Review of Anomalies Detection Schemes in Smart Grids

Andres F. Murillo *

* Grupo de Teleinformática e Automação, UFRJ - COPPE/PEE - DEL/Poli, Rio de Janeiro – RJ – Brazil
Email: afmurillo@gta.ufrj.br

***Abstract*—This paper presents a review of some Anomalies Detection Scheme, the schemes analyzed used authentication techniques, codification techniques and traffic analysis to avoid intrusion and the malfunctioning of a Smart Grid a discussion is offered for each of these schemes.**

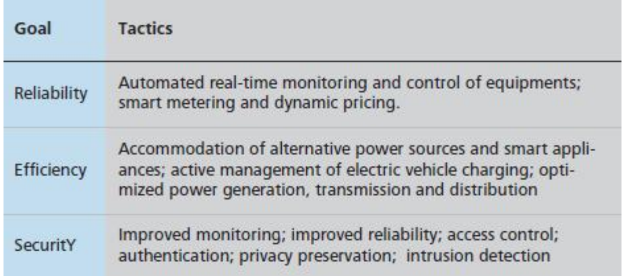
I. Introduction

Smart Grids have been defined as an answer to improve the current Power Electric Grid that has lacked of the extensive use of Communications developments that have took place in the last years. With the integration of a Communications Network the Power Electric Grid will be able to obtain more information about users consume and the state of the Grid, this will enhance the current Charge and Balance Control mechanisms, and allow the use of optimization techniques to find the best power generation, transmition and delivery strategies for a determined state of the grid. In order to accomplish with these goals the Smart Grids must be very secure networks that can guarantee the traditional security premises that have been identified in traditional Communications Networks. This proposes a big challenge due to the importance of the Power Electric Grid to the actual society, before the Smart Grids are generally deployed secure frameworks should be proposed, deployed and tested to ensure that they will protect the Grid for attacks that could put in risk the functionality of the Power Electric Grid. In this paper a review of some Anomalies Detection Scheme is presented, the schemes analyzed used authentication techniques, codification techniques and traffic analysis to avoid intrusion and the malfunctioning of a Smart Grid.

The organization of the paper is the following: Section II Presents the current Architecture for Smart Grids, Section III presents the currently identified threats for Smart Grids, Section IV presents the Anomalies Detection Schemes and Section V presents the Conclusions

II. Architecture of Smart Grids

Smart Grids are presented as the convergence between the traditional Power Electric Network and a Telecommunications Network. This convergence would allow the power utilites to collect a wide range of information about the electric system, such as: user consumption rates, charge level at the substations and state of the electric grid equipment. This convergence could also ease the inclusion of Distributed Energy Generation, with the participation of Alternative Energy Sources. This flow of information could enhance the Grid functionality, increase its controllability and create new paradigms of energy consume. Consumers and energy suppliers alike can take advantage of the convenience, reliability, and energy savings provided through real time energy management [1]. Some of its goals and tactics are shown in the figure 1.



Goal	Tactics
Reliability	Automated real-time monitoring and control of equipments; smart metering and dynamic pricing.
Efficiency	Accommodation of alternative power sources and smart appliances; active management of electric vehicle charging; optimized power generation, transmission and distribution
SecuritY	Improved monitoring; improved reliability; access control; authentication; privacy preservation; intrusion detection

Figure 1. Smart Grids goals and tactics [2]

Along with these enhancements come multiple security risks [3] that should be managed in order to supply a secure framework for Smart Grid that allows its proper functioning, to understand these risks it is necessary to explain the architecture of Smart Grids, its characteristics, possibilities, and components. The related literature explains Smart Grids through two perspectives: A perspective from the point of view of the Power Electrical Grid, composed by Generation, Transmission, Distribution, Consumption, Service Provision; and a perspective from the Telecommunications Network: Home Area Network (HAN), Neighborhood Area Network, (NAN) and Wide Area Network, (WAN). The figure 2 shows these perspectives [4].

A. Perspective of Power Electrical Grid

This perspective is the traditional way of understanding the Electrical Grid and consists of five components [5]

- Generation: Power system generators produce electric power by different means such as hydropower, solar, wind, tidal forces, and other generation sources.
- Transmission: A very high voltage infrastructure transfers electrical energy from power plants to electrical substations.
- Distribution: Distribution networks step down voltage and delivers electricity from substations to consumers.
- Consumption: Energy consumers use the electric energy in a multitude of ways.

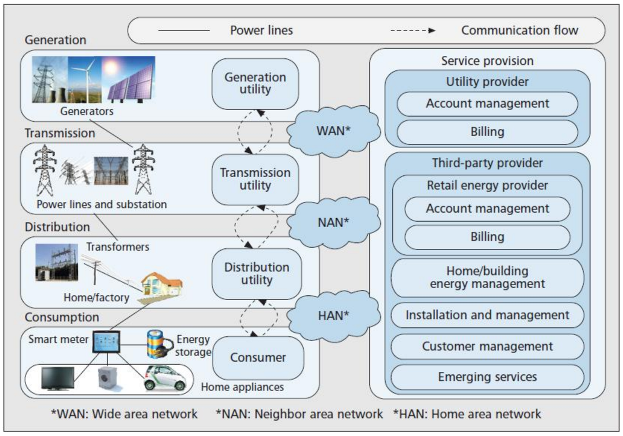


Figure 2. An overview of the Smart Grid with various service providers [4]

• Service provision: The service provider performs services to support the business processes of power system generators and consumers

With Smart Grid in the Generation component alternative sources of energy could be included in the main network, this implies that a constant flow of information would be established between these points of generation and the Control entities of the Main Generators, the infrastructure for this bidirectional flow of information should be protected, as it could be information used to take decisions related to load balancing and response to possible events, such as blackouts. In the Distribution component In the Distribution component, information about Energy Consumption will flow constantly towards the Service Providers and Electrical Utilities, this information could be privacy sensitive, could be prone to falsification and be used to create denial of services attacks.

B. Perspective of Telecommunications Networks

From this perspective the Smart Grid (SG) is analyzed can be viewed as an information sharing network comprising a number of hierarchical components: Home Networks (or Building Networks), Neighborhood Networks and Wide Area Networks [6]. Broadly speaking, a city has a number of regions, each of which is covered by a distribution substation. Every region comprises several neighborhoods, each neighborhood has many buildings, and each building may have a number of apartments. We derive our smart grid communication architecture from this real-life planning of a metropolitan area.

Home Area Network (HAN)

Each HAN could represent a House, a Building or any sort of Individual user of the Smart Grid. In each HAN there are advanced meters called smart meters deployed in the SG architecture that represent and Advanced Metering Infraestructure (AMI) for enabling automated two-way communication between the utility meter and the utility provider. The smart meters are equipped with two interfaces: A power reading interface and a communication gateway interface.

Neighborhood Area Network (NAN)

A NAN is a network that groups one or more HAN Networks and counts with interfaces to communicate with the higher layer in the Smart Grid [7], this is a is a large metering and controlling network which collects metering and service information from the multiple HANs that are geographically near each other.

Through a NAN GW, the utility provider is able to monitor how much power is being distributed to a particular neighborhood by the corresponding distribution substation [8].

Wide Area Network (WAN)

The WAN layer provides broadband wired and wireless communication between the NAN, substations, other distributed grid devices, and the utility [7]. This layer should have similar characteristics to a backbone network, aggregating information from the users and transporting it to the control centers of the Smart Grid.

III. Information Security Threats in Smart Grids

As mentioned earlier, Smart Grids could enhance the current features of the Power Electric Grids by bridging it with a Communications Network, this kind of convergence could offer real-time information about the grid operation status, so the control centers may easily ensure power efficiency by applying optimization techniques to find the best power generation, transmission and delivery strategies with respect to given constraints [2]. However this convergence brings the traditional security threats of a communications network to the electric grid and also creates new kinds of threats that are still under study. These threats could take place in both the physical and information space; in this paper only the later are analyzed. The Smart Grids increased openness favors adversaries and brings additional security vulnerabilities to the grid. In conventional power grid, there is normally only one access point to the grid management system in a neighborhood. In smart grid, smart meters are massively deployed as access points, one per customer, in order to engage customers in utility management. They are connected to the Internet for ease of management. These access points are ideal portals for intrusions and malicious attacks [2]. Also, in Smart Grids the energy is generated in a distributed manner, implying that some control information must be exchanged between the generation centers and the control centers, these centers should mutually authenticate in order to ensure the proper operation of the generation layer, also the information sent by these centers must be accurate and secure to avoid malfunctions. In the following some types of attacks will be presented to offer a general idea of the security threats in Smart Grids, first some general type of attacks are presented, later some more specific attacks are presented and their possible impact in Smart Grids. It should be noticed that until the time of redaction of this paper, in the consulted literature, no real tests of attacks have been performed in Test Beds of Smart Grids, it could be interesting to set up controlled scenarios to evaluate in a more realistic manner the impact of these attacks.

Among the general attacks, mentioned in [2] there are:

• Device attack: Aims to compromise (control) a device. It is often the initial step of a sophisticated attack, in which the compromised device will be used to launch further attacks such as data attacks and network availability attacks toward the smart grid or perform malicious physical actuation (if the device is a control element). For example, a compromised IED such as a circuit breaker may break a circuit maliciously and cause power outage. To resist device attacks, strict access control is necessary.

• Data attack: Attempts to malicious insert, alter, or delete data or control commands in the network traffic so as to mislead the smart grid to make wrong decisions/actions. One commonly observed data attack is that a customer jeopardizes the smart meter in order to reduce its electricity bill. Another example is that a compromised RTU is informed about a fault detected by a faulted circuit indicator (FCI) device, but it refuses to report the fault to the control center, resulting in increased outage time. To resist this attack, data integrity and authenticity must be protected, and effective intrusion detection mechanisms ought to be developed.

• Privacy attack: Aims to learn/infer users' private information by analyzing electricity usage data. In smart grid, electricity usage information is collected multiple times per hour by smart meters so as to obtain fine-grained information about the grid status and improve grid operation efficiency. Clearly, such privacy-sensitive information must be protected from unauthorized access.

• Network availability attack: Takes place in the form of denial of service (DoS). Its objectives are to use up or overwhelm the communication and computational resources of the smart grid, resulting in delay or failure of data communications. For example, an adversary may flood a control center with false information at very high frequency such that the control center spends most of he time verifying the authenticity of the information and is not able to timely respond to legitimate network traffic. Communication and control in smart grid are time critical. A delay of a few seconds may cause irreparable damage to the national economy and homeland security. A network availability attack must be handled effectively.

Some more elaborated attacks that could be present in Smart Grids [8] [9] are:

• Data Integrity Attacks: Involve manipulating the signals to spurious values that could either force the control center to make wrong decisions, or force the actuator to incorrectly modify the physical device, depending on what signal is attacked.

• Denial of Service (DoS) Attacks: Will result in delayed control action. In a scenario where the physical system requires deadline-constrained corrective control, a DoS attack could drive the system to instability.

• Replay Attacks: Involve the retransmission of legitimate control or measurement packets. This may result in incorrect decision making, this kind of attacks can heavily affect the networked power controlled systems.

• Timing Attacks: Are a variation of the DoS attack. Instead of completely denying communication between the system and control, the adversary will introduce a delay in signal transmission, this delay will affect the performance of the Controller, it could even destabilize the controlled system.

• Desynchronization Attacks: A variation of timing attacks, are attacks that target controls that require strict synchronization.

• Sniffing attacks: This kind of attacks could expose sensitive data related to the Smart Grid users, and also related to the internal functioning of the electrical companies.

• Reconfigure attack: This involves installing malicious firmware on Smart Grid devices, and using them to perform different kind of attacks to the Grid.

IV. Intrusion Detection

Provide a secure environment for Smart Grids is a great challenge in the actuality, deploying Smart Grids without the appropriate security measures could lead to huge economical and social losses due to the important of the Electric Power Grid to the society. Although there is no perfect system of security, efforts should be continuous directed to improve the current security tools to the communications networks and develop new ones as we slowly start to understand the unique characteristics of the Smart Grids. This paper is focused in the detection of intrusions in a Smart Grid, defining intrusion as the use of resources of the Smart Grid for unauthorized parties or the intentioned actions oriented to tamper the performance of the Grid. Various proposals have been done in this field; in this paper we will group some of them under the following categories:

• Autentication mechanisms • Detection of unexpected behavior • Information codification

A. Autentication Mechanisms

Most of the authentication mechanisms for Smart Grids have been inspired in the authentication models such as PKI, some modifications have been done to adjust to the SG characteristics, that is the case of "A lightweight message authentication Scheme for SG", that reduces the number of authentication messages exchanged between the parties in order due to the limited computational resources of smart meters and gateways and the estimated huge number of these devices in a SG.

1) Privacy-preserving and accountable authentication framework:

The framework[4] is based on an scenario showed in Figure 3. Here a Service Provider is introduced in the traditional interactions between users and electric utilities, these Service Provider is independent from the Electric utility, one of the main characteristics of this proposal is that none of this parties is considered to be trustworthy. Also a Law Authority is considered as an upper layer party which could audit the Grid.

The proposal involves three kinds of entities: electric utility, service providers, and consumers organized in groups. Each consumer group is a collection of consumers according to contacted service provider. Each consumer group has one group manager responsible for distributing member secret keys, adding and removing consumers.

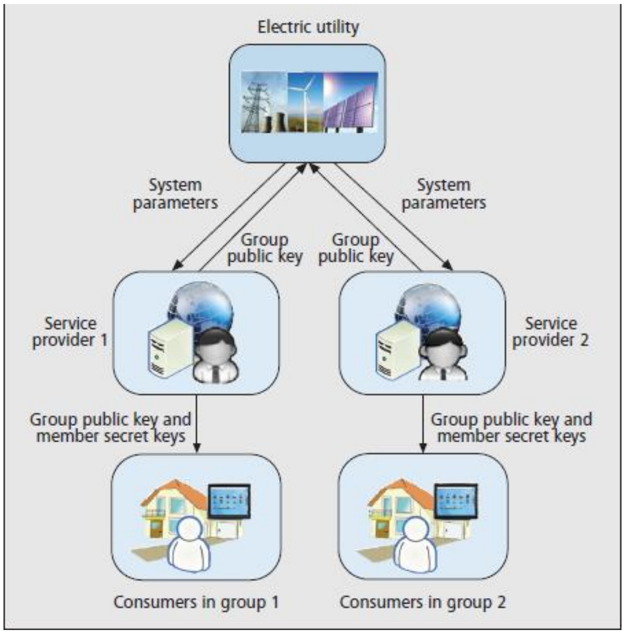


Figure 3. Trust and key management model of the proposed privacy-preserving and accountable authentication framework.

Before accessing a service provider, each consumer has to enroll in the consumer group whose manager thus knows the real identity of the consumer. The electric utility generates the system parameters and group private key, and keeps the group private key secretly. Upon receiving a registration request from a service provider, the electric utility delivers the system parameters to this service provider. Then, as the group manager, the service provider generates the group public key. Such a key management scheme is based on the principle of "separation of powers" and possesses a number of salient features. First, from the point of view of access control, each legitimate consumer with a valid member secret key can generate a valid access credential (i.e., the group signature of a fresh access request). The validity of this access credential can be verified by the service provider through the group public key. Hence, access security is guaranteed. Second, the proposal divides the group private key and the mapping of the member secret keys to the identities of the consumers among two autonomous entities: the electric utility and service provider. Electric utility knows the group private key, but not the mapping of the member secret keys to the identities of the users; as the group manager, a service provider knows the mapping of the member secret keys to the identities of the consumers, but not the group private key. As a result, given an access credential generated by a consumer, neither the service provider nor the electric utility can determine consumer's identity or compromise his/her privacy. Therefore, user privacy is enhanced. Finally, with the help from both electric utility and user group manager, only the law authority can link any communication session to the corresponding consumer who is responsible.

Autentication Mechanism:

First, the electric utility generates the group private key gmsk and system parameters, keeps the former secretly, and distributes the latter to each group manager

Second, with the system parameters, each group manager selects a random number y as the private key, and then computes the group public key gpk.

Third, after that, the group manager delivers the group public key gpk to each group member. The group manager keeps the mapping between each individual consumer i and his/her corresponding member secret key gsk_i =(A_i, x_i) , where x_i is a number randomly picked for each user, and A_i is computed from x_i and x_y.

It is important to notice that with this mechanism is the Electrical Utility that has the role of a CA in the traditional PKI Model. This means that the addition of any Service Provider to the Smart Grid will require authorization by the Electrical Utility, which creates a certain dependency between them.

2) A lightweight two-step mutual authentication protocol:

This protocol [8] is based on the assumption that some Smart Grid devices, such as Smart Meters, will have limited memory and computational resources and aims to simplify the authentication protocol. The protocol is showed in the Figure 4.

At the first step, i encrypts $i \parallel j \parallel g^a$ with j's public key (a is a random number), and sends the ciphertext to j. At the second step, j decrypts the received ciphertext and responds to i with a newly generated ciphertext on $i \parallel j \parallel g^b$ using i's public key (b is a random number). After these two steps, both devices i and j can calculate $g^{ab} = (g^a)b = (g^b)a$, and derive the shared session key as $k_{ij} = H(i \parallel j \parallel gab)$, where $H : \{0, 1\}^* n \rightarrow Z_q^*$ is a publicly known hash function. Both of them are able to identify each other since the secrets g^a and g^b can be accessed only by each other. Because random numbers a and b are deleted after the generation of k_ij the compromise of either i's or j's long-term private keys does not affect the security of the previous session keys.

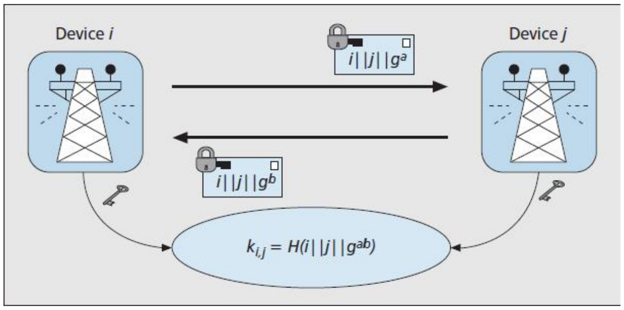


Figure 4. Two-step mutual authentication

This mechanism lacks an CA and could have some debilities due to the fact that it does not solve the validity of the public keys generated, however it could use a mechanism that generates the public key using the devices ID to tackle this problem.

3) Zero configuration identity based Signcryption scheme for Smart Grid:

This scheme [10] tries to get rid of the need of a CA party that guarantees the identity of the interacting components in an authentication scheme, that is, the validity their public keys. For these each component is assumed to have an unique ID and this ID is in turn used as the identity of the device for all subsequent cryptographic functions. First, a device must register with a central key-generating server (KGS) to obtain its private key if it wants to decrypt message received or sign message to be transmitted during its operation. The KGS holds the master key of the system that is required for generating the private key of a device. Once equipped with its private key, a device may then communicate with any other devices in the smart grid without contacting the KGS again. In this sense, the workload of our KGS is much lower than a certificate authority (CA) of a conventional public-key infrastructure (PKI). Subsequently, when a device A wants to transmit data to device B, A would encrypt each individual packet with a unique key generated based on B's public key and sign each packet using its own private key. Upon receiving an encrypted packet, B decrypts the encrypted packet using its own private key and verifies the content of the decrypted packet using A's public key. As a proof-of-concept, AES was chosen in our scheme for the encryption of the content of data packets. As the authors mention, using this scheme would require to consider the KGS to be ultra-secure, as it encompasses the full knowledge of private keys of all devices, allowing it to decrypt any message sent to any device or impersonate any device to sign any message sent to others. There are two ways to reduce the risk of breaking the entire IBC system owing to the compromise of the KGS; first, by using distributed key generating servers, and second, by using short-lived master key. In the first method, x is split into two or more parts. Each part, x_i, is then kept independently by a different key generating server, KGSi. When a device, such as Alice registers with the system, she must approach each KGS independently. Each KGS will then return a partial private key as well as x_{iP} to her after verifying her identity. Once equipped with such information, Alice may then calculate her true private key, x_A as well as x_P. Since each KGSi possesses only x_i, no individual KGS can calculate the private key of any device unless all KGS conspire to do so, which also reduces the risk of compromising x if any one KGS is compromised. However with this approach an attacker could cause a Negation of Service type of attack be compromising one of the KGS, due to the fact that only with the totality of the KGS the authentication would work. The second method to lower the chance of compromising the master secret key, x is by employing a short-lived master key. In this case, KGS changes the value of x at a regular interval. With each new master key, private keys for all devices are also updated, to perform this actualization the GKS generates a new master key, calculates the private keys of all devices in the system and uses the device's old public key to encrypt the new private key to each device. After generating the private keys of all smart meters, KGS needs to distribute the private key to each smart meter. As the total number of smart meters in a smart grid may be huge, it is not possible to distribute the keys to all smart meters simultaneously. It is proposed to have a grace period in which both the expired key and the new key can coexist. This functionality would cause a periodic "flood" of the devices private keys, which could compromise the system security, also the grace period could cause false repulsion between devices or allow the authentication of compromised devices with old keys.

B. Activity analysis mechanisms

1) Codification technique to protect and Distributed Storage System from Malicious Nodes:

Although not specifically designed for Smart Grid, the authors in [11] propose a coding mechanism to Secure Dynamic Distributed Systems (DSS) from Malicious Nodes. An SDS has certain characteristics that are very similar to a Smart Grid in the sense that the information contained in the Smart Meters and other devices that form the Advanced Meterin Infraestructure (AMI) is stored in a distributed matter, but commonly analyzed in a centralized manner by a Control Center.

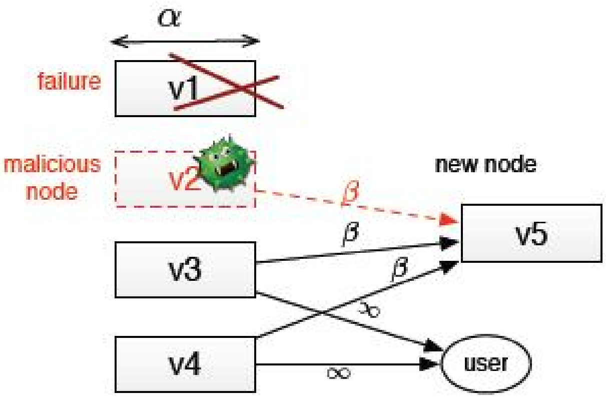


Figure 5. Distributed Storage System under attack by malicious nodes

The figure 5 shows the scenario of an DSS with malicious nodes. The DSS is formed by n storage nodes $v_1 ... v_n$ each having a storage capacity of α symbols. The storage nodes are individually unreliable and may fail over time.

To guarantee a desired level of reliability, the system is repaired when a failure occurs by replacing the failed node with a new node of the same storage capacity

$$\alpha$$

. The DSS should allow any legitimate user or data collector to reconstruct the file by contacting any k out of the n active storage nodes. The condition is termed as the reconstruction property of distributed storage systems.

Repair Process: It is assumed that nodes fail one at a time1 and we denote by v_{n+i} the new replacement node added to the system to repair the i-th failure. The new replacement node connects to some d nodes, $d \geqslant k$, chosen, possibly randomly, out of the remaining active n - 1 nodes and downloads γ symbols in total from them, which is then possibly compressed ($\alpha < \gamma$) and stored on thenode. Thus, the DSS is denoted by the triplet (n, k, d). The total amount of data (in symbols) downloaded for repair is γ , as the repair bandwidth of the system. The new replacement node downloads equal amounts of β= γ/d symbols for each contacted node.

Adversary Model: A presence of an active adversary Calvin is assumed, he can control a certain number of nodes in the DSS. Calvin is assumed to be omniscient, i.e., he knows the stored file and the data stored on the individual nodes. Moreover, Calvin can control b nodes in total, where 2b ¡ k, that can include some of the original nodes v_1...; v_n, and/or some replacement nodes v_{n+1}, v_{n+2}.... Calvin can maliciously alter the data stored on the nodes under his control. He can also send erroneous outgoing messages when contacted for repair or reconstruction.

This could be the scenario of a AMI present in a Smart Grid, where a number of malicious nodes are compromised and thus could report false information to the upper layers, possibly causing that the Control Centers report false information or take wrong decisions about the Smart Grid state.

The authors determined and upper level equal to

$$C_r(\alpha,\gamma) \leq \sum_{i=2b+1}^{k} min(d-i+1)\beta, \alpha$$

With β= γ / d for k $\leq$ 2b, $C_r(\alpha,\gamma)$ = 0 Also the authors propose the use of RSKR-repetition code to protect the information for malicious nodes (respecting the upper bound established earlier) and an algorithm for decodification that could help to identify malicious nodes, this due to the fact that the decoder can decode the correct message, and thus can identify the indices of the erroneous symbols. The data collector can then report this set of indices to a central authority (tracker) in the system. This authority can further combine such information from multiple data collectors, and knowing the RSKR-repetition structure, it forms a list of suspected nodes that will surely include the malicious nodes. Since there are at most b malicious nodes and each symbol xi is stored on exactly two nodes, the size of the list will be at most 2b. The system is then purged by discarding the nodes in this list The problem with this proposal is that the complexity of the decoding algorithm increases exponentially with the number of nodes and it's unpractical to implement it against a powerful adversary than can control a lot of nodes.

2) Malicious activity Detection using traffic analysis:

This proposal [6] is aimed to prevent certain sort of attacks such as DoS or DDoS, and is based in the estimated characteristics of the regular traffic in a Smart Grid infrastructure. The objective of this proposal is to use well known patterns of traffic and requests to detect malicious activity. For example, a group of nodes trying to perform a DoS would not use the typical traffic pattern present in a Smart Grid, with this information the system could detect that anomaly is present in the network and the nodes responsible for it. The authors design this scheme to be implemented in certan gateways along the Smart Grid.In the proposal they used for case study a node doing a Dos attack by continuously sending authentication requests, the authors specify that in a real system this gateways should be able to deal with various types of malicious activity.

This detection scheme is based in the principle that legitimate traffic has well defined characteristics, it has the debility that an attacker could use some "good" pattern to perform an attack, increasing the probability that the Detection Scheme does not properly identify the attack

3) Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids:

In this paper [7] a new architecture for a hierarchical and distributed intrusion detection system called the smart grid distributed intrusion detection system (SGDIDS) is presented. This distributed intrusion detection system (DIDS) is able to successfully analyze communications traffic using an analyzing module (AM) that leverages classification algorithms such as support vector machine (SVM) and artificial immune system (AIS) in order to determine if an attack is occurring, what type of attack it is, and where it comes from in the communication system.

The proposal presents an Smart Grid composed of various layers (HAN, NAN and WAN). Each of these layers has Intrusion Detection Systems (IDS) that can determine whether determinate activity is a valid activity or is an attack to the network. If an IDS from a layer cannot safely classify this activity it reports the event to the IDS of the upper layer and delivers the classification responsibility. The architecture is presented in the figure 6

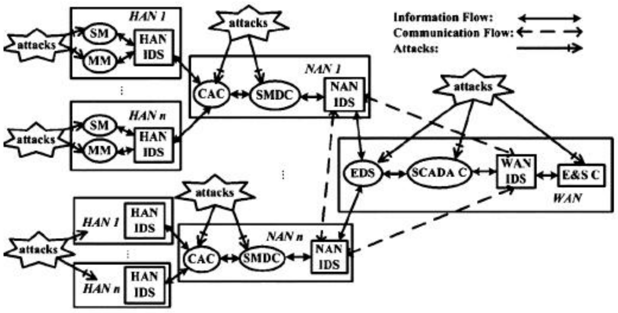


Figure 6. Three-layer network architecture.

In the figure, heach component from the layer has its respescitve IDS (HANIDS, NANIDS, WANIDS) and communicates with its respective upper layer.

The SGDIDS is able to classify attacks efficiently and effectively through the use of a robust classification algorithm, a support vector machine (SVM) and an artificial immune system (AIS) are used to accomplish this.

AIS are computational algorithms that emulate the mechanisms of human immune systems. They involve learning, memory, and optimizing capabilities for conforming supervised and nonsupervised computational algorithms. The primary advantages of AIS are that only positive examples are needed in the algorithms, and the patterns AIS has been trained with or learned can be explicitly examined. In the proposal, the clonal selection algorithm is considered because of its flexibility. Its theory is used for emulating the basic process of an adaptive immune response to the antigenic stimulus. Only those cells that can recognize the antigens are allowed to clone and proliferate.

Its theory is used for emulating the basic process of an adaptive immune response to the antigenic stimulus. Only those cells that can recognize the antigens are allowed to clone and proliferate.

The authors validated their proposal using Matlab to simulate a multi layered Smart Grid, and using NSL-KDD dataset

V. Conclusions

This paper presents a review of some of the actual proposals for malicious activity detection in Smart Grids, the functioning and characteristics are presented and analyzed.

In the current literature there is not yet a well defined Smart Grid architecture, in the sense that the protocols, topologies and architectures inside each of the Smart Grid layers is not defined. This lack of consensus affects the proposal's validity as the security requirements at each layer are not specifically defined.

The reviewed proposals have been simulated in controlled scenarios, defining test beds to test some of these proposals would help to validate them and improve them.

References

[1] ”Security analysis of Dutch smart metering systems” S. Keemink and B. Roos Available: http://staff.science.uva.nl/ delaat/ sne-2007-2008/p33/report.pdf. 2008

[2] ”Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges” Li, X. Lille, I. Lian, X. Lu, R. Shen, X. Lin, X. Zhu, H. IEEE Communications Magazine, August 2012

[3] “Security and privacy challenges in the smart grid” P. McDaniel and S. W. Smith, [Online]. Available: http://www.patrickmcdaniel.org/ pubs/sp-smartgrid09.pdf

[4] “Secure Service Provision in Smart Grid Communications” He, D. Chen, Ch. Bu, J. Chan, S. Zhang, Y. Guizani, M. IEEE Communications Magazine, August 2012

[5] “Cyber-Physical Security of A Smart Grid Infrastructure” Y. Mo et al, Proc. IEEE, vol. 100, no. 1, Jan. 2012, pp. 195–209.

[6] “An Early Warning System against Malicious Activities for Smart Grid Communications” IEEE Network, vol. 25, no. 5, 2011, pp. 50–55.

[7] “Distributed Intrusion Detection System in A Multi-Layer Network Architecture of Smart Grids” Y. Zhang et al. IEEE Trans. Smart Grid, vol. 2, no. 4, 2011, pp. 796–808.

[8] “A Light-Weight Message Authentication Scheme for Smart Grid Communications” M. Fouda et al. IEEE Trans. Smart Grid, vol. 2, no. 4, 2011, pp. 675–85.

[9] “Cyber Attack-resilient Control for Smart Grid” Sridhar, S. Hahn, A. Govindarasu. IEEE PES Innovative Smart Grid Technologies (ISGT), 2012

[10] “Zero-Configuration Identity-based Signcryption Scheme for Smart Grid” H. K.-H. So et al., Proc. IEEE Smart- GridComm, 2010, pp. 321–26.

[11] ”Securing Dynamic Distributed Storage Systems from Malicious Nodes” Pawar, S. Rouayheb, S. Ramchandran, IEEE International Symposium on K Information Theory Proceedings (ISIT), 2011