MICRO GRID: Security Issues and Solutions

Silpa P S[1], Gayathri S Menon[2], Sethuraman N Rao[3]
Amrita Centre for Wireless Networks & Applications (AmritaWNA)
Amrita School of Engineering, Amritapuri
Amrita Vishwa Vidyapeetham, India
[1]silpasajeevan93@gmail.com, [2]gayathri.menon94@gmail.com, [3]sethuramanrao@am.amrita.edu

***Abstract*—Smart Grid consists of a network of computer infrastructure that takes care of power to monitor, manage and control power usage. Inclusion of various electronic, electrical and intelligent modules in the grid poses several cyber security challenges and needs different countermeasures to be applied. Micro Grid, a part of Smart Grid is also facing the same issues. This is due to the computational resource scarcity, communication constraints, and sensitive information in the data. In developing countries such as India, Micro Grid is an innovative opportunity to conserve power and reduce power consumption on a large scale. This paper gives an idea of the Micro Grid designed by our research center and shows how it helps in power conservation and lowering power consumption. Further it describes the potential security challenges faced by Micro Grid and corresponding solutions for the issues.**

Keywords – Micro Grid; Security Attacks; Solutions

I. INTRODUCTION

Smart Grid is one of the emerging applications in power management and power consumption of any country. A. R. Devidas and M. V. Ramesh [3] give an idea of a smart grid that can be implemented in a country like India. The major components of the proposed smart grid shown in Fig. 1 are:

- Smart Wireless Consumer Sensor Node (SWCSN): or smart metering device which measures the power consumed by each home.
- Smart Transmission Line Sensor Node (STLSN): is the transmission line between SWCSN and upper layers. It works on a sleep-wake mode.
- Smart Wireless Transformer Sensor Node (SWTSN): that is the other end of the STLSN. It collects the data from SWCSN via STLSN aggregates the data and makes decisions accordingly.
- Smart Controlling Station (SCS): aggregates data from all SWTSN and performs automatic billing and storage of data.

However, to the best of our knowledge it lacks research on the security and privacy issues. The advancement in both technology and user experience leads to well-known privacy and security threats.

The main features supporting Micro Grid is its decentralized energy generation, controlling power theft, reliability due to renewable resources of energy and advancement in both metering and billing systems. The implementation of the Micro Grid system requires integration and utilization of multiple devices, communication systems, sensor networks etc. The problems can be in the transmission line or in the nodes.

In Fig. 2, the schematic of Micro Grid architecture is explained. The main components used to design Micro Grid architecture are listed below. In this paper, the security issues related to these components are discussed in detail.

- Distribution Poles
- Smart Homes (assuming a renewable energy source at each smart homes)
- Smart Meters to continuously monitor the bidirectional flow of power of power to/from home.
- Intelligent modules present at each distribution poles to improve robustness. (Since a 3-phase line is considered in [2], three intelligent modules are placed at each distribution pole)
- Control Station for decision making based on data obtained from sensors placed inside intelligent modules.

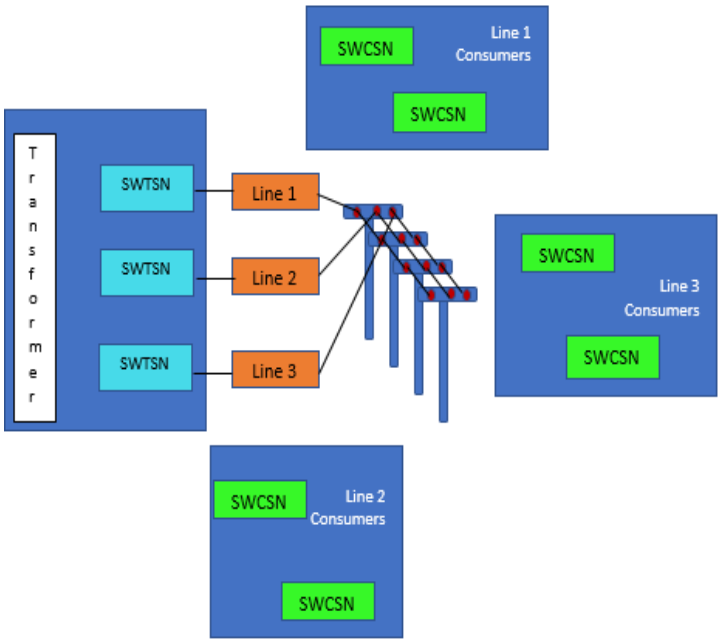

Fig. 1. Architecture of Smart Grid [3]

978-1-5090-6621-6/17/$31.00 ©2017 IEEE

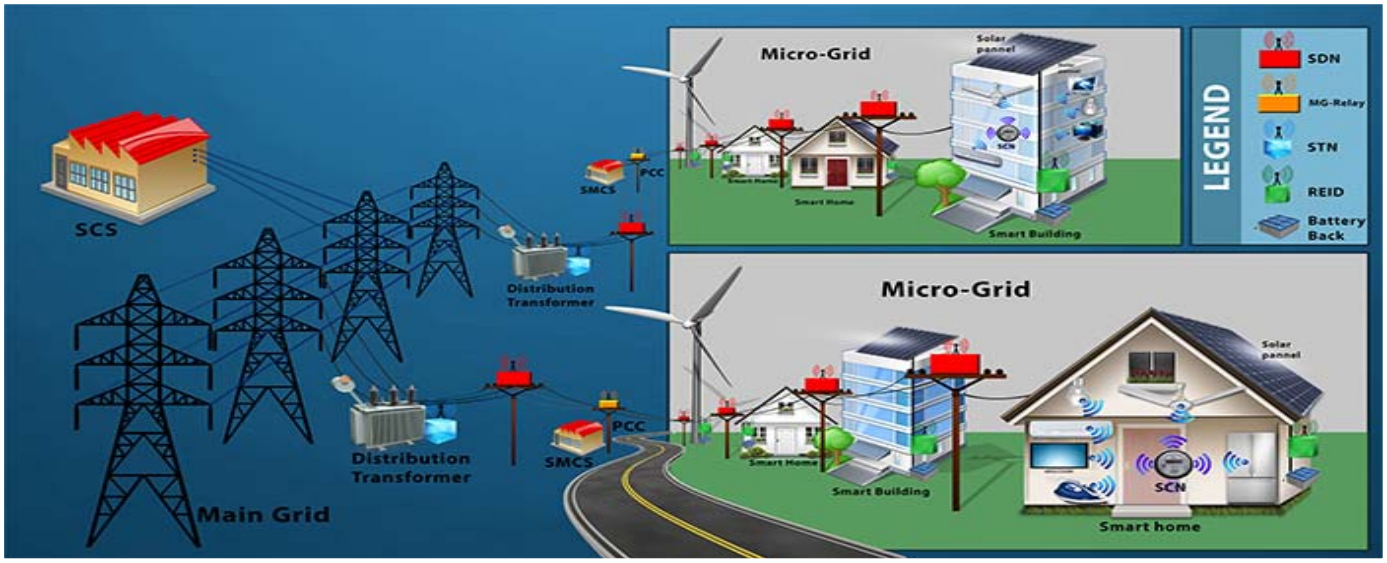

Fig. 2. Schematic structure for Micro Grid [10]

The rest of the paper describes about the vulnerabilities and the solutions - the personal privacy of users using the Micro Grid technology, the protection against corruption and destruction of information, guaranteeing the origin and termination of the data, reliability and timeliness of the data access, and authenticity and validity of data which is stored.

Section II describes the state of the art of security issues in Micro Grid. Sections III and IV explain the security and privacy challenges in the Micro Grid infrastructure and solutions to them. Section V, finally, describes the conclusion of the work and future work that can be incorporated.

II. Related Work

The authors of [3] have introduced Smart Grid architecture to be implemented in India. This paper emphasizes on the need for power grid in India which constitutes electricity generation, power transmission, distribution and provisioning system. According to the authors, the considered scenario is the power generation in a remote location, like banks of natural water bodies, and distribution of power in a wide area to far away locations such as urban or semi-urban regions where power consumption is high due to the presence of factories and buildings. With the introduction of technologies like smart buildings, smart homes and smart enterprises, the power system is to be upgraded to adapt to such new innovative solutions. This results in Micro Grid, sister of Smart Grid.

They can be considered as a single functioning unit or as a part of Smart Grid. Work [3] brings out architecture for Smart Grid. Work [2] gives an in-depth knowledge of major problems faced by power grids today such as line faults and provides an algorithm as a solution for this issue. This paper proposes another unique architecture for a 3-phase isolated Micro Grid architecture. But this paper focuses only on the fault detection and isolation. A real-life implementation of can have lot more security issues and challenges. Work [1] by same authors gives a pictorial view of the Micro Grid infrastructure for power theft detection. Work [4] highlights the risk of unnecessary disturbances or blackouts in Smart Grid, prospective knowledge of failure and corresponding solutions. This paper provides an analysis of network protection and emphasizes the importance of predicting failure in power and take necessary actions.

Micro Grid is one of the real-life implementations of wireless sensor network (WSN). Work [5] takes the reader through different types of attack a WSN system can face and corresponding counter measures to resolve them. Work [6] also explains the general attacks on a WSN and its solutions. Papers [7] [8] and [9] provide solutions to some basic attacks on the WSN system.

III. Types of Security Attack on Micro Grid

Each element in Micro Grid design is prone to attack. The attack can be harmful in terms of human injury and economical loss. As each component in the architecture carries vital information, attack on any one component can cause leakage of confidential data. Some of the possible attacks based on the components are listed below.

Components highly prone to attack are:

- Intelligent Module (Distribution Pole)
- Wireless Communication module between control station and other components
- Main Grid
- Smart Meter

The main component of the micro grid system is the Intelligent Module (IM). The main function of this module is to monitor the distribution pole. IM constitutes current sensor, voltage sensor to continuously monitor current and voltage condition at each phase line. The processor checks the value from sensor and compares with a preset threshold value. If it exceeds the threshold, circuit breaker opens the line circuit. One

of the possible attacks on this module is the "Man-in-the-Middle" attack where the attacker stays in the middle of sensor and microcontroller. It can change the sensor data. If the current flow is beyond a threshold limit, there is a high chance for electric appliances to explode or people to get electric shock. If the attackers tamper with the microcontroller to change the value, the circuit breaker will not break the line circuit leading to major electric accidents resulting in human loss. Interference or noise insertion in the output of current or voltage sensor can also lead to improper functioning of circuit breaker.

If the attacker attacks the microcontroller, where the threshold comparison is done, proper decision-making fails. For example, if the threshold value for voltage was set to V volts [10], the attacker by some means changes the value to V` volts. Once a higher voltage that can lead to accident or electric shock reaches the microcontroller for threshold comparison, it gets compared with the fake V` volts instead of V volts thus giving a false response leading to electric shock for the customers using the Micro Grid system.

Circuit Breaker [12] is a switching device used to protect the device or electrical circuit from damage due to excess current which can be caused by a short-circuit in an overload condition. One of the security attacks that a circuit breaker can be a victim of is if someone deliberately planted a faulty circuit breaker in the circuit breaker system resulting in an "inappropriate-access-by-an-unauthorized-personnel".

ZigBee is the communication module used in this Micro Grid design. Another security threat that can occur in this system is in the wireless connectivity. ZigBee, can also be a victim of communication related attack. The main attacks related to ZigBee are the jamming attack and Denial of Service attack (DoS) [9].

Smart Controlling Station (SCS) is the center of Micro Grid architecture where the billing and data storage takes place. The confidentiality and integrity [16] of data is the prime factor in SCS. The data stored in the SCS should be secured in terms of programming, hardware components and communication protocols. Data confidentiality prevents unauthorized disclosure. If confidentiality is maintained, it will ensure the trust, dignity and respect of the users.

IV. Solutions to the Possible Attacks

Component wise solution description is a better approach for the Micro Grid system. One solution can be applied to more than one issue.

One of the major attacks in Micro Grid is DoS attack. Some malware like Trojan can be installed on the router located in the communication network or disproportionately large files uploaded to the network. This can be prevented by using proper security firewalls, to differentiate between legitimate and malicious traffic. Also increasing bandwidth of the communication system can limit the DoS [9] attack up to an extent. In a replay attack, a valid data transmission is normally repeated or delayed. By using One Time Password (OTP) or time stamp on the data or using a message authentication code, the replay attack can be protected.

Jamming attack affects the communications channels of ZigBee. The state estimation, online checking and billing get impacted. Jamming attack is difficult to prevent. DSSS spread spectrum technique can be used as a counter measure. The secret pseudo random noise codes are known to only the communication parties. The ZigBee system is using128 bit AES encryption standard [18]. The standard encryption algorithms and authentication mechanisms in the communication system can improve the integrity and confidentiality. This cryptographic encryption technique [8] can prevent several issues related to confidentiality. The key exchange mechanism is the best solution to improve confidentiality in the entire network.

Man in the middle (MITM) attack happens when the sensor data to the microcontroller get altered. End to end reliability is an important factor in wireless communication systems. For this, several reliable protocols are designed specifically for wireless sensor networks. Typically, reliability of the transport layer is assured with acknowledgment (ACK) and negative acknowledgement (NACK) feedback mechanisms. While ACK is vulnerable to reliability attacks, NACK based protocols are only susceptible to energy depleting attacks [19]. To avoid MITM use of NACK based protocols can be used.

V. Conclusion & Future Work

The Micro Grid architecture discussed in [1] an [2] is vulnerable to many of the security and privacy challenges. In this work, these issues are discussed component wise. The solutions for each problem are explained in detail. Since Micro Grid is a unit of Smart Grid, the analysis of Micro Grid can be beneficial in case of scalability. To maintain the three key factors, confidentiality, integrity and availability in the Micro Grid architecture it is necessary to follow the security measures.

VI. Acknowledgment

The authors gratefully recognize the motivation and immense support provided by our Chancellor, Dr. Mata Amritanandamayi Devi, for writing this paper.

VII. References

[1] A. R. Devidas and M. V. Ramesh, "Power theft detection in Micro Grids," 2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), Lisbon, Portugal, 2015, pp. 1-8.

[2] M. V. Ramesh, N. Mohan and A. R. Devidas, "Micro grid architecture for line fault detection and isolation," 2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), Lisbon, Portugal, 2015, pp. 1-6.

[3] A. R. Devidas and M. V. Ramesh, "Wireless Smart Grid Design for Monitoring and Optimizing Electric Transmission in India," 2010 Fourth International Conference on Sensor Technologies and Applications, Venice, 2010, pp. 637-640.

[4] J. Fuchs and J. Jaeger, "Smart grid study on protection security issues," *IEEE PES ISGT Europe 2013*, Lyngby, 2013, pp. 1-5.

[5] Tarek Azzabi, HasseneFarhat, Nabil Sahli, "A survey on wireless sensor networks security issues and military specificities", Advanced Systems and Electric Technologies (IC_ASET) 2017 International Conference on, pp. 66-72, 2017.

[6] A. Rani and S. Kumar, "A survey of security in wireless sensor networks," 2017 3rd International Conference on Computational

Intelligence & Communication Technology (CICT), Ghaziabad, 2017, pp. 1-5.

[7] H. N. Dai, H. Wang, H. Xiao, X. Li and Q. Wang, "On Eavesdropping Attacks in Wireless Networks," 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), Paris, 2016, pp. 138-141.

[8] M. H. Ahmed, S. W. Alam, N. Qureshi and I. Baig, "Security for WSN based on elliptic curve cryptography," International Conference on Computer Networks and Information Technology, Abbottabad, 2011, pp. 75-79.

[9] R. S. Singh, A. Prasad, R. M. Moven and H. K. Deva Sarma, "Denial of service attack in wireless data network: A survey," 2017 Devices for Integrated Circuit (DevIC), Kalyani, India, 2017, pp. 354-359

[10] https://www.amrita.edu/research/project/micro-grid-complete-solution-rural-area-electrification

[11] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2763825/

[12] https://www.electrical4u.com/electrical-circuit-breaker-operation-and-types-of-circuit-breaker/

[13] http://wnss.sv.cmu.edu/teaching/14814/s17/schedule.html

[14] Jyrki T. J. Penttinen, "Security Risks in the Wireless Environment," in Wireless Communications Security:Solutions for the Internet of Things , 1, Wiley Telecom, 2015, pp.336.

[15] A. N. Rukavitsyn, K. A. Borisenko, I. I. Holod and A. V. Shorov, "The method of ensuring confidentiality and integrity data in cloud computing," 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, 2017, pp. 272-274.

[16] T. P. Thao, A. Miyaji, M. S. Rahman, S. Kiyomoto and A. Kubota, "Robust ORAM: Enhancing Availability, Confidentiality and Integrity," 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), Christchurch, 2017, pp. 30-39.

[17] J. F. C. Joseph, A. Das, B. C. Seet and B. S. Lee, "Cross Layer versus Single Layer Approaches for Intrusion Detection in MANETs," 2007 15th IEEE International Conference on Networks, Adelaide, SA, 2007, pp. 194-199.

[18] David Boyle, Newe Thomas, "Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, vol. 3, no. 1, JANUARY 2008.

[19] https://pdfs.semanticscholar.org/100e/c41e726ca5e4b7ee50fd2f3ade7224e66e9.pdf