FPGA BASED SYSTEM FOR DENIAL OF SERVICE DETECTION IN SMART GRID

A. Jayanth Balaji and D. S. Harish Ram
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham University, Coimbatore, India
E-Mail: ds_harishram@cb.amrita.edu

ABSTRACT

The availability of cheap computing power and instrumentation electronics accompanied by the communication revolution has engendered a complete paradigm shift in the design and implementation of electrical grids. Power grids are envisaged to be transformed into "Smart Grids" incorporating a high degree of intelligence with a view to enhance the reliability and efficiency of generation, transmission and distribution systems. Real-time monitoring of grid parameters enables more effective management of power generation. Prevention of theft by means of smart metering is another major advantage. However, the large scale use of embedded systems, computing resources and communication networks makes the grid vulnerable to cyber attacks. These vulnerabilities can result in consequences ranging from diminished quality of service to catastrophic events such as line trips, extended blackouts and downright damage or destruction of assets. This paper gives a review of the current state-of-the art in cyber security for the smart grid environment. An FPGA based engine for detection of denial-of-service attacks in packets in an Ethernet link is also proposed.

Keywords: smart grid, cyber security, FPGA design, denial of service.

1. INTRODUCTION

The Smart Grid paradigm envisages a complete integration of all the entities involved in the generation, transmission and distribution of power with the ultimate objective of improving reliability and efficiency in delivery and utilization of electrical energy. Unlike in legacy power systems, the smart grid implements a two-way communications model which acts as an enabler for novel services such as smart metering and demand response systems [1]. Smart Grids also facilitate the two-way flow of energy. Smart metering systems provide real-time information to the utility which paves the way for introducing demand based tariff structures and better management of the network.

The upgrading of legacy power systems to a smart grid environment has become a global imperative due to some of the pressing issues that besiege the energy scenario. Some of the major challenges that drive development initiatives towards the smart grid are the ever increasing energy demands, need to curtail global CO_2 emissions and the increasing intermittent renewable energy capacity [2]. Higher availability of energy from solar and wind based power plants have placed higher demands on the grids to absorb intermittent renewable energy [2]. Moreover, generation is getting increasingly distributed with the availability of larger captive generation capacity based on fossil as well as non-fossil sources. These concerns are reflected in the core objectives of the European Union's energy policy namely, sustainability, competitiveness and security of supply [3]. The smart grid is expected to be able to effectively address these challenges. This would necessitate large scale adoption of Information and Communication Technologies (ICT) and their integration into the power grid.

The tangible benefits that would accrue as a result of adopting smart grid approaches are innumerable. They include more efficient power management, emergence of "microgrids" and real time pricing for consumers to name a few. On the transmission and distribution front, a combination of IT and distributed intelligence can ensure better safety and stability to the entire grid [2].

The presence of extensive communications infrastructure exposes the smart grid to cyber security vulnerabilities. The presence of these vulnerabilities can jeopardize one or more of the three factors that are indispensible for reliable power systems operation namely availability, confidentiality and integrity [1] [4]. This imposes more stringent requirement on cyber security measures in the grid compared to the Internet [1]

In this paper the current state of the art in smart grid security is surveyed. We also propose an FPGA based engine for detection of Denial of Service (DoS) attacks. The rest of the paper is organized as follows. Section II presents a review of the literature pertaining to smart grid security. Some of the key vulnerabilities that need to be addressed by cyber security systems catering to the smart grid are outlined in this section. Section III describes the details of the proposed system for detection of DoS attacks. Section IV presents the results of the DoS implementation and Section V concludes the paper.

2. REVIEW OF RELATED WORKS

The different entities comprising a typical smart grid and the communications and power flow between them is depicted in Fig. 1. This model described in [4] envisages a vast network comprising utilities and customers who are linked by the power transmission as well as communication infrastructure. The other entities in the network are involved in providing value added services for improving efficiency and facilitation of buying and selling of power driven by supply demand dynamics

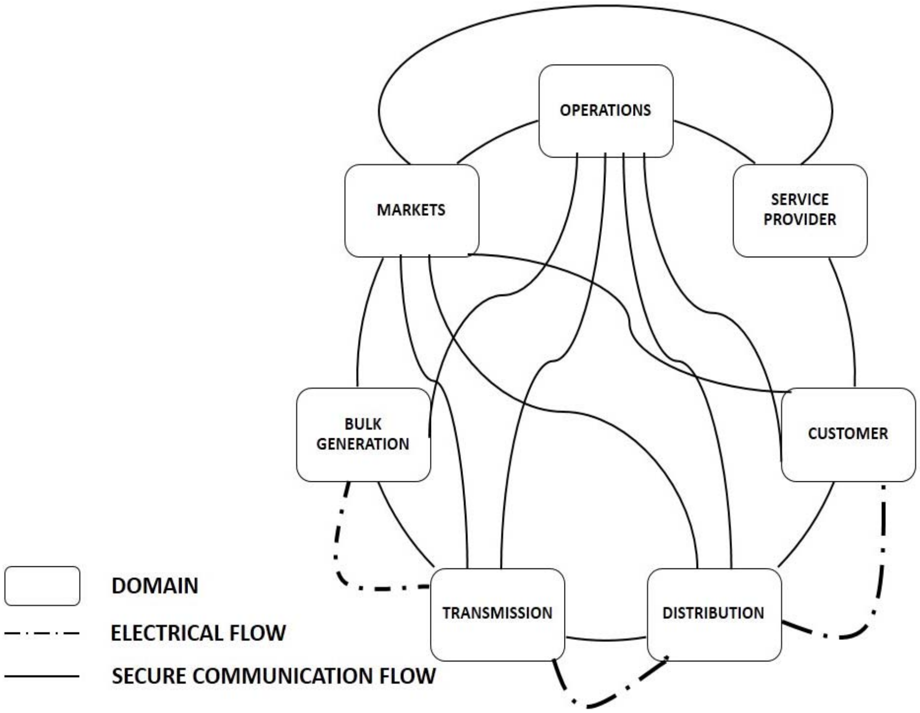

Figure-1. Block diagram of Smart Grid communication and power flow.

In [1] the different aspects of network security in the Smart Grid scenario are examined in detail. The paper provides taxonomy of potential network security threats and their countermeasures. The countermeasures suggested are mainly at the *network*, *cryptographic* and *protocol* levels. The paper discusses the enhancement of commonly used communication protocols such as DNP3 and IEC 61850. The emergence of the smart grid in Europe and the consequent threats and vulnerabilities are examined in [3]. The paper gives a roadmap to the European Union for making the European Smart Grids secure. The US National Institute of Standards and Technology (NIST) have laid down a detailed set of guidelines for smart grid security which are documented in the NISTIR 7628 standard [4].

Denial of Service (DoS) attacks has been widely studied and mitigation measures have been proposed in the literature. In [5], denial of service caused by SYN flood and Buffer overflow are analyzed. The authors propose a data mining based approach for intrusion detection. A probabilistic approach for providing advance information on DoS activity is reported in [6]. The technique is also capable of warning potentially harmful events in the grid such as surges in the line voltage. Time to Live (TTL) information is used as a means to identify DoS in [7]. The work also proposes marking system and MAC based attack identification and mitigation measures.

The communication infrastructure in a smart grid comprises among others, a large number of packet based networks based on standards such as the Ethernet. These networks have replaced SONET/SDH based system traditionally employed in SCADA systems which were less vulnerable to intrusion attempts [8]. Network intrusion in general has been well researched and a host of signature based detection schemes have been proposed in the literature such as [9] and [10]. FPGA based schemes such as the one suggested by [10] are ideal for network backbones where data rates are of the order of tens to hundreds of gigabytes necessitating high throughput.

A Kalman filter framework is reported in [11] for prevention of injection of false data as well as DoS. The authors describe both χ^2 estimation and Euclidean distance based approaches for detecting the attacks from the estimator data.

Replay attacks in plant control systems have been extensively reported and studied. Smart grids are also vulnerable to these attacks given their heavy dependence on real time data. In a replay attack, genuine grid data from an earlier instance is injected into the system thereby evading detection and crippling the entire control system. In [12] a scheme is proposed to handle replay attacks. The proposed technique seeks to achieve improved robustness at the expense of control system performance.

Network security countermeasures are not adequate for ensuring data integrity and confidentiality [1]. This can be accomplished by means of a combination of countermeasures involving encryption, authentication and key management. Low cost embedded hardware such as smart meters have limited computing power and therefore incorporating data security measures is a major challenge [1]. A homomorphic encryption scheme for aggregated metering data is proposed in [13]. The technique involves developing an aggregation tree and on the fly encryption of data from each node. Data security by concealment of metering data source information is addressed in [14]. The data source is periodically subjected to concealment (once in a few minutes). However the basic assumption is that the source information is not required. The approach may be used for data analysis by a utility where the location rather than the specific identity of a consumer is of relevance.

The cloud computing paradigm is increasingly getting adopted as a powerful and efficient means for distributed computing and storage. Smart grids are also likely to integrate cloud computing in their overall computing framework. A scheme for power monitoring in a local area system based on the cloud is proposed in [15]. However, security is not addressed in the work.

Though DoS attacks have been studied and several mitigation approaches have been suggested, FPGA based solutions have not been reported in the literature. FPGAs offer the advantage of high throughput over software based systems. Another added attraction is their reconfigurability which is especially attractive from a network security perspective since the system can be easily reconfigured to adapt to any new threat. We propose an FPGA engine for detection of DoS attacks which employs source IP validation and the time to live (TTL) information in an Ethernet environment.

3. HARDWARE DESIGN OF PROPOSED SYSTEM

The proposed system seeks to protect consumer metering data from DoS attacks on the Ethernet link. The packet structure is shown in Figure-2.

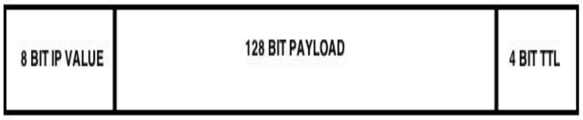

Figure-2. Frame structure of packet.

The 8-bit IP field holds the source address of the packet. The 128-bit payload contains the power consumption information of the node. The 4-bit TTL field has the time to live information of the packet. A potential intruder can spoof the network with a packet having a large TTL value thereby flooding the network. It is assumed that the proposed design will reside on the server side of the communication network. The *pkt_rdy* signal indicates the arrival of a packet. Than is customary. The *bsy* bit is de-asserted to indicate that the unit is ready to receive a packet. The controller state machine routes the packet bits to the appropriate sub-module responsible for checking the different fields of the received packet as shown in Fig. 3. The IP field of the received packet is routed to the IP validator which has a golden list of valid IPs. If the received IP value does not match with any of the entries in the golden list, then the LSB of the rslt [2:0] output is asserted indicating an invalid IP field.

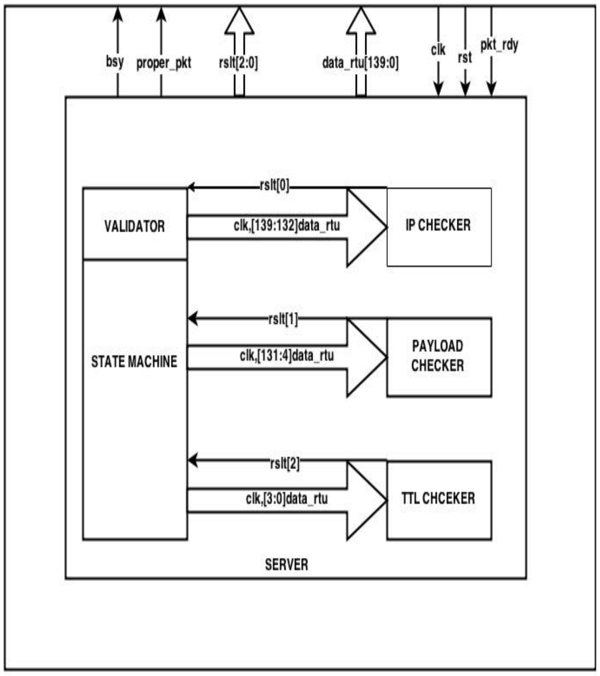

Figure-3. Block diagram of proposed system.

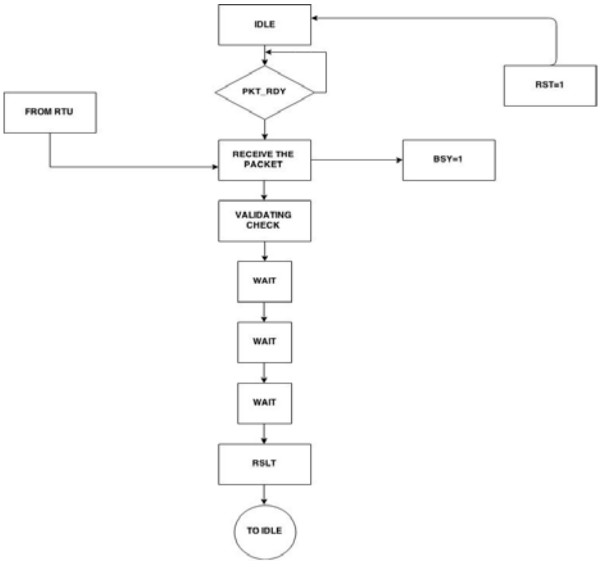

Figure-4. Controller state machine

The payload checker and TTL checker also functions in a similar fashion. The received payload is compared against the expected payload from a given source. The expected payload may be characterized by either a range of values or a single value depending on the source from which the packet is received. An invalid payload field for a given source will be signaled by asserting the first bit in the output port rslt [2:0]. Likewise, the port number 2 of the output rslt [2:0] is asserted on detection of an invalid TTL field.

The controller state machine (Figure-4) initiates the packet reception on sensing the pkt_rdy line which indicates the readiness of a node to transmit packets. On reception of a packet, the bsy signal is asserted indicating that the server cannot receive any packets. The controller goes to the VALIDATE state and further waits for three clocks before completion of the packet processing sequence.

4. RESULTS

The design was modeled in Verilog HDL and synthesized to the Zynq 7000 target FPGA using the Xilinx ISE environment. The results are presented in Table-1.

Table-1. FPGA synthesis results.

Area	21 LUT's
Delay	11.504 ns
power	65 uW

5. CONCLUSIONS

An overview of the state of the art in Smart Grid security is presented. The paper also proposes an FPGA engine for denial of service detection. The engine works on matching the different fields in the packet with expected golden data. The design is synthesized to an FPGA target and the power, area and delay reports are analyzed. Future work will include further evaluation of the design on real time network traffic and integration with a micro grid system. Augmenting the system by adding capability of detecting more known attacks will also be explored. The proposed system can be made part of a complete Smart Grid security solution.

REFERENCES

[1] G. Wang, Wenye, and Zhuo Lu. "Cyber security in the Smart Grid: Survey and challenges," Computer Networks. vol. 57, pp. 1344-1371, January 2013.

[2] Y. Aillerie, S. Kayal, J. Mennella, R. Samani, S. Sauty and L. Schmitt, "Smart Grid Cyber Security: Smart Grid Development Requires A New End To End Security Approach," Intel White Paper, 2013.

[3] Pearson, Ivan LG. "Smart grid cyber security for Europe," Energy Policy. vol. 39, pp. 5211-5218, June 2011.

[4] National Institute of Standards and Technology, "NISTIR 7628 Guidelines for Smart Grid Cyber Security," 2010.

[5] K. Choi, X. Chen, S. Li, M.Kim, K. Chae and J. Na, "Intrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid," Energies vol. 5, pp.4091-4109, October 2012.

[6] Z. M. Fadlullah, M.M. Fouda, N. Kato, X. Shen, and and Y. Nozaki, "An early warning system against malicious activities for smart grid communications. Network, "IEEE Network. vol. 5, pp. 50-55, 2011.

[7] B. Karthikeyan, "Detecting and Isolating Distributed Denial of Service Attack in Smart Grid Systems", Thesis, May 2014.

[8] RAD Data Communications, "Cyber Security for Power Utilities: A Defense Primer for the Operational Network", White Paper, December 2013.

[9] Pungila, Ciprian. "Hybrid Compression of the Aho-Corasick Automaton for Static Analysis in Intrusion Detection Systems." International Joint Conference CISIS'12-ICEUTE´ 12-SOCO´ 12 Special Sessions. Springer Berlin Heidelberg, 2013.

[10] S. Pontarelli, G. Bianchi, and S. Teofili, "Traffic-Aware Design of a High-Speed FPGA Network Intrusion Detection System," Computers, IEEE Transactions on vol. 62, no.11, pp. 2322-2334, November 2013.

[11] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Combating False Data Injection Attacks in Smart Grid Using Kalman Filter," Proceedings of IEEE Computing, Networking and Communications (ICNC) International Conference on. pp. 16-20, February 2014.

[12] F. Miao, P. Miroslav and G. J. Pappas, "Stochastic game approach for replay attack detection," Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on. pp. 1854-1859, 2013.

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

[14] Efthymiou, Costas, and Georgios Kalogridis. "Smart grid privacy via anonymization of smart metering data." Smart Grid Communications (Smart Grid Comm), 2010 First IEEE International Conference on. IEEE, 2010.

[15] R. Takano, H. Nakada, T. Shimizu, and T. Kudoh, "A Scalable and Distributed Electrical Power Monitoring System Utilizing Cloud Computing," Ubiquitous Information Technologies and Applications. pp. 809-817. Springer Berlin Heidelberg, 2014.