Identifying Security Challenges in Renewable Energy Systems: A Wind Turbine Case Study

Anish Jindal, Angelos K. Marnerides, Andrew Scott, David Hutchison
School of Computing & Communications, Lancaster University, Lancaster, UK
{a.jindal3,angelos.marnerides,a.scott,d.hutchison}@lancaster.ac.uk

ABSTRACT

Distributed renewable energy systems (DRESs) and their interconnection network, typically using Internet-based protocols, are susceptible to a wide range of cyber-security and resilience challenges. These challenges have been shown to cause problems for the overall grid optimization process. In order to detect such events, we argue that an adequate correlation between network and energy generation data is required. Therefore, in this study, we provide a work-in-progress insight related to the profiling of real network data and energy generation measurements gathered by a local wind-turbine at Lancaster University. We argue that such an analysis is very important to profile various attack vectors in the modern energy networks that consider DRESs and take necessary actions to prevent any data breaches in the future.

1 INTRODUCTION

The continuous and incremental consumer-side energy demand has unavoidably escalated the burden on power grids on a global scale [1]. The integration of distributed renewable energy sources (DRESs) is considered as a promising solution towards aiding the core grid during peak demand periods by supplying considerably "green" energy with limited costs in comparison with traditional sources of energy (e.g., fossil fuels). According to the Energy Information Administration, DRESs constitute 12.5% of the total energy generation of the world and their use is further anticipated to rise to 20% by the year 2040 to produce about 130 quadrillion Btu per year [1]. However, this large DRESs network is prone to attacks such as cyber-attacks that can, in the worst case scenario, lead to grid breakdown or even blackouts [2]. This is because DRESs, apart from fulfilling the partial energy needs of the consumers, also partake in providing ancillary services such as frequency regulation for maintaining grid stability. Any deviation from their normal working can lead to disruption in the grid that can ultimately cause grid breakdown. Therefore, it is important to detect and prevent any attempted unauthorized access to deployed DRES systems.

While most communication, in DRESs, is and will be protected through the use of secure protocols, this by itself is not enough. The use of, and dependency on, ancillary services and protocols allows more opportunity for attacks. We argue that explicitly within DRES systems, a particular point of interest is the analysis of identified correlations between network traffic and energy generation, either in terms of management/ operational data or updates to controls/ set points. Working in this direction, in this work-in-progress paper, we conduct a measurement-based approach and analyze the network flow and generation data within a real DRES end-system (the local wind turbine) to identify potential security loopholes.

2 SYSTEM DESCRIPTION

An overview of the schematics and the main network connections of the wind turbine installed at Lancaster University are shown in Fig. 1. The installed capacity of this wind turbine is 2.3 MW, working on a 11kV electrical line. Fig. 1 illustrates that the turbine communicates with an external server in charge of storing its generation data. Moreover, this external server is responsible for managing system configurations, micro-controller settings, data security assurance, and any associated software or network-related issues that relate to the wind turbine. Data is collected for the real wind turbine energy generation unit along with the associated network data flows between the wind turbine and the server. The wind turbine generation data is gathered for every minute and consists of 30 different attributes. The network-related data is monitored using NetFlow, with records generated whenever any IP address attempts to communicate with the turbine using its IP interface. IP addresses in the network data have been further post-analyzed using geolocation data and the dataset is extended to comprehensively profile both legitimate and any potentially malicious network flows.

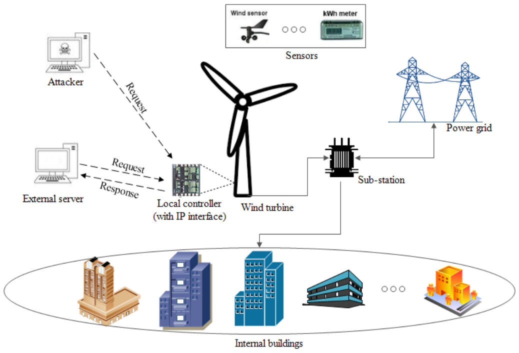
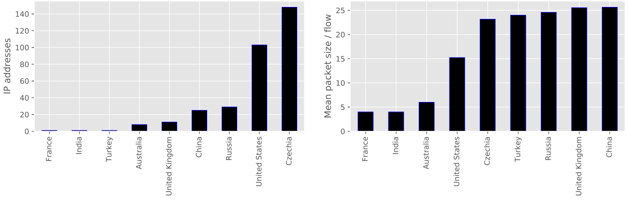


Figure 1: System overview - Schematics & connections.

3 RESULTS AND DISCUSSION

In order to perform the statistical analysis, one day's data (1st January 2019) is analyzed with respect to the energy generation from the wind turbine as well as the network flow data. Our initial findings suggest that the corresponding network information to/from the data server does not necessarily depend on the energy generation of the wind turbine. We identify that the wind-turbine updates the server periodically by sending all of the previous hour's data in one burst (after being ESP encapsulated, [3]), while the residual continuous packet flow (over TCP/UDP) results from active monitoring of various sensors installed on the wind turbine. Moreover, the average packet size does not vary significantly from its pattern, thus it is implied that the underlying network communication is not synchronized with the actual energy generation.

We also provide an insight related to malicious scans aiming to identify security loopholes on the wind turbine. The profile of malicious intent scanning (or unauthorized data access requests) for one given day is shown in Fig. 2. With the use of honeypot data provided by BadPackets LLC (BadPackets LLC: https://badpackets.net/), a correlation analysis between the various access requests to the wind-turbine is performed. Based on the correlation analysis, we identify 327 distinct IP addresses originating from Autonomous Systems (ASes) distributed in 8 different countries. All IP addresses were flagged as members of Mirai-alike botnets and they all initiated scans with malicious intent in order to penetrate the wind-turbine within a single day. Table 1 highlights the top 8 ASes from which most of the identified malicious scans were received.



(a) (b)

Figure 2: (a) Count of malicious IP addresses per country; (b) Mean packet size per malicious scan flow.

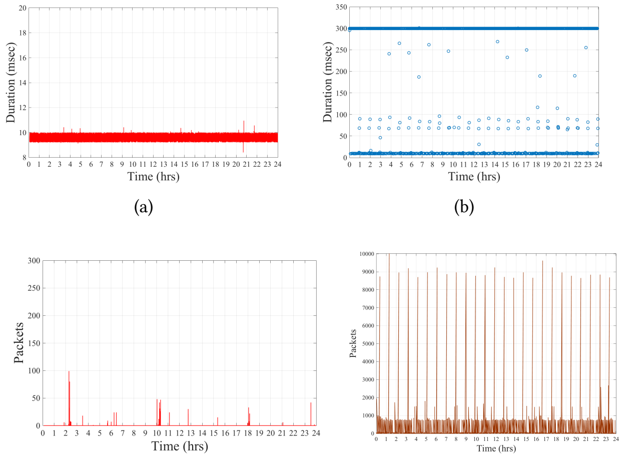
Table 1: Top 8 ASes targeting local wind-turbine

Organisation	IP count	Country
SuperNetwork s.r.o.	148	Czechia
CariNet, Inc.	49	USA
HLL LLC	29	Russia
CHINA UNICOM Backbone	18	China
LeaseWeb Netherlands B.V.	16	Netherlands
QuadraNet, Inc	15	USA
Jisc Services Limited	14	UK
Merit Network Inc.	12	USA

Further analysis of the identified unauthorized IP addresses shows that they send requests within a very short duration and send few data packets as evident from Figs. 3(a) and 3(c). This is due to the fact that these IP addresses are corresponding to potentially malicious/bot devices that aim to establish a connection in order to further infiltrate the wind turbine.

This analysis reveals the contrasting nature of unauthorized IPs and the legitimate IPs as it can be seen in Figs. 3(b) and 3(d) that a longer-lived connection is established when monitoring the sensors, while major packet flow is happening in short bursts of time. Consequently, our analysis leads to an interesting correlation that both the malicious attempts and major data flows happen for a shorter time duration. Thus, we can utilise this observation to profile attack signatures such as to block the wind turbine on transmitting data to unauthorized IP addresses.

The Pearson correlation output of the malicious access attempts revealed that unauthorized requests are more random in nature as compared to legitimate requests where the correlation between IP source port and IP destination port is high, by more than 40%. It is to be noted that unauthorized access requests happen mostly via the TCP/UDP protocols, however, a few of the unauthorized IPs tried to access the wind turbine using the ICMP protocol, where the targeted attack was much more focused. The ICMP-based access control requests are anticipated to be a potential “ping of death" attack where the attacker sent crafted ICMP packets greater than 1500 bytes as being the threshold for the acceptable Maximum Transmission Unit (MTU) size over Ethernet-based networks.



(a) (b)

(c) (d)

Figure 3: (a) Duration for unauthorized requests; (b) Duration for authorized requests; (c) Packets sent for unauthorized requests; (d) Packets flow for authorized requests.

4 CONCLUSION

This work-in-progress paper provides a first insight on the network and data generation-wise analysis of a wind-turbine installed within the Lancaster University campus. Through an inter-correlation analysis, we identify the patterns in which the wind-turbine updates a remote server hosted by the managing third-party company. From a pure network-based analysis, we observe the number of scans with malicious intent by Mirai-infected bots aiming to penetrate the wind-turbine and obtain useful information. In addition, we observe a "ping of death" performed by one of the scanners in which large sized ICMP packets were sent to various ports on the turbine. We argue that this piece of work can act as a useful input on the systematic cyber-security assessment of DRES end-systems.

5 ACKNOWLEDGMENT

The authors acknowledge the support of the H2020 EU’s Enable Ancillary Services by Renewable Energy Sources (EASY-RES) project (Agreement No.764090) for funding this research work. The authors are also thankful to Jan Bastiaans, Denes Csala and John Couzins of Lancaster University for providing the necessary datasets. The authors would also like to thank Mr. Troy Mursch from BadPackets LLC for providing the Mirai datasets.

REFERENCES

[1] EIA. International energy outlook 2018. Technical report, U.S. Energy Information Administration, 2018. Available: https://www.eia.gov/outlooks/ieo/.

[2] Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, and Raja Masood Larik. Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, 5(3):468–483, December 2018. doi: https://doi.org/10.1016/j.jesit.2018.01.001.

[3] S. Kent. IP Encapsulating Security Payload (ESP). RFC 4303, RFC Editor, December 2005. URL https://www.rfc-editor.org/rfc/rfc4303.txt.