Information security threats and an easy-to-implement attack detection framework for wireless sensor network-based smart grid applications

G Tuna¹, H Örenbaş², R Daş³, D Kogias⁴, M Baykara³ and K Gülez²
¹ Department of Computer Programming, Trakya University, Edirne, Turkey
² Department of Control and Automation Engineering, Yildiz Technical University, Istanbul, Turkey
³ Department of Software Engineering, Firat University, Elazig, Turkey
⁴ Department of Electronics Engineering, Piraeus University of Applied Sciences, Aigaleo, Greece

E-mail: gurkantuna@trakya.edu.tr, orenbas@yildiz.edu.tr, rdas@firat.edu.tr, dimikog@teipir.gr, mbaykara@firat.edu.tr, gulez@yildiz.edu.tr

Abstract. Wireless Sensor Networks (WSNs) when combined with various energy harvesting solutions managing to prolong the overall lifetime of the system and enhanced capabilities of the communication protocols used by modern sensor nodes are efficiently used in Smart Grid (SG), an evolutionary system for the modernization of existing power grids. However, wireless communication technology brings various types of security threats. In this study, firstly the use of WSNs for SG applications is presented. Second, the security related issues and challenges as well as the security threats are presented. In addition, proposed security mechanisms for WSN-based SG applications are discussed. Finally, an easy-to-implement and simple attack detection framework to prevent attacks directed to sink and gateway nodes with web interfaces is proposed and its efficiency is proved using a case study.

1. Introduction
With the addition of renewable energy solutions, existing power grids manage to partially serve the globally increasing demand for electricity, but still have to deal with problems such as equipment failures, blackouts, poor communication and lack of effective monitoring of the infrastructure. Those challenges, along with production instabilities caused by structural or operational characteristics, can easily lead to huge economic losses, inefficient electricity usage, customer dissatisfaction and pollution from a huge amount of CO₂ emissions. Taking, also, under consideration the costly maintenance of the aged existing infrastructures along with the rising costs for building new ones and the declining number of skilled personnel, the need for more dynamic and efficient operation of the system has risen. Real-time monitoring of the various grid components, surveillance and management of distribution and transmission systems become more and more important. In this respect, the grid's efficiency can be improved by the use of various sensors. This approach allows collecting real-time data from various devices in a power grid and spreading it along the infrastructure. In this way, any problems in the system's functionality can be diagnosed proactively and timely generated remedial
actions can be taken in order to prevent any unpleasant dysfunctionalities that might affect the grid's performance. They will, also, reduce person hours to locate and deal with system faults and, consequently, significantly reduce loss of revenue. The sensors can be installed on critical power grid equipment and can be used to monitor many components essential to the grid, such as voltage, current, temperature, system frequency and power quality disturbances [1-4]. This way a next-generation electric power system is created, the Smart Grid (SG) [2, 3].

Recently Wireless Sensor Networks (WSNs) have been widely recognized as a technology promising to enhance various aspects of SGs, especially those that deal with power generation, bidirectional delivery, utilization and seamless monitoring, providing an energy efficient, reliable and low-cost solution for control management [1,5,6]. WSN applications for smart grids, both existing and future ones, range from advanced metering, demand response and dynamic pricing, equipment fault diagnostics, fraud detection, load control, power automation and remote power system monitoring and control. SG is also considered as a data communications network; therefore the communication capabilities among the elements of the electrical power system will play a huge role on the efficient performance of any WSN-based SG application. But the selection for the right communication technology varies, depending on environmental conditions and cost and is usually the result of careful analysis.

Data collection is an essential operation for WSN-based SG applications. However, WSNs are challenged by various constraints such as limited computation and memory resources, limited power supply resource and vulnerability to failures and therefore addressing these challenges plays a key role in improving the efficiency, reliability and robustness of WSN-based SG applications. For this purpose, effective data collection methods [7, 8] to save energy and speed up the data collection process have been investigated in recent years. On the other hand, improving the data collection process alone is not enough for the success of SG applications, as wireless communication technology incurs various types of security threats. In this paper, an easy-to-implement attack detection framework is proposed to address common information security risks and prevent attacks directed to sink and gateway nodes with web interfaces, and its efficiency is proved using a case study. The rest of the paper is organized as follows. The use of wireless sensor networks for data collection in SG environment is explained in Section 2. Section 3 reviews security threats, challenges and proposed security mechanisms, and explains the proposed framework to address security threats in WSN-based SG applications. Finally, the paper is concluded in Section 4.

2. Wireless sensor network-based smart grid applications

In recent years, surveillance and management of transmission and distribution systems as well as real-time monitoring of the various grid components has become more and more important. In this respect, the grid’s efficiency can be improved by the use of various sensors. This approach allows collecting real-time data from various devices in a power grid and communicating it along the infrastructure. In this way, a problem in the grid can be diagnosed proactively and timely generated remedial actions can be taken in order to prevent any unpleasant dysfunctionalities that might affect the grid’s performance. It also helps to reduce man hours to locate and deal with system faults and, consequently, significantly reduce loss of revenue. The sensors can be installed on the critical power grid equipment and can be used to monitor essential grid components such as voltage, current, temperature, system frequency and power quality disturbances [1-4]. This way a next-generation electric power system is created, the Smart Grid (SG).

A SG is a modernized power transmission and distribution (T&D) network which uses robust two-way data communications, distributed computing technologies and smart sensors to improve reliability, safety and efficiency of power delivery and use [2-4]. Using a sophisticated information processing and communication technology infrastructure, SG will be able to fully use and benefit from its distributed power generation system, while maximizing the whole system's energy efficiency [2, 3]. Consequently, SG is also considered as a data communication network which, by supporting many power management devices, achieves seamless and flexible inter-operation abilities among different
advanced system components that leads to efficient performance. The power system infrastructure is comprised of all the devices found on existing electrical grids, as was described above, with the additions of smart meters and sensors spread throughout the grid to detect outages and measure critical performance metrics that should be forwarded to, the buck-haul system's detection and decision data centres [2, 4]. It generally includes the power generation, T&D system and the customer premises.

In a SG, there basically are two types of information flow [11]. The first flow is from sensors and electrical appliances to smart meters and the second information flow between the smart meters and the data centres of the utility. The first information flow can be accomplished with the use of power-line communication (PLC) [10, 12] or by using wireless communications technologies, such as 6LowPAN, ZigBee, and others [5]. The second information flow can be accomplished by using the internet (public network) or cellular communications. Generally, the expected characteristics of the selected technology would be its simplicity, robustness, mobility and the capability to improve the network's performance, to balance the network's load, to extend the network coverage range and to increase the data transfer capacity and security.

Due to the various components included in the power system infrastructure, SG transformation requires the handling of both the flow from sensors and electrical appliances to smart meters and the flow between the smart meters and the data centres [2]. Generally, the expected characteristics of the selected communication technology for the SG transformation would be its simplicity, robustness, mobility, the capability to improve the network's performance, to balance the network's load, to extend the network coverage range, to increase the data transfer capacity and security, etc. [2, 10]. The choice for the selected technology highly depends on the environmental conditions in the area and should be the result of careful cost versus benefit analysis because not all solutions combine the characteristics mentioned above, so there is no solution that can be considered as a default.

The evolution in WSN, especially on the problems related to energy exhaust, energy harvesting, mobility, and communication, has open new perspectives for their usage in a SG environment. Various, diverse range power grid applications from home area networks (HANs) to power T&D monitoring have been developed and used [12-14], allowing for robust and energy-efficient monitoring and control in a SG [4]. Although SG transformation brings many benefits to electric utilities, SG deployments create much more data compared to traditional power grid deployments and require the handling of new types of information [15]. In this regard, WSNs play a key role in data collection operation in SGs and enhance the ability of SG operators by creating new opportunities such as improving service reliability and delivering useful information.

3. Proposed attack detection framework and a case study
A WSN is a wireless network consisting of scattered tiny sensor nodes with limited computational capabilities and battery power. It is typically used to monitor physical or environmental conditions. There is no doubt that WSNs bring many advantages to industrial, scientific and military applications due to the sensing technology combined with processing power and wireless communication capability. On the other hand, in most applications, WSNs process sensitive data and face information security threats such as data fraud, data manipulation, and sensor destruction or replacement. This concerns critical monitoring and control applications, and becomes severe in large-scale WSN deployments in which security risks increase highly due to limited physical protection of the sensor nodes and openness of the wireless communication channel [16].

The existing security solutions proposed for traditional wireless networks cannot be used for WSNs due to the constraints inherent to the WSN infrastructure. In WSNs, all the data collected by the inner layer sensor nodes are forwarded to the sink node which is a resource-rich node. The sink is responsible for collecting the sensed data from the sensor nodes and sending it to the operation centre via the Internet or other communication architectures. Therefore, the placement of the sink node has a great impact on the energy consumption and network lifetime [17] and the sink must be protected from unauthorized access since it acts as a gateway to the external world [18]. One of the newest design trends in WSNs is Web Services approach in which sensor nodes are service providers and
applications are clients of such services [19]. This approach enables a flexible architecture where sensed data can be accessed by users spread all over the world. Therefore, especially, the sink nodes with also acts as a web service provides must be protected against potential security threats.

WSNs are vulnerable to many attack types including passive information gathering, traffic analysis, message corruption, capture of a sensor node, addition of malicious sensor nodes, node malfunction, node outage, and sophisticated attacks such as selective forwarding, wormhole attacks, hello floods, Sybil attacks, and spoofed, altered or relayed routing information [20, 21]. Sink nodes providing web services are vulnerable to other common attack types such as Denial of Service (DoS) and Distributed Denial of Service (DDoS). In this section, we present an easy-to-implement attack detection framework for the sink nodes in WSN-based SG applications.

A DoS is a type of attack on a network which is designed to make a server or a network resource unavailable to users by flooding it with useless traffic. Its main goal is to temporarily interrupt or suspend the services of a host connected to the Internet. On the other hand, a distributed DoS (DDoS) is a malicious attempt where multiple compromised systems are used to target a single system causing a DoS attack. Resources targeted in DoS attacks can be an entire network, a specific host, a port or service on the targeted system, or one or more components of a given network. DDoS has started to become the preferred method of attack due to its simplicity, potential for major disruption, and ease of distribution. Different from attacks relying on the security vulnerability of operating systems, DDoS attacks are relatively low-tech and easy-to-stage.

Since DDoS are one of the most common attack types, they must be prevented to ensure system availability. In this study, to address the potential security threats of DDoS attacks, a security framework is proposed. The proposed framework’s flowchart is shown in Figure 1 and its pseudo code is listed below. To prove the framework’s effectiveness and usability, a simulation study was carried out using Visual Studio 2012, Microsoft SQL Server 2014 and LOIC [22], a network stress testing tool. Figure 2 shows the database and tables used by the proposed security framework. After the developed framework run, the system on which the proposed framework was running was tested with LOIC. As shown in Figure 3, when the proposed security framework detected a DoS attack, it stopped the attack by blocking the host’s IP address, from which the DoS attack was sourcing.

Pseudo code of the proposed framework

```
Begin
Get source host’s IP address
Get total number of records of this IP address (Record_Num) in BlockedIP table
If Record_Num > 0
    Get system time and the previous request’s minute field (Time_Difference)
    If Time_Difference<60
        Open “Access Blocked” Page
    If Time_Difference>60
        Clear information belonging to the source IP address
If the source IP address already exists (IPExists_Num)
    If IPExists_Num=0
        Store IP information
    If IPExists_Num>0
        Begin
            Request_Number++
            Save access information
        End
Calculate and save the difference between the last and first requests of the source host (Time_Difference)
Calculate and save the total number of requests in the calculated time difference (Request_Num)
If Time_Difference>10 and Request_Num>100
```
Store the source IP address in BlockedIP table
Notify system administrator via e-mail
End

**Figure 1.** Flowchart of the proposed framework.
4. Conclusion

Wireless Sensor Networks (WSNs) are commonly used in various monitoring and control applications as well as many other applications. In recent years, WSNs have been commonly implemented in Smart Grid (SG) environment and served for different SG applications. Although many techniques have been proposed to enhance routing, clustering, lifetime and data handling issues of WSNs, security issue somehow has been neglected. However, this may lead to many critical problems in WSN-based SG applications. To address this need, in this study, a practical and easy-to-implement attack detection framework was proposed and its efficiency was proved using a case study. The proposed framework is suitable for all-IP based WSNs.
References

[1] Gungor, VC, Bin, L and Hancke, GP 2010 Opportunities and challenges of wireless sensor networks in smart grid IEEE Trans. Industrial Electronics 57(10) 3557-64

[2] Gungor, VC, Sahin, D, Kocak, T, Ergüt, S, Buccella, C, Cecati C and Hancke, GP 2011 Smart Grid Technologies: Communication Technologies and Standards IEEE Transactions on Industrial Informatics 7(4) 529-539

[3] Sood, VK, Fischer, D, Eklund, JM and Brown, T 2009 Developing a communication infrastructure for the smart grid Proc. IEEE Electrical Power and Energy Conference (EPEC 2009) pp 1-7

[4] Tuna, G, Gungor, VC and Gulez, K 2013 Wireless Sensor Networks for Smart Grid Applications: A Case Study on Link Reliability and Node Lifetime Evaluations in Power Distribution Systems International Journal of Distributed Sensor Networks 2013 Article ID 796248

[5] Yang Y, Lambert F and Divan D 2007 A survey on technologies for implementing sensor networks for power delivery systems IEEE Power Engineering Society General Meeting pp. 1-8

[6] Ullo S, Vaccaro A and Velotto G 2010 The role of pervasive and cooperative Sensor Networks in Smart Grids communication IEEE Mediterranean Electrotechnical Conference (MELECON 2010) pp. 443-447

[7] Francesco MD, Das SK and Anastasi G 2011 Data Collection in Wireless Sensor Networks with Mobile Elements: A Survey ACM Trans. Sen. Netw. 8(1)

[8] Durmaz Incel O, Ghosh A, Krishnamachari, B and Chintalapudi K 2012 Fast Data Collection in Tree-Based Wireless Sensor Networks IEEE Transactions on Mobile Computing 1 86-99

[9] Wang Y, Zhang J and Xu HS 2012 The Design of Data Collection Methods in Wireless Sensor Networks Based on Formal Concept Analysis Advances in Intelligent and Soft Computing 169 33-38

[10] Yigit M, Gungor VC, Tuna G, Rangoussi M and Fadel E 2014 Power Line Communication Technologies for Smart Grid Applications: a review of advances and challenges Computer Networks 70 366-383

[11] Moghe R, Yi Y, Lambert F and Divan D 2009 A scoping study of electric and magnetic field energy harvesting for wireless sensor networks in power system applications Proc. of IEEE Energy Conversion Congress and Exposition (ECCE 2009) pp. 3550-3557

[12] Amin M and Wollenberg BF 2005 Toward a Smart Grid Power and Energy Mag. 3(5) 34-41

[13] Erol-Kantarci M and Mouftah HT 2011 Wireless Multimedia Sensor and Actor Networks for the Next-Generation Power Grid Ad Hoc Networks 9(4) 542-551

[14] Leon RA, Vittal V and Manimaran G 2007 Application of Sensor Network for Secure Electric Energy Infrastructure IEEE Trans. Power Delivery 22(2) 1021-28

[15] Kayastha N, Niyato D, Hossain E and Han Z 2014 Smart grid sensor data collection, communication, and networking: a tutorial Wireless Communications and Mobile Computing 14(11) 1055-87

[16] Pathan A K, Lee H -W, and Hong C S 2006 Security in wireless sensor networks: issues and challenges The 8th International Conference on Advanced Communication Technology 2 pp. 1043-1048

[17] Zhou Y, Fang Y and Zhang Y 2008 Securing Wireless Sensor Networks: A Survey IEEE Communications Surveys & Tutorials 10(3) 6-28

[18] Shahabuddin M, Furqan Z and Guha R 2005 Wireless sensor network security: a secure sink node architecture 24th IEEE International Performance, Computing, and Communications Conference pp. 371-376

[19] Delicato F C, Pires P F, Pirmez L and Carmo L F R C 2003 A Flexible Web Service Based Architecture for Wireless Sensor Networks The 23rd International Conference on Distributed Computing Systems p. 730

[20] Undercoffer J, Avancha S, Joshi A and Pinkston J 2002 Security for sensor networks CADIP Research Symposium
[21] Karlof C and Wagner D 2003 Secure routing in wireless sensor networks: Attacks and Countermeasures *Ad Hoc Networks* **1**(2-3) 293-315
[22] http://sourceforge.net/projects/loic