Smart Grid Cyber Security

Faheem Ahmad Qureshi, Donna O'Shea, and Mubashir Husain Rehmani
Munster Technological University (MTU)
faheem.qureshi@mycite.ie, Donna.OShea@cit.ie, Mubashir.Rehmani@cit.ie

Electric Grid

- Electric grid has served us for over century, but the existing grid framework is now outdated.
- It lacks efficiency and reliability.
- Deficiency of real-time monitoring & control.
- Renewable energy resources (RER) integration and power system applications like demand response and real time pricing requires dual flow of power and information.
- To overcome these challenges, the Smart Grid paradigm has been proposed with variety of information and communication technologies.
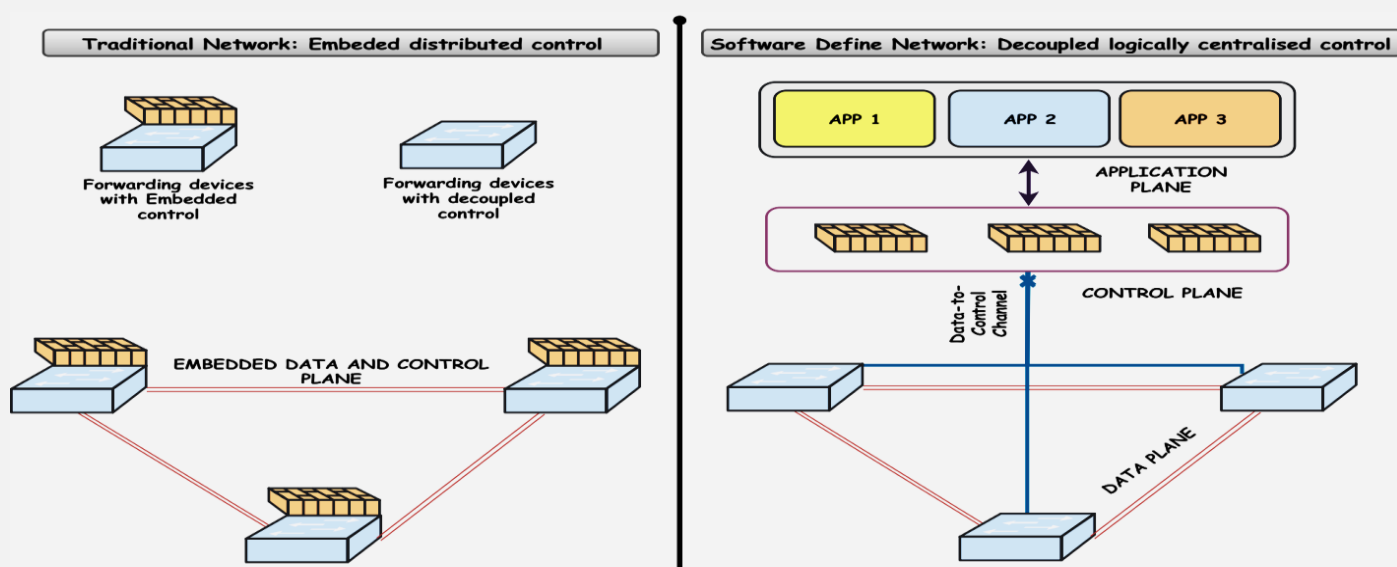

Smart Grid (SG)

- SG has revolutionised the electric grid, however its communication layer has certain limitations.
- SG operates on traditional networks with preinstalled network protocols offering distributed control. This restricts real-time changes in SG.
- Implementation of SG network policies, require network operators need to configure each individual network device separately, no network automation.
- All these factors makes the SG infrastructure static and non-adaptive.
- To overcome said challenges, latest state of art SG architecture suggest the usage of SDN for its communication layer.

Software Defined Networks (SDN)

- A programmable communication paradigm with isolated data and control plane to offer real-time configurable network.
- Provides global view of underlying forwarding devices, traffic engineering and automation.

Software Defined Network based Smart Grid (SDN-SG)

- Real time changes in SG network are possible enabling a highly programmable network.
- Global view of SG traffic at SDN controller enables the real-time monitoring and control of SG network.
- Moreover, with the help of SDN applications, SG network operations can be automated with minimum error prone human involvement.
- Emerging SDN-SG is in infancy stages and still have various security challenges. Hackers can exploit those security challenges to compromise SDN-SG and its a big deal for sate stability.
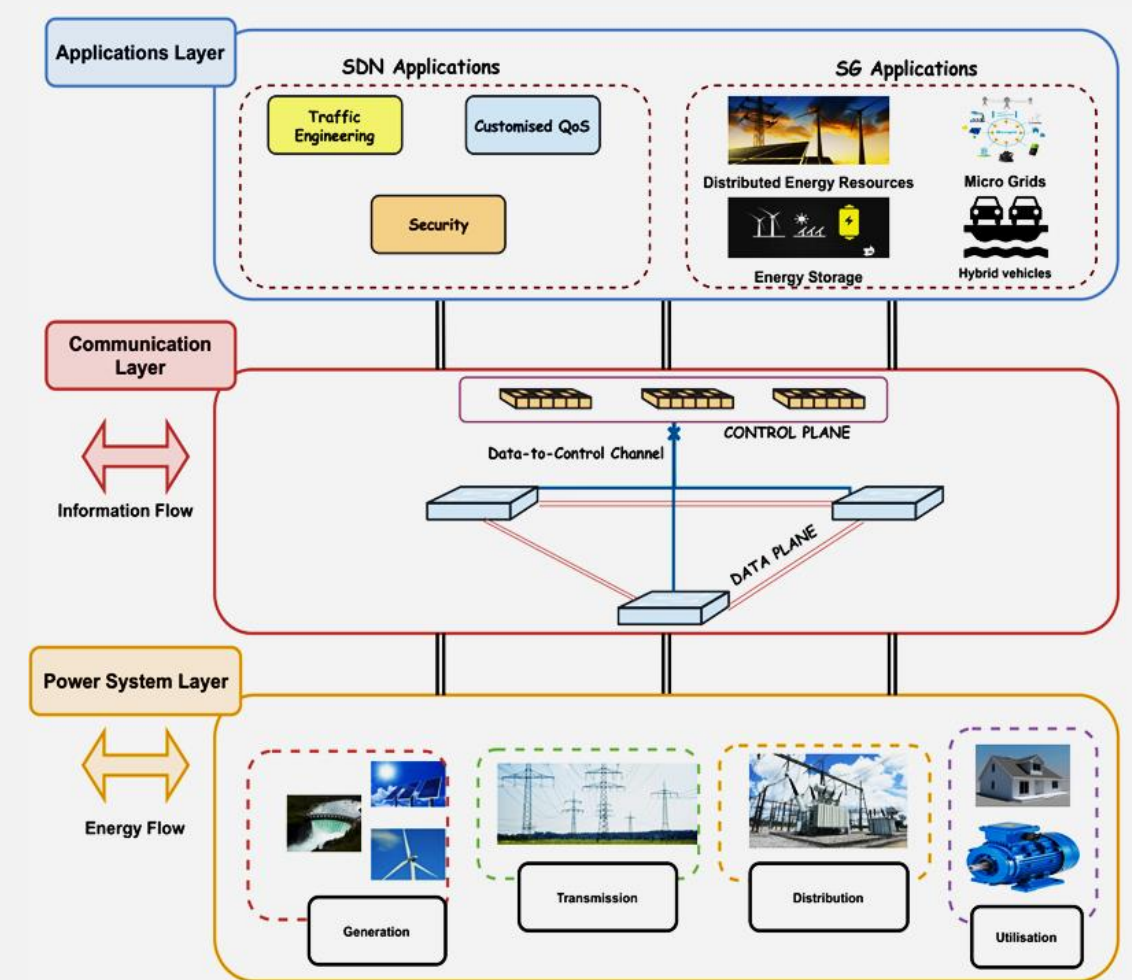
Review of Cyber Security Attacks on Smart Grid

Year	Country	Description	Impacts
2019	USA	DoS attack on the power utility of Converse, Los Angeles, and Salt Lake County of USA.	Interrupted power supply for 12 million customers for about 10 hours and caused a financial loss of over 10 million USD.
2016	Ukraine	DoS was launched on transmission substation.	It cut off around 20% of the power of the Kiev city of Ukraine affecting 560,000 population for one night.
2015	Ukraine	DoS attack compromised three energy distribution SCADA control.	It was estimated that about 230 thousand people were left without electricity for a period of 6 hours.
2015	USA	ISIL tries to hijack the USA electrical smart grid.	System sustained the attack but hints possible vulnerabilities.

Outcome of Research

- Analysis of SDN-SG under cyber attacks.
- Attack mitigation techniques for handling cyber attacks.
- Defence system that can counter cyber attacks before it compromise the system.
- Ensure reliable, stable and cyber resilient SDN-SG.

Significance for the Society

- SDN-SG advocates utilization of renewable energy systems, promoting a green environment.
- Resilient SG will ensure the reliable operations of other critical infrastructures.
- Cyber resilient Smart Grid enables a standard living of the inhabitants (Health, Education, Services, etc).
- SG complements the economic growth of society by energising industries.
- SG ensures reliable military defence of the state by providing uninterruptable energy supply.
- Secure SG guarantees the stable operation of society and its inhabitants.