Applications of attack mitigation mechanisms in energy networks, attack detection and preventive methods for security in the smart grid

Dimitrios Simeonidis¹*

¹University of Economics – Varna, Department of Informatics, Varna, Bulgaria

Abstract. The Smart Grid promotes energy and environmental sustainability through the integration of vast distributed energy resources. The implementation of such a green system has huge economic and social benefits. The new generation of sensors, the smart one's meters and electronic devices are integral elements of the smart network. However, the upcoming development of smart devices in different levels and their integration into communication networks may cause cyber threats. Failure to address these problems will create difficulties in modernizing the existing electrical system. Another key concern is the protection of privacy associated with collecting and using energy consumption data. Keywords—Smart Grid, cybersecurity, attacks threats, attack mitigation, encryption, data security

1 Introduction

Owing to the Cyber-Physical System nature of Smart Grid (SG) and the large impact energy systems, the primary objective of safety for Operation SG's is availability. Denial-of-Service (DoS) attacks, which have a direct impact on availability of communication and control systems [1], are characterized as the main network security threats in SG. Detection and defense against DoS attacks are determined mainly by network security measures such as traffic, monitoring and filtering the network. Therefore, an effective network approaches against attacks DoS are provided.

It is the interaction of information networks and electricity in energy systems that makes it necessary for the SG be able to detect and neutralize DoS attacks which may be executed anywhere on the network's communications [2].

2 Attack detection for energy networks

Detecting an attack is the first step in ensuring countermeasures against it. Detection of existing DoS attacks can be categorized into several schemes, as follows:

* Corresponding author: simeonidis@ue-varna.bg
• Signal-based detection: on the physical plane or MAC plane, a detector the information strength of the received signal can be measured by a detector DoS attack. Received signal strength information (RSSI) to identify that a 87 attack has occurred (for instance wireless jamming): provided that the multi-packet RSSI exceeds the limit (which means that they must be received correctly by the receiver) but the package decoder shows errors, attack detector may spell danger to the presence of an aggressor.

• Package-based detection: solutions that fall into this category can be applied at each level to measure the transmission effect of each package and the discovery of possible attacks detecting a significant increase in failures of transmission packages. That is a general and effective scheme for detection given that DoS attacks can result in degradation of network performance in terms of loss or delay packages.

• Preventative method: its essence is to design algorithms which try to detect DoS attacks at an early stage by sending probing packages to test or measure the potential attackers’ situation.

• Hybrid method: a scheme that combines different ideas to improve the accuracy of attack detection may also be designed. For instance, the combining of packet-based and signal-based detection for the effective detection of jamming attacks on wireless networks.

Most methods of detecting DoS attacks belong to passive detection which monitors the status of the network, such as traffic load) and packet transmission ratio, and signals a warning against an attack when there is an apparent lack of compatibility between new specimens and historical data [3]. Thus, the available methodology for detecting DoS attacks can be applied directly to communications networks in SG. For instance, probes based on signals can be easily used in SG wireless applications and packet-based detection methods are appropriate for detecting DoS attacks on Advanced Metering Infrastructure (AMI) networks and substations [4]. Preventive methods may be limited to non-time critical networks because inevitably add extra burden to communication (overhead) with packet transmission crawler.

3 Applications of attack mitigation mechanisms in energy networks

Along with detection schemes for DoS attacks, there may be implemented attack mitigation mechanisms to protect network nodes from such attacks. DoS schemes of attack mitigation include the following approaches: first, moderating DoS network layer attacks so that target resources are depleted and second, mitigation of physical engagement attacks physical layer to disrupt wireless communications.

3.1 Network level mitigation

The most common approaches to mitigating attacks DoS are developed for the network level and most of them have proven effective for the Internet [5], e.g. the mechanisms as follows:

• Rate-limiting: the core idea of rate-limiting mechanisms is to impose a percentage limit on a set of packages identified as possibly maliciously from the detection mechanism. It is usually applied when the mechanism detection has false positives (false positives) or cannot it just characterize the attack’s flow.

• Email Filtering: with the help of attack detection methods, the filtering mechanisms can distinguish between the source of packet addresses and the blacklist provided by attack detectors to filter all suspect flows in this way further forwarding or routing packages to the victims.
• Reconfiguration: to mitigate or effect DoS attacks, a possible solution is the reconfiguration of the network architecture, like altering the topology of the victim or network intermediary by adding more sources to the victim or by isolating attack devices.

3.2 Physical level mitigation

Because wire networks are used in local systems in SG, the wireless jamming becomes the main DoS attack on wireless energy networks, especially in some scenarios involving distribution and transmission systems (fig. 1). Thus, wireless communication that is resistant to jamming attacks, is very important for SG applications to deal with these attacks and maintain continued transmission of information [6]. There has been significant progress in the development of wireless network shapes which are resistant to jamming attacks. Schemes like these may be designed either coordinated or uncoordinated.

Coordinated protocols are conventional against jamming attacks transmission schemes already explored in the field of wireless communications [7]. They can be categorized as Dispersion by direct sequence spectrum (DSSS), Frequency switching spectrum dispersion (FHSS) and Dispersion frequency slip spectrum (CSS). However, the issue related to the coordinated protocols is that the secret, such as the direct sequence in DSSS and the switching pattern in CSS, is considered confidential to others (for instance, of attackers). This assumption does not apply to standards open communication, such as WiFi and cellular networks [8]. Therefore, coordinated protocols are vulnerable to deliberate attacks with knowledge of their information protocol.

Fig.1. Essential Smart Grid components [9].

Uncoordinated protocols have potential for securing wireless communication in distributed environments. Uncoordinated protocols need the transmitter and receiver to share an advanced known secret between them [10, 11, 12]. They accidentally create a secret (for example, the pattern switch to FHSS) for each transmission and avert attacks from the acquisition of adequate knowledge to disrupt communication. The standard FHSS and DSSS, have indeterminate equivalents of UFHSS and UDSSS respectively.

4 Encryption for Data Security

Encryption mechanisms are intended to safeguard the confidentiality, integrity, and non-disclaimer of data. Encryption may be symmetric or asymmetric. The most common algorithms in symmetric encryption are the standard encryption data (DES) and advanced
standard encryption (AES) [13]. On the other hand, two keys for data encryption are used in asymmetric encryption: a private key and a public key (public key). RAS (Rivest-Shamir-Adleman) is an asymmetric crypto algorithm key. In SG, different elements with their own computing potential coexist. It may be concluded that both the symmetric and the asymmetric key encryption, and their choice depend on various factors among which are data criticality, time limitations [14] and computational resources.

Authentication is defined as the action of verifying the validity of the identity of an object, e.g., using a password. It may be a user, a smart device, or any connected item in the network of SG. Multicast authentication is a special authenticity type, and its applications are used extensively in SG. There are three methods of achieving authentication for multi-emitting applications [15]: secret information asymmetry, time asymmetry and hybrid asymmetry.

Key management is a critical approach to encryption and authenticity [16]. Managing public keys or managing shared secrets keys can be used to ensure authenticity for communication between networks. In the public key infrastructure (PKI), the identities of the two entities are stored by a certificate issued by a third party, an entity called the Certification Authority (CA). The mechanism is done prior to establishing connection between the two entities. In managing a common secret key, four steps are employed to maintain communication security: key creation, key distribution, key storage, and key update. Because of the distributed nature of SG, some specific requirements for management planning should be considered cryptographic key. Basic but important requirements of the management scheme key are efficiency, growth capacity, scalability, and safe management. Furthermore, several key management frameworks have been proposed especially for electricity systems, such as: unique key (single key), installing a key for SCADA systems (SKE), architecture key management for SCADA systems (SKMA), Advanced Architecture key management (ASKMA) ASKMA+ and tiered management method cryptographic key (SMOCK). The selection of a frame is determined by different criteria, including scalability, computing capacity resources and multipurpose support. Research has been conducted to compare among the abovementioned key management schemes. It was based on scalability, multi-emission support, resilience to key violation and application to electricity systems. ASKMA+ and SMOCK presented interesting outcomes. ASKMA+ is an effective key management scheme supporting multi-emission, yet it suffers from scalability. SMOCK, on the other hand, presents good scalability, but it has got some weaknesses amongst which are nonsupport multi-emission and low computational efficiency.

5 Conclusion

Both coordinated and uncoordinated protocols may be used in SG to attain durable wireless communications against jamming attacks. In contrast with coordinated protocols, uncoordinated ones are safer and more resistant to deliberate attacks. They share an advanced known secret between transmitter and receiver. On the other hand, the cost of uncoordinated protocols is delayed execution because one needs to negotiate a secret before starting data communication. These schemes and other existing schemes such as DEEJAM and Timing-channel (TC), may easily be used in AMI wireless networks and home networks where the communication movement is chronically critical. However, it is still unclear if they may be utilized effectively in distribution and transmission systems, where performing the communication at the millisecond level is necessary.

Although great progress is being made to ensure the present and future implementation of the smart grid, there are still many challenges that they need to be addressed Security and privacy.
They are essentially based on promoting the use of best security practices information in the implementation and development of new smart initiatives networks. Cooperation in industry and state support are essential to establish entities for the management, coordination, and dissemination of information about security incidents, vulnerabilities, problems and solutions and privacy in the smart grid.

Particular attention should be paid to consumer privacy and the establishment of entities to protect consumer privacy rights.

References


