2017 IEEE 37th International Conference on Distributed Computing Systems Workshops

A Security Framework for SDN-enabled Smart Power Grids

Uttam Ghosh*, Pushpita Chatterjee†, Sachin Shetty‡
*Tennessee State University, Nashville, TN, USA
†SRM Research Institute, Bangalore, India
‡Old Dominion University, Suffolk, VA, USA
ughosh@tnstate.edu*, pushpita.c@res.srmuniv.ac.in †, sshetty@odu.edu‡

***Abstract*— Emerging software defined networking (SDN) paradigm provides flexibility in controlling, managing, and dynamically reconfiguring smart grid networks. It can be seen in the literature that considerably less attention has been given to provide security in SDN-enabled smart grid networks. Most of the efforts focus on protecting smart grid networks against various forms of outsider attacks only by providing consistent access control, applying efficient and effective security policies, and managing and controlling the network through the use of a centralized SDN controller. Furthermore, centralized SDN controllers are plagued by reliability and security issues. This paper presents a framework with multiple SDN controllers and security controllers that provides a secure and robust smart grid architecture. The proposed framework deploys a local IDS in a substation to collect the measurement data periodically and to monitor the control-commands that are executed on SCADA slaves. A global IDS in control center collects the measurement data from the substations and estimates the state of the smart grid system by utilizing the theory of differential evolution. The global IDS further verifies the consequences of control-commands issued by SDN controller and SCADA master. An alarm is generated upon detection of an attacker or unsteady state of the smart grid system. The framework also deploys light-weight identity based cryptography to protect the smart grid network from outside attacks. Performance comparison and initial simulation result have been presented to show that the proposed framework is effective as compared to existing security frameworks for SDN-enabled smart grids.**

***Index Terms*—SDN, Smart Grids, IDS, Attacks, Security**

I. Introduction

Smart grid is a large-scale heterogeneous complex networking between a several number of sensors, actuators, smart meters, supervisory control and data acquisition (SCADA) systems, and also end-user devices and appliances located on residential and commercial premises in order to facilitate the generation, transmission and distribution of power. The communication infrastructure must be scalable, reliable, secure and efficient to sustain the transmission of a massive amount of real-time data generated by the deployed sensors in smart grid. Software defined networking (SDN) can be integrated in smart grid to achieve such communication infrastructure. It allows to manage and verify the correctness of network operations at run time. The globalized view of the SDN controller allows fault (due to accidental failures and malicious attacks) detection, isolation of affected components, and remediates of abnormal operation in the SDN-enabled smart grid networks more efficiently as compared to legacy based networks.

The proliferation of the smart grid technologies brings the promise of an era of easy and optimal use of power delivery systems as well as intelligence and efficiency. Recently, a number of research papers have been proposed in the literature [1]–[8] to introduce the concept of SDN in smart grid networks. Most of these proposals mainly focus on (i) the advantages and potential risks of using SDN in smart grid and (ii) investigation how SDN can fulfill communication requirements of smart grid communication networks regarding properties like quality of service (Qos), latency and link failover time (recovery time from a link failure). However, considerably less attention has been given to provide security in SDN-enabled smart grid networks [9]–[11]. Most of the researchers assume that SCADA master, SDN controller and their applications are non-compromised. They further consider that SDN can offer security in smart grid by providing consistent access control, applying efficient and effective security policies, and managing and controlling the network centrally. Their main focus on protecting the smart grid networks against various forms of outsider attacks and providing security assurance within the cyber (or SDN) domain only. They significantly overlook the insider attacks that may harm the smart grid system as a whole [12]. It further suffers from possible reliability and security issues due to use of a centralized SDN controller.

Contributions: In this paper, we propose a security framework with multiple SDN controllers and intrusion detection systems (IDS) to provide a secure and robust smart grid architecture. A light-weight identity based cryptography [13] has been used to protect the smart grid network from outside attacks. A local IDS is deployed in a substation to collect the measurement data periodically and to monitor the control-commands that are executed on SCADA slaves. Whereas a global IDS runs at control center and collects the measurement data from the substations and estimates the state of the smart grid system by utilizing the theory of differential evolution [14]. It further verifies the consequences of control-commands issued by either SDN controller or SCADA master. The global IDS generates an alarm and notifies to the intrusion elimination system (IES) if it detects unsteady state of smart grids.

Paper Overview: The remainder of the paper is organized as follows: The state-of-the-art study is presented in Section II followed by the attack scenario and system model in Section III and Section IV respectively. In Section V we present our proposed security framework for SDN-enabled smart grid.

2332-5666/17 $31.00 © 2017 IEEE
DOI 10.1109/ICDCSW.2017.20

Section VI compares the proposed framework with existing security frameworks and Section VII discusses simulation environment and initial result. Finally, the paper is concluded in Section VIII.

II. Related Works

In [1], Goodney *et al.* proposed to use SDN for controlling communication between PMUs. The authors developed a SDN-based network application to facilitate the management of PMUs and implemented multicast and data rate filtering functionalities using OpenFlow rules installed on SDN switches. Dorsch *et al.* [2] demonstrated the use of SDN for controlling and managing the transmission and distribution in power grids. The authors introduced algorithms for fast recovery from a link failure and load management. They developed a SDN testbed to measure the communication delays for IEC 61850 traffic. They further demonstrated the QoS enforcement for grid data traffic with different priorities. Kim *et al.* proposed in [3] to use OpenFlow switches to form virtual local area networks (VLANs) for multiple grid applications with different QoS requirements. In [4], Gyllstrom *et al.* also developed and evaluated fast recovery from a link failure algorithm in SDN-based smart grid networks.

In [5], Aydeger *et al.* demonstrated the usefulness of SDN to achieve resilience in smart grid networks. They introduced multiple connection interfaces among distributed substations and investigated the effect of failures of the wired connection. Zhao *et al.* discussed in [7] the efficacy of SDN to improve the quality of service (QoS) routing for smart grids. The authors designed a framework to enable an efficient decoupled implementation of dynamic routing protocols. Akkaya *et al.* [6] presented different SDN deployment scenarios in local networks of smart grid to substantiate the potential utilization of the SDN technology. Ghosh *et al.* in [8] proposed a simulation based analysis to demonstrate the effect of controller faults (single-point-of-failure) in a SDN-enabled smart grid infrastructure.

Molina *et al.*, presented a SDN based architecture in [10] for a substation that follows the IEC 61850 standard. The authors included automation techniques for performing a flow-based resource management that enable features such as routing, traffic filtering, QoS, load balancing, monitoring, or security. Cahn et al. [9] proposed a SDN-based power grid architecture, called Software-Defined Energy Communication Network (SDECN). This architecture mainly provides substation automation that allows the network to auto-configure, secure and reliable against possible incorrect configured systems. The authors developed the SDECN prototype using Ryu OpenFlow controller and tested with real intelligent electronic devices (IEDs). Dong *et al.* presented a position research study [11] to show how SDN can improve the resilience of smart grid networks to malicious attacks. The authors further discussed additional risks introduced by SDN in smart grids and how to manage them.

III. Attack Scenario

A SDN-enabled smart grid mainly consists of three parts: (1) a control center; (2) communication networks and (3) smart power grid devices. Figure 1 illustrates the attacks in smart grid. Control center runs the SDN controller and SCADA master commodity computers and servers. The SCADA master performs various grid control applications, e.g., grid status monitoring, under-frequency load shedding, frequency and voltage controls, and so forth. It collects measurement data periodically from the SCADA slaves (sensors, actuators) through the use of OpenFlow (OF) switches and SDN controller. The SCADA master processes the received data and sends the control-command (such as read, write or execute [15]) to the SCADA slaves.

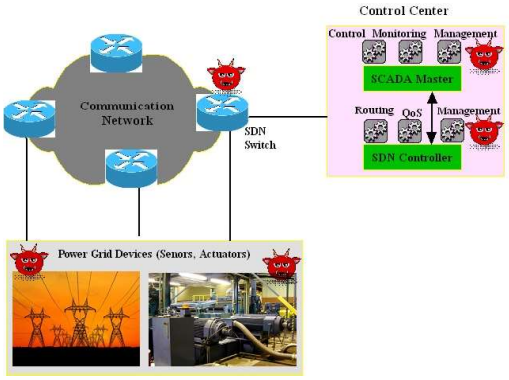

Fig. 1. Attack Scenarios in SDN-enabled Smart Grids

TABLE I
Control-commands in SDN-enabled smart grids

SCADA Control Commands	Functionalities	SDN Controller Commands	Functionalities
Read	Retrieve measurements from substations	Add_Flow	Add a new flow in OF switches
Write	Configure Smart grid devices	Del_Flow	Remove a flow from OF switches
Execute	Operate smart grid devices	Mod_Flow	Edit a flow in OF switches

In *first attack scenario*, an application of SCADA master or SCADA master itself can be compromised. Similarly, an application of SDN controller or SDN controller itself can be compromised. The compromised SDN controller may issue malicious control-commands (such as Add_Flow, Del_Flow, Mod_Flow) to degrade the performance of the network and subsequently smart grid. Table I summarizes the control-commands in SDN-enabled smart grid networks.

In *second attack scenario*, the OF switches may be compromised. These OF switches may drop, inject false packets and delayed the packets that carry measurement data/control-commands from SCADA slaves/master to SCADA master/slaves. For example, a packet that carries a critical control-command like open a breaker of a relay. This packet can be dropped or delayed by an intermediate malicious switch. It may cause a potential risk to physical infrastructure of a substation.

The detection and identification of bad data in measurements are important phases for state estimation of a smart grid. The poor calibration of SCADA slaves, the failure communication between SCADA slaves and SCADA master,

and also inject malicious measurements by SCADA slaves [16] are the main sources of bad data. These bad data can influence the quality of results obtained from state estimation algorithm. In *third and final attack scenario*, we consider compromised SCADA slaves that can inject malicious measurements [16] into smart grid network.

IV. System Model

We consider a SDN-enabled smart power grid network that has several substations with a control center. We assume that all the smart grid and communication devices have unique IDs and registered to either their corresponding substation or control center. In addition, the public (KP_A) /private (KS_A) key pair of a device A is generated using the following technique [13]: $G1$ and $G2$ be the two groups of a prime order q, $Q1$ and $Q2$ be the generators of $G1$, and a bilinear pairing is a map $e : G1 \times G1 \rightarrow G2$ having the following properties:

- Bilinear: $e(uQ1, vQ2) = e(Q1, Q2)^{uv}$, $\forall u, v \in Z_q$;
- Non-degenerate: There exist $Q1, Q2 \in G1$ such that $e(Q1, Q2) \neq 1$;
- Computable: $\forall Q1, Q2 \in G1$, there is an efficient algorithm to compute $e(Q1, Q2)$.

All the devices in smart grid network keep the security parameters $G1$, $G2$, e, $H1$, $H2$, $Q1$, $P_{pub} = sQ1$, where s is the master key and it is kept secret by control center. Here, $H1$ and $H2$ are two cryptographic hash functions such that $H1 : \{0,1\}^* \rightarrow G1$ and $H2 : \{0,1\}^* \times G1 \rightarrow Z_q$. For a device A with identifier ID_A, there will be a public key $KP_A = H1(ID_A)$ and a private key $KS_A = sKP_A$. The device identifiers IDs are type specific. For example, the meter number is the ID for a smart meter whereas hardware/IP address is the ID for a sensor.

In order to generate a secret session key K_{AB} between devices A and B, they exchange random numbers r_1 and r_2 to each other. Device A generates the secret session key using $K_{AB} = e(r_1 KS_A, r_2 KP_B)$, whereas device B also generates the secret session key using $K_{BA} = e(r_1 KP_A, r_2 KS_B)$. The following equation shows that both devices A and B generate the same secret session key [17]:

$$\begin{aligned} K_{AB} &= e(r_1 KS_A, r_2 KP_B) = e(KS_A, KP_B)^{r_1 r_2} \\ &= e(sKP_A, KP_B)^{r_1 r_2} = e(KP_A, KP_B)^{s r_1 r_2} \\ &= e(r_1 KP_A, r_2 sKP_B) = e(r_1 KP_A, r_2 KS_B) = K_{BA} \end{aligned}$$

V. The Proposed Security Framework for SDN-enabled Smart Grids

Figure 2 presents the propose secure framework for SDN-enabled smart grids. Our framework mainly includes a control center and a several number of substations and all of them connected in a wide area network. Control center comprises of three components: (1) a global SDN controller which is responsible for communication between control center to substations and a substation to other substations; (2) a SCADA master which is mainly responsible for controlling, monitoring and managing smart grid devices such as sensors, actuators

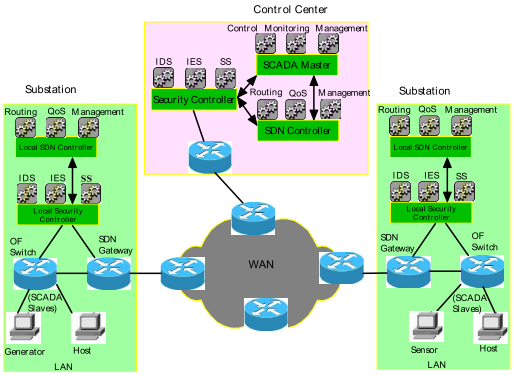

Fig. 2. Secure SDN-enabled Smart Grid Architecture

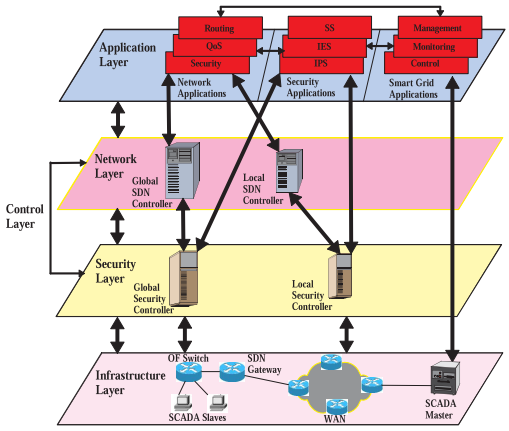

Fig. 3. Secure SDN-enabled Smart Grid Layers

(in general SCADA slaves in substations); and (3) a global security controller which is responsible for providing security in both smart grid and communication devices. A substation contains: (1) a local SDN controller that controls the communication between devices inside the substation; (2) a local security controller that provides security inside the substation; and (3) openflow (OF) switches, a gateway and SCADA slaves.

With respect to SDN layers, the propose secure SDN-enabled smart grid layering architecture is shown in Figure 3. It has infrastructure, control and application layers. Infrastructure layer contains OF switches, SCADA master and slaves. We divide control layer into security and network sub-layers. Security sub-layer includes a global security controller (for control center) and a local security controller (for a substation). Network sub-layer involves with a global SDN controller (for control center) and a local SDN controller (for a substation). Application layer runs the application programs at SDN controller, security controller and SCADA master. SDN controller runs the application programs to manage devices and provide routing and QoS in infrastructure layer. SCADA master runs the application programs to control, configure and manage the smart grid devices (SCADA slaves). Security controller runs three application programs: (1) a security

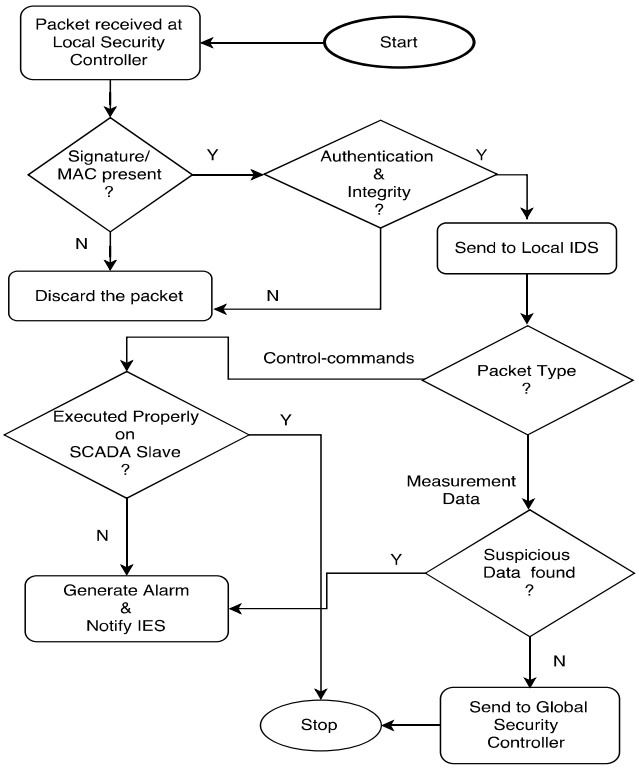

Fig. 4. Workflow at Local Security Controller

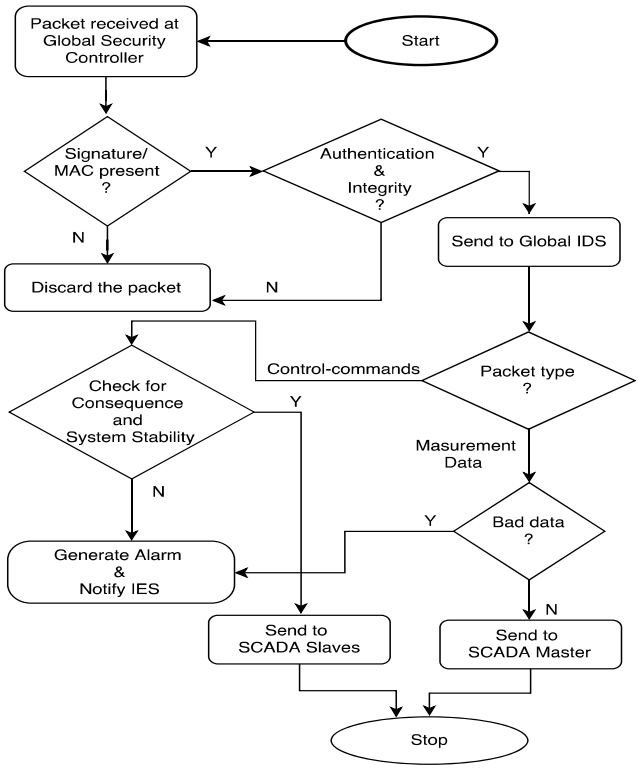

Fig. 5. Workflow at Global Security Controller

system (SS) that generates and manages the cryptographic keys (public/private or shared keys as discussed in Section IV) and provides message authentication and integrity for each device; (2) an intrusion elimination system (IES) that eliminates the attackers (detected by IDS) from smart grid network through the use of SDN controller; and (3) an intrusion detection system (IDS) that monitors all the devices and their activities in a substation/control center and generates an alarm and notifies to IES once attacks detected.

In order to provide message authentication and integrity in smart grid communication, we use digital signature for broadcasting/multicasting messages and MAC for unicasting messages. Device A generates the digital signature using its private key KS_A to the broadcast/multicast messages and sends the signed messages along with its ID_A. On receiving the signed message, device B can verify the signature by using the public key KP_A of A. For unicast communication, device A generates a MAC tag using the secret session key K_{AB} to the message and sends the message along with the MAC tag to device B. Device B also generates a MAC tag using the secret key K_{BA} on the received message from A. It then compares both generated MAC tag and received MAC tag from A. Device A is authenticated to B if both tags are same.

A global security controller runs in control center whereas a local security controller runs in a substation. The workflow diagrams of the local security controller and the global security controller are presented in Figure 4 and Figure 5 respectively. Both security controllers discard the packet if they receive it without the authentication tag (signature or MAC). The security controllers further verify authentication and integrity of the packet. If verification successful, the local security controller sends the packet to local the IDS whereas the global security controller sends the packet to the global IDS.

The local IDS collects the measurement data periodically from SCADA slaves and verifies for suspicious data. It generates an alarm and notifies to IES if suspicious data detected. Otherwise the local IDS allows to send the measurement data from the substation to control center. It further monitors the control-commands (sent by SCADA master) that are executed on SCADA slaves. The global IDS collects the measurement data from the substations. It verifies the measurement data for bad data detection and identification and estimates the state of the smart grid system by utilizing the theory of differential evolution [14] (discussed below). The global IDS further measures the consequences of control-commands issued by either SDN controller or SCADA master. It generates an alarm message and notifies the intrusion elimination system (IES) if an unsteady state of smart grid system found.

Our proposed IDS allows to insert flows (defined by IP/hardware/port address, VLAN) into the network and monitors each of them. A predefined threshold has been set by IDS for each flow in order to detect DoS attack. Our IDS further monitors the OF switches and computes the packet drop ratio (β), packet false injection ratio (γ), and an average packet delay (δ) for each OF switch. The parameters are defined as follows:

TABLE II
COMPARISON WITH EXISTING FRAMEWORKS

Framework/ Architecture	First Attack Scenario		Second Attack Scenario	Third Attack Scenario	Security	Robustness
	SCADA Master Security	SDN Controller Security	OF Switch Security	SCADA Slave Security	Tool Used	
Cahn *et al.* [9]	Not Considered	Not Considered	Considered	Not Considered	SDN Controller Policies	Robust
Molina *et al.* [10]	Not Considered	Not Considered	Considered	Not Considered	sFlow Collector	Robust
Dong *et al.* [11]	Considered	Not Considered	Considered	Not Considered	Centralized IDS	Not Robust
Proposed	Considered	Considered	Considered	Considered	Distributed IDS	Robust

- β: a ratio between the number of packets drop by a switch and the total number of packets received by the switch.
- γ: a ratio between the number of packets falsely injected by a switch and the total number of packets sent by the switch.
- δ: the average time difference between arrival time to a switch and departure time from the switch for n number of packets

There is a predefined threshold (ω_β, ω_γ, ω_δ) respectively associated with each behavior. An OF switch is detected as malicious by our IDS if one of the parameters reaches or exceeds the threshold *e.g.*, $\beta \geq \omega_\beta$ or $\gamma \geq \omega_\gamma$ or $\delta \geq \omega_\delta$. For example, an average packet delay in an OF switch is 2ms when there is no congestion in the network. In a worst case, this average packet delay increases to 5ms due to increase of congestion in the network. An OF switch is detected as malicious if the average packet delay for 100 packets exceeds the threshold 5.1ms by the switch. It may be noted that SDN controller has the global view on the network conditions (such as network congestion, link delays) in a substation.

State Estimation and Bad Data Detection: We use differential evolution (DE) [14] to estimate the state of smart grid and detect bad data. The state vector is composed of all or most of the voltages (module and argument) system, except for the argument bus reference. Therefore this state vector has the dimension $2 * b - 1$, where b is the number of buses in the system,

$$\mathrm{X} = \begin{bmatrix} \mid V_1 \mid \\ \mid V_2 \mid \\ \vdots \\ \mid V_b \mid \\ \mid \theta_1 \mid \\ \mid \theta_2 \mid \\ \vdots \\ \mid \theta_{b-1} \mid \end{bmatrix}$$

In DE, in order to get a new population at each iteration it is necessary to optimize the problem by using mutation, crossover and selection.

- **Mutation:** For each vector belonging to the population, a new mutated vector is created using Equation 1.

$$k_{i,G+1} = x_{\upsilon_1,G} + F \times (x_{\upsilon_2,G} - x_{\upsilon_3,G}) \qquad (1)$$

  Where the indices $\upsilon_1, \upsilon_2, \upsilon_3 \in \{1, 2, ..., NP\}$ are all mutually different and random. These are different from the index i. G corresponds to the current iteration of the simulation. F is a constant real value, $F \in [0, 2]$ and controls the amplification of the differential variation $(x_{\upsilon_2,G} - x_{\upsilon_3,G})$.

- **Crossover:** To introduce a wider range of results from several generations of populations, crossover is used to create a new vector y using the following Equation,

$$y_{ji,G+1} = \begin{cases} k_{ji,G+1}, & \text{if}(randb(j) \leq CR) \text{or } j = rnbr(i) \\ x_{ji,G}, & \text{if}(randb(j) > CR) \text{or } j \neq rnbr(i) \end{cases}$$

  Here, $randb(j)$ is the jth evaluation of a uniform random number generator with outcome $\in [0, 1]$ where CR is the crossover constant, a real and constant value chosen from $\in [0, 2]$, given by the user. $rnbr(i)$ is a randomly chosen index $\in [1, 2, ..., D]$ to ensure that $y_{i,G+1}$ gets at least one parameter from $k_{i,G+1}$.
- **Selection:** In order to verify whether the new test vector y may be inserted into the new population of values, it is necessary to check if this function has a lower cost compared to the same position as the previous generation (vector x). If the cost function of the test vector is less than the amount reported by the vector x, it is replacing, otherwise the previous value is kept unaltered.

Once the selection process is done using DE method, the measured data is selected if there is no bad data. If bad data is detected by the IDS, it generates an alarm and notifies IES.

VI. PERFORMANCE COMPARISON

Table II presents the comparison of proposed framework with existing security frameworks for SDN-enabled smart grids. It can be seen that our propose framework only consider the security of all the attack scenarios discussed in Section III. We use distributed IDS to provide security in substations and control center. The propose framework further deploys multiple SDN controllers in substations and control center. The global SDN controller at control center can be used as the backup controller in case a SDN controller fails in a substation. Hence the propose framework is robust.

VII. SIMULATION AND INITIAL RESULT

In our simulation, we use Mininet [18] to simulate an IEEE 37-buses smart grid network as shown in Figure 6. The network connects 15 substations with a control center over a wide-area network. Control center has (1) a global SDN controller GSC, (2) a virtual host that runs our IDS ($IDS - G$), and (3) a virtual host that runs as DNP3 server. Each substation, say i, consists of: (1) a local SDN controller (LSC_i), (2) an open flow (OF) switch (S_i), (3) a SDN-enabled gateway (SGW_i), (4) an IDS ($IDS - L_i$), (4) a sensor/actuator (T_i) that runs DNP3 clients to mimic communications between control center (with DNP3 server) and electronic devices in the substation, and (5) a virtual host (H_i) to generate background traffic. The SDN has a data plane with 26 OpenFlow

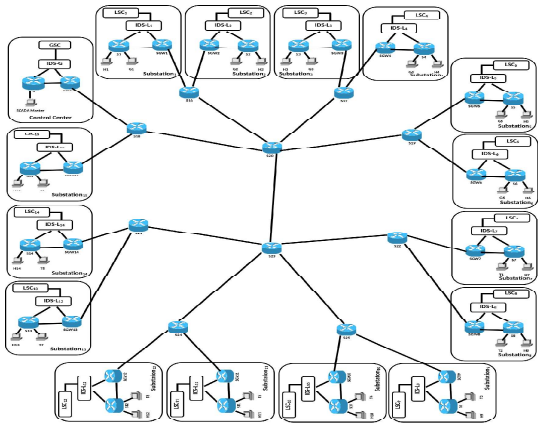

Fig. 6. Network Topology for IEEE 37-buses

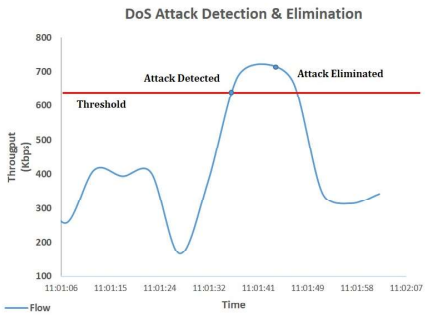

Fig. 7. DoS Attack Detection and Elimination

(v1.3) [19] enabled switches and 16 gateways. A Ryu [20] controller is running remotely on Linux (Ubuntu 3.16.0-38-generic kernel) from the switches.

Figure 7 shows DoS attack detection and elimination using our proposed IDS and IES respectively. In this DoS attack, an attacker (H_1) that floods ICMP Echo Request packets. We set a threshold of 100 packets per second in our IDS.

VIII. Conclusion

In this paper, we have presented a framework with multiple SDN controllers and security controllers to provide a secure and robust smart grid architecture. We have used a light-weight identity based cryptography to protect the smart grid network from outside attacks. A local IDS collects the measurement data periodically and monitors the control-commands that are executed on SCADA slaves in a substation. Whereas a global IDS is deployed to collect the measurement data from the substations and estimate the state of the smart grid system by utilizing the theory of differential evolution. The consequences of control-commands issued by SDN controller and SCADA master are verified by the global IDS further. It generates an alarm and notifies to the intrusion elimination system whenever the IDS detects an attacker and unsteady state of the smart grid system. We have compared the proposed framework with existing security frameworks to show that the proposed framework is more efficient against attacks related to SDN-enabled smart grids.

Acknowledgement

This material is based upon work supported by the Department of Energy under award number DE-OE0000780 and DHS Award 2014-ST-062-000059. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] A. Goodney, S. Kumar, A. Ravi, and Y. H. Cho, "Efficient pmu networking with software defined networks," in *IEEE SmartGridComm*, 2013.

[2] N. Dorsch, F. Kurtz, H. Georg, C. Hagerling, and C. Wietfeld, "Software-defined networking for smart grid communications: Applications, challenges and advantages," in *IEEE SmartGridComm*, 2014.

[3] Y.-J. Kim, K. He, M. Thottan, and J. G. Deshpande, "Virtualized and self-configurable utility communications enabled by software-defined networks," in *IEEE SmartGridComm*, pp. 416–421, 2014.

[4] D. Gyllstrom, N. Braga, and J. Kurose, "Recovery from link failures in a smart grid communication network using openflow," in *IEEE SmartGridComm*, pp. 254–259, Nov 2014.

[5] A. Aydeger, K. Akkaya, and A. S. Uluagac, "Sdn-based resilience for smart grid communications," in *Network Function Virtualization and Software Defined Network (NFV-SDN), 2015 IEEE Conference on*, pp. 31–33, IEEE, 2015.

[6] K. Akkaya, A. S. Uluagac, and A. Aydeger, "Software defined networking for wireless local networks in smart grid," in *Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th*, pp. 826–831, 2015.

[7] J. Zhao, E. Hammad, A. Farraj, and D. Kundur, *Network-Aware QoS Routing for Smart Grids Using Software Defined Networks*. 2016.

[8] U. Ghosh, X. Dong, R. Tan, Z. Kalbarczyk, D. K. Yau, and R. K. Iyer, "A simulation study on smart grid resilience under software-defined networking controller failures," in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, CPSS '16, pp. 52–58, 2016.

[9] A. Cahn, J. Hoyos, M. Hulse, and E. Keller, "Software-defined energy communication networks: From substation automation to future smart grids," in *IEEE SmartGridComm*, pp. 558–563, 2013.

[10] E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa, "Using software defined networking to manage and control iec 61850-based systems," *Comput. Electr. Eng.*, vol. 43, pp. 142–154, Apr. 2015.

[11] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *1st ACM Workshop on CPSS*, 2015.

[12] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 796–808, 2011.

[13] J. C. Cha and J. H. Cheon, "An identity-based signature from gap diffie-hellman groups," in *Public Key Cryptography*, vol. 2567, pp. 18–30, 2003.

[14] R. Storn and K. Price, "Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces," *J. of Global Optimization*, vol. 11, pp. 341–359, Dec. 1997.

[15] H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[16] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, (New York, NY, USA), pp. 21–32, ACM, 2009.

[17] U. Ghosh and R. Datta, "A secure addressing scheme for large-scale managed manets," *IEEE Transactions on Network and Service Management*, vol. 12, pp. 483–495, Sept 2015.

[18] "Mininet: An instant virtual network on your laptop (or other pc)." http://mininet.org/.

[19] "Openflow switch specification." http://www.openflow.org/documents/openflow-spec-v1.0.0.pdf.

[20] "Ryu sdn framework." https://osrg.github.io/ryu/.