\alpha}(Y_A(1-\tfrac{C_a}{1-a})+\beta-S)\\
&+\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\in L_N}}(W_ip_i(1-a)-p_iC_aW_i)\\
=&\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\in L_N}} p_i(1-a)(W_i(1-\tfrac{C_a}{1-a})\\
&\qquad\qquad-\tfrac{1}{\alpha}(Y_A(1-\tfrac{C_a}{1-a})+\beta-S))\\
&<0
\end{aligned}$$

and,

$$\begin{aligned}
&\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\notin L_N}}(W_ip_i(1-a)-p_iC_aW_i)\\
&+\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\notin L_N}} p_i\sum_{j\in Ch(i)}W_j(1-a)\\
&-\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\notin L_N}} p_iW_m((1-a)(1-s_m^0)-C_a)\\
&-\mathbb{1}_{N_S(m)\neq N}\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\notin L_N}} p_i\sum_{k\in Ch(m)}(1-a)W_k\\
=&\sum_{\substack{i\in\mathcal{V}\setminus\mathcal{V}_S\\ i\notin L_N}} p_i(1-a)(W_i(1-\tfrac{C_a}{1-a})+\sum_{j\in Ch(i)}W_j\\
&\qquad\qquad-\tfrac{1}{\alpha}(Y_A(1-\tfrac{C_a}{1-a})+\beta-S))\\
&<0
\end{aligned}$$

Therefore, $U_A(p,s)-U_A(p',s)<0$. The payoff of the attacker is greater when operating on $p^{'}$ instead of p. The attacker attacks only nodes in $\mathcal{V}_S$.

Proof of Theorem 2*:*
The attacker needs to solve the following optimization problem:

$$\max_p U_A(p,s)\ s.t.\sum_i p_i=P$$

The Lagrangian of this optimization problem is given by:
$\mathcal{L}_1(p,s,\lambda)=U_A(p,s)+\lambda(P-\sum_i p_i)$ s.t $\lambda>0$

$\forall i\in\mathcal{L}(\mathcal{T}_S)$,
$$W_i(1-a)(1-s_i)-C_aW_i+\mathbb{1}_{(N_S(i)\neq N)}\sum_{j\in Ch(i)}(1-a)W_j=\lambda$$

$\forall i\in L_k\cap(\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S))$,
$$W_i(1-a)(1-s_i)+\sum_{j\in Ch_S(i)}W_j(1-a)(1-s_j)+\sum_{j\in\overline{Ch_S(i)}}W_j(1-a)-C_aW_i=\lambda$$

Let's assume that $\forall i\in L_k\cap(\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S))$, we have the general formula:

$$\begin{aligned}
&W_i(1-a)(1-s_i)-C_aW_i-\lambda(1+\sum_{j=k+1}^{N_S(i)}(-1)^{j-k}\Delta_i^j)\\
=&\ C_a\sum_{j=k+1}^{N_S(i)}(-1)^{j-k}\sum_{m\in Ch_S(i,j)}W_m\\
&-\sum_{j=k+1}^{N_S(i)}\sum_{\substack{m\in L_j\cap\mathcal{L}(\mathcal{T}_S)\\ m\in Ch_S(i,j)}}\mathbb{1}_{(j\neq N)}(-1)^{j-k}\sum_{t\in Ch(m)}(1-a)W_t\\
&+(1-a)\sum_{j=k+1}^{N_S(i)}(-1)^{j-k}\sum_{\substack{m\in\overline{Ch_S(i,j)}\\ f(m)\in\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S)}}W_m
\end{aligned}\tag{1}$$

Equation 1 is true $\forall i\in L_{N-1}\cap\mathcal{V}_S$. We suppose it is true $\forall i\in L_k\cap(\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S))$. We want to prove that equation 1 is valid $\forall i\in L_{k'}\cap(\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S)),k'=k-1$.

We have $\forall i\in L_{k'}\cap\mathcal{V}_S,k'=k-1$,

$$\begin{aligned}
&W_i(1-a)(1-s_i)-C_aW_i+\sum_{j\in Ch_S(i)}W_j(1-a)(1-s_j)\\
&\qquad+(1-a)\sum_{j\in\overline{Ch_S(i)}}W_j=\lambda\\
&\Rightarrow W_i(1-a)(1-s_i)-C_aW_i+\sum_{j\in Ch_S(i)}C_aW_j\\
&\quad+\sum_{j\in Ch_S(i)}(1-a)\sum_{l=k+1}^{N_S(j)}(-1)^{l-k}\sum_{\substack{m\in\overline{Ch_S(j,l)}\\ f(m)\in\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S)}}W_m\\
&\quad+\sum_{j\in Ch_S(i)}\lambda(1+\sum_{l=k+1}^{N_S(j)}(-1)^{l-k}\Delta_j^l)\\
&\quad+C_a\sum_{j\in Ch_S(i)}\sum_{l=k+1}^{N_S(j)}(-1)^{l-k}\sum_{m\in Ch_S(j,l)}W_m\\
&-\sum_{j\in Ch_S(i)}\sum_{l=k+1}^{N_S(j)}\sum_{\substack{m\in L_l\cap\mathcal{L}(\mathcal{T}_S)\\ m\in Ch_S(j,l)}}\mathbb{1}_{(l\neq N)}(-1)^{l-k}\sum_{t\in Ch(m)}(1-a)W_t\\
&\quad+(1-a)\sum_{j\in\overline{Ch_S(i)}}W_j\\
&\quad=\lambda
\end{aligned}$$

However,

$$\begin{aligned}
&C_a\sum_{j\in Ch_S(i)}\sum_{l=k'+2}^{N_S(j)}(-1)^{l-(k'+1)}\sum_{m\in Ch_S(j,l)}W_m\\
&\quad+\sum_{j\in Ch_S(i)}C_aW_j\\
&=-C_a\sum_{l=k'+2}^{N_S(i)}(-1)^{l-k'}\sum_{j\in Ch_S(i)}\sum_{m\in Ch_S(j,l)}W_m\\
&\quad+C_a\sum_{j\in Ch_S(i)}W_j\\
&=-C_a(-\sum_{j\in Ch_S(i)}W_j+\sum_{l=k'+2}^{N_S(i)}(-1)^{l-k'}\sum_{m\in Ch_S(i,l)}W_m)\\
&=-C_a\sum_{l=k'+1}^{N_S(i)}(-1)^{l-k'}\sum_{m\in Ch_S(i,l)}W_m
\end{aligned}$$

and $\lambda - \sum\limits_{j \in Ch_S(i)} \lambda(1 + \sum\limits_{l=k+1}^{N_S(j)} (-1)^{l-k} \Delta_j^l)$

$$= \lambda(1 - \sum_{j \in Ch_S(i)} 1 - \sum_{j \in Ch_S(i)} \sum_{l=k'+2}^{N_S(j)} (-1)^{l-k'-1} \Delta_j^l)$$

$$= \lambda(1 - \Delta_i^{k'+1} + \sum_{l=k'+2}^{N_S(i)} (-1)^{l-k'} \Delta_i^l)$$

$$= \lambda(1 + \sum_{l=k'+1}^{N_S(i)} (-1)^{l-k'} \Delta_i^l)$$

and $\sum\limits_{j \in Ch_S(i)} (1-a) \sum\limits_{l=k+1}^{N_S(j)} (-1)^{l-k} \sum\limits_{\substack{m \in \overline{Ch_S(j,l)} \\ f(m) \in \mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)}} W_m$

$$+(1-a) \sum_{j \in \overline{Ch_S(i)}} W_j$$

$$= -(1-a)(- \sum_{j \in \overline{Ch_S(i)}} W_j$$

$$- \sum_{l=k'+2}^{N_S(i)} (-1)^{l-k'-1} \sum_{j \in Ch_S(i)} \sum_{\substack{m \in \overline{Ch_S(j,l)} \\ f(m) \in \mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)}} W_m)$$

$$= -(1-a)(- \sum_{j \in \overline{Ch_S(i)}} W_j$$

$$+ \sum_{l=k'+2}^{N_S(i)} (-1)^{l-k'} \sum_{\substack{m \in \overline{Ch_S(i,l)} \\ f(m) \in \mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)}} W_m)$$

$$= -(1-a) \sum_{l=k'+1}^{N_S(i)} (-1)^{l-k'} \sum_{\substack{m \in \overline{Ch_S(i,l)} \\ f(m) \in \mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)}} W_m$$

and finally,

$$- \sum_{j \in Ch_S(i)} \sum_{l=k+1}^{N_S(j)} \sum_{\substack{m \in L_l \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(j,l)}} \mathbb{1}_{(l \neq N)} (-1)^{l-k} \sum_{t \in Ch(m)} W_t$$

$$= - \sum_{j \in Ch_S(i)} \sum_{l=k'+2}^{N_S(j)} \sum_{\substack{m \in L_l \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(j,l)}} \mathbb{1}_{(l \neq N)} (-1)^{l-k'-1} \sum_{t \in Ch(m)} W_t$$

$$= \sum_{l=k'+2}^{N_S(i)} \sum_{j \in Ch_S(i)} \sum_{\substack{m \in L_l \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(j,l)}} \mathbb{1}_{(l \neq N)} (-1)^{l-k'} \sum_{t \in Ch(m)} W_t$$

$$= \sum_{l=k'+1}^{N_S(i)} \sum_{m \in L_l \cap \mathcal{L}(\mathcal{T}_S) \cap Ch_S(i,l)} \mathbb{1}_{(l \neq N)} (-1)^{l-k'} \sum_{t \in Ch(m)} W_t$$

Therefore, equation 1 is true $\forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S))$.

Let $A_i = \lambda(1 + \sum\limits_{j=k+1}^{N_S(i)} (-1)^{j-k} \Delta_i^j)$

$$+C_a \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \sum_{m \in Ch_S(i,j)} W_m$$

$$+(1-a) \sum_{j=k+1}^{N_S(i)} (-1)^{j-k} \sum_{\substack{m \in \overline{Ch_S(i,j)} \\ f(m) \in \mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)}} W_m$$

$$- \sum_{j=k+1}^{N_S(i)} \sum_{\substack{m \in L_j \cap \mathcal{L}(\mathcal{T}_S) \\ m \in Ch_S(i,j)}} \mathbb{1}_{(j \neq N)} (-1)^{j-k} \sum_{t \in Ch(m)} (1-a) W_t$$

$$\Rightarrow \begin{cases} s_i = 1 - \frac{C_a}{1-a} - \frac{\lambda}{(1-a)W_i} \\ \quad + \frac{\mathbb{1}_{(N_S(i) \neq N)}}{W_i} \sum\limits_{j \in Ch(i)} W_j \quad \forall i \in \mathcal{L}(\mathcal{T}_S) \\ s_i = 1 - \frac{C_a}{1-a} - \frac{A_i}{(1-a)W_i} \qquad \forall i \in L_k \cap (\mathcal{V}_S \backslash \mathcal{L}(\mathcal{T}_S)) \end{cases}$$

We have $\sum\limits_i s_i = S$, where $0 \leq s_i \leq 1 \ \forall i$.

Therefore, we find that,

$$\lambda = \frac{(1-a)}{\alpha}(Y_A(1 - \frac{C_a}{1-a}) + \beta - S)$$

where α and β are given in Appendix B.

By substituting λ in the equations of s_i, we find the results in Theorem 2.

Defender optimization problem:

The defender needs to solve the following optimization problem:

$$\max_s U_D(p, s) \ s.t. \sum_i s_i = S$$

The Lagrangian of this optimization problem is given by:

$\mathcal{L}_2(p, s, \lambda) = U_D(p, s) + \mu(S - \sum\limits_i s_i)$ with $\mu > 0$

We consider that the sensible target set $\mathcal{V}_S$ is nonempty. Therefore, at least the root node of the tree belongs to $\mathcal{V}_S$. We refer by 1, the root node of $\mathcal{T}$.

From Definition 2, we know that $\forall i \in \mathcal{V}_S, \ f(i) \in \mathcal{V}_S$.

We have $W_1(1-a)p_1 - C_e W_1 = \mu$

$\forall i \in L_k \cap \mathcal{V}_S, k \geq 2,$

$W_i(1-a)(p_i + p_{f(i)}) - C_e W_i = \mu$

Let's assume that $\forall i \in L_k \cap \mathcal{V}_S, k \geq 2$, we have the general formula:

$$W_i(1-a)p_i - p_1 W_1 (1-a)(1 + W_i \sum_{j=1}^{k-1} \frac{(-1)^{k-j}}{W_i^j})$$

$$= C_e W_i (\frac{1+(-1)^k}{2}) + C_e W_1 (-1 + \mathbb{1}_{(k>2)} W_i \sum_{j=2}^{k-1} \frac{(-1)^{k-j+1}}{W_i^j}) \tag{2}$$

We note that $W_i^k = W_i, \ \forall i \in L_k$. We want to prove that equation 2 is true $\forall i \in L_{k'} \cap \mathcal{V}_S, k' = k+1$ and $f(i) \in \mathcal{V}_S$.

We have:

$$W_i(1-a)(p_f(i)) = p_1 W_1 (1-a)(\frac{W_i}{W_{f(i)}} + W_i \sum_{j=1}^{k-1} \frac{(-1)^{k-j}}{W_{f(i)}^j})$$

$$+W_1 C_e (-\frac{W_i}{W_{f(i)}} + W_i \sum_{j=2}^{k-1} \frac{(-1)^{k-j+1}}{W_f(i)}) + C_e W_i \frac{1+(-1)^k}{2}$$

We know that $W_i^j = W_{f(i)}^j$. Therefore, $\forall i \in L_{k'}$:

$$p_i W_i (1-a) - C_e W_i$$

$$= p_1 W_1 (1-a) - C_e W_1 - p_{f(i)} W_i (1-a)$$

$$\Rightarrow p_i W_i (1-a) + C_e W_i (-1 + \frac{1-(-1)^{k'}}{2})$$

$$= p_1 W_1 (1-a)(1 - \frac{W_i}{W_i^k} + W_i \sum_{j=1}^{k'-2} \frac{(-1)^{k'-j}}{W_i^j})$$

$$+C_e W_1 (-1 + \frac{W_i}{W_i^k} + W_1 \sum_{j=2}^{k'-2} \frac{(-1)^{k'-j+1}}{W_i^j})$$

$$\Rightarrow W_i (1-a) p_i - C_e W_i \frac{(1+(-1)^{k'})}{2}$$

$$= p_1 W_1 (1-a)(1 + W_i \sum_{j=1}^{k'-1} \frac{(-1)^{k'-j}}{W_i^j})$$

$$+C_e W_1 (-1 + W_i \sum_{j=2}^{k'-1} \frac{(-1)^{k'-j+1}}{W_i^j})$$

We have $\sum\limits_{i \in \mathcal{V}_S} p_i = P$, where $0 \leq p_i \leq 1 \ \forall i$. By substituting the values of p_i in this equation and solving it, we find the results in Theorem 2.

APPENDIX B

$$
\begin{aligned}
\alpha &= \sum_{i\in\mathcal{V}_S}\frac{1}{W_i}+\sum_{r=1}^{N-1}\sum_{i\in L_r\cap(\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S))}\frac{\sum_{j=r+1}^{N_S(i)}(-1)^{j-r}\Delta_i^j}{W_i}\\
\beta &= \sum_{r=1}^{N-1}\sum_{i\in L_r\cap\mathcal{L}(\mathcal{T}_S)}\sum_{j\in Ch(i)}W_j\sum_{l=1}^{r}\frac{(-1)^{r-l}}{W_i^l}\\
&-\frac{C_a}{1-a}\sum_{r=1}^{N-1}\sum_{i\in L_r\cap(\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S))}\sum_{j=r+1}^{N_S(i)}\sum_{m\in Ch_S(i,j)}\frac{(-1)^{j-r}W_m}{W_i}\\
&-\sum_{r=1}^{N-1}\sum_{i\in L_r\cap(\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S))}\sum_{j=r+1}^{N_S(i)}\sum_{\substack{m\in\overline{Ch_S(i,j)}\\ f(m)\in\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S)}}\frac{(-1)^{j-r}W_m}{W_i}\\
A_i &= \frac{(1-a)}{\alpha}(Y_A(1-\frac{C_a}{1-a})+\beta-S)(1+\sum_{j=k+1}^{N_S(i)}(-1)^{j-k}\Delta_i^j)\\
&+C_a\sum_{j=k+1}^{N_S(i)}(-1)^{j-k}\sum_{m\in Ch_S(i,j)}W_m\\
&+(1-a)\sum_{j=k+1}^{N_S(i)}(-1)^{j-k}\sum_{\substack{m\in\overline{Ch_S(i,j)}\\ f(m)\in\mathcal{V}_S\setminus\mathcal{L}(\mathcal{T}_S)}}W_m\\
&-\sum_{j=k+1}^{N_S(i)}\sum_{\substack{m\in L_j\cap\mathcal{L}(\mathcal{T}_S)\\ m\in Ch_S(i,j)}}\mathbb{1}_{(j\neq N)}(-1)^{j-k}\sum_{t\in Ch(m)}(1-a)W_t\\
\gamma &= 1+W_1\sum_{r=2}^{N}\sum_{i\in L_r\cap\mathcal{V}_S}(\frac{1}{W_i}+\sum_{j=1}^{r-1}\frac{(-1)^{r-j}}{W_i^j})
\end{aligned}
$$

ACKNOWLEDGMENT

The authors would like to thank Frederic Guyomard in the Department SINETICS at EDF for his help and support that improved the quality of this paper.

REFERENCES

[1] U.S. Energy Information Administration, *International Energy Outlook 2013*, URL: http://www.eia.gov/forecasts/ieo/pdf/0484(2013).pdf, July 2013.

[2] European Network and Information Security Agency, "Smart Grid Security: Annex I. General Concepts and Dependencies with ICT", 2012.

[3] European Network and Information Security Agency. "Smart Grid Security: Annex II. Security aspects of the smart grid", 2012.

[4] EBIOS (Expression of Needs and Identification of Security Objectives) Risk Management Method, *ANSSI*, URL: http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf, 2010.

[5] M. J. Osborne and A. Rubinstein, "A course in game theory". *MIT Press*, 1994.

[6] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges", *Computer Networks*, vol. 57, Issue 5, April 2013.

[7] D.K. Mulligan, L. Wang and A.J. Burstein, "Privacy in the smart grid: an information flow analysis", Report for the Privacy Issues in the Smart Grid project, March 2011.

[8] F. Li, B. Luo and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption", *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 327-332, 2010.

[9] C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford and P. Armstrong, "Power signature analysis", *Power and Energy Magazine*, IEEE, vol. 1, no. 2, pp. 56-63, Mar-Apr 2003.

[10] C. Rottondi, G. Verticale and C. Krauss, "Distributed Privacy-Preserving Aggregation of Metering Data in Smart Grids", *Journal on Selected Areas in Communications*, Smart Grid Communications series, vol.31, no.7, pp.1342–1354, July 2013.

[11] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data", *IEEE SmartGridComm'10*, pp. 238-243, 2010.

[12] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis and R. Capeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures", *1st IEEE International Conference on Smart Grid Communications*, pp. 232–237, 2010.

[13] A. Rial and G. Danezis, "Privacy-Preserving Smart Metering" , *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, 2011.

[14] C. Rottondi, G. Verticale and A. Capone, "Privacy-Preserving Smart Metering with Multiple Data Consumers", *Computer Networks*, vol.57 no.7, pp.1699–1713, May 2013.

[15] L. Chen and J. Leneutre, "A game theoretical framework on intrusion detection in heterogeneous networks", *IEEE Transactions on Information Forensics and Security*, 4(2), pp. 165-178, june 2009.

[16] W. Saad, Z. Han, H. V. Poor and T. Basar, "Game theoretic methods for the smart grid", *IEEE Signal Processing Magazine, Special issue on Signal Processing for the Smart Grid*, vol. 29, no. 5, pp. 86–105, September 2012.

[17] R. Berthier and W.H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures", *In Proceedings of the 17th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC)*, pp. 184-193, December 2011.

Ziad Ismail is currently Ph.D. candidate in the Department SINETICS at EDF and the department of Computer Science and Networks of Telecom Paristech, Paris. He received his B.E. degree in Telecommunication Engineering from ESIB, Lebanon in 2009 and the Engineer Diploma from Telecom ParisTech, Paris in 2012. His main research interests include security policies optimization and enforcement in smart grids, modelling of security strategies for smart grids, and game theory.

Jean Leneutre received his Ph.D in Computer Science from Telecom ParisTech, Paris, in 1998. He is currently an associate professor in the Department of Computer Science and Networks at Telecom ParisTech, CNRS LTCI UMR 5141, and is co-leader of the Network and Information Security team. His main research interests include the definition of security models and design of security mechanisms for complex systems and networks.

David Bateman graduated from the University of Sydney in 1988 (BSc (Physics) with 2nd class honours), and from the same university in 1990 (BEng with 1st class honours). He then worked with the CSIRO Division of Telecommunications and Technology, Sydney, till 1999 where his research interests were in the electromagnetic analysis and measurement of antennas. During his time with CSIRO he completed his PhD, graduating in 1998. From 2000 to 2008 he worked for Motorola Labs Paris, where he was a senior staff research engineer dealing with RF aspects of WLAN systems and leader of a radio prototyping team which includes aspects of PHY and system design. He is the manager of the Computing, Communication and Security Infrastructure group of EDF R&D

Lin Chen received his B.E. degree in Radio Engineering from Southeast University, China in 2002 and the Engineer Diploma, Ph.D from Telecom ParisTech, Paris in 2005 and 2008, respectively. He also holds a M.S. degree of Networking from the University of Paris 6. He currently works as associate professor in the department of computer science of the University of Paris-Sud XI. His main research interests include modeling and control for wireless networks, security and cooperation enforcement in wireless networks and game theory.