Efficient Electricity Theft Identification and Notification Mechanism Using Modified Consensus Based Algorithm

Vasanth V,
UG Scholar, Department of IT, Velammal Engineering College, Chennai.
Email: vasanthv1901@gmail.com
Udaya Raja S,
UG Scholar, Department of IT, Velammal Engineering College, Chennai.
Email: udayaraja98@gmail.com
Ahamed Ali S
Associate Professor, Department of IT, Velammal Engineering College, Chennai.
Email: haiahamed@gmail.com

ABSTRACT

This paper introduces a data integrity attack on the well-developed consensus-based energy management algorithm. We have a tendency to show that by causation out intricately falsified information during the consensus iterations, attackers could manipulate the system in operation purpose and gain further economic benefits.This data integrity attack has two major features: 1) Attackers solely deem native info to complete the attack, no additional information about system topology nor extra colluders area unit required; 2) The assaultive effect is accumulative, that permits attackers to decide on to end in either single or multiple iterations. It conveys the message that besides the efforts of designing novel distributed energy management algorithms to address the renewable energy integration challenges, it's equally important to protect the distributed energy management algorithms from possible malicious attacks to avoid potential economic losses.

Keywords - **Consensus algorithm, Energy management,Distributed Control, Power system security, Data Integrity attack**

I. INTRODUCTION

To maintain a balance between optimizing the use of resources and the real-time control requirements for keeping the frequency and voltage of the power grid at their design levels, the power grid uses a daily and hourly scheduling of generation units to match the forecast electricity load via wholesale market transactions. A scheduling coordinator solicits generation through some form of auction where lowest bidders generate electricity and this in turn creates an economically optimal schedule of generators. In contrast to these traditional wholesale markets (e.g., between generation utilities and distribution utilities), many retail markets (e.g., between a distribution utility and an industry consumer of electricity) have traditionally adopted static pricing schemes such as fixed and time-of-use tariffs, under which consumers have limited incentives to adapt their electricity consumption to market conditions.This lack of incentives results in high peak demands that strain infrastructure capacities and unnecessarily increase operational costs.This approach is inefficient, since the system infrastructure used to guarantee supply under peak hours is not completely used most of the time. According to the Energy Department of India, 10% of the whole generating capacity and 25% of distribution capacity is used less than the 5% of the time.

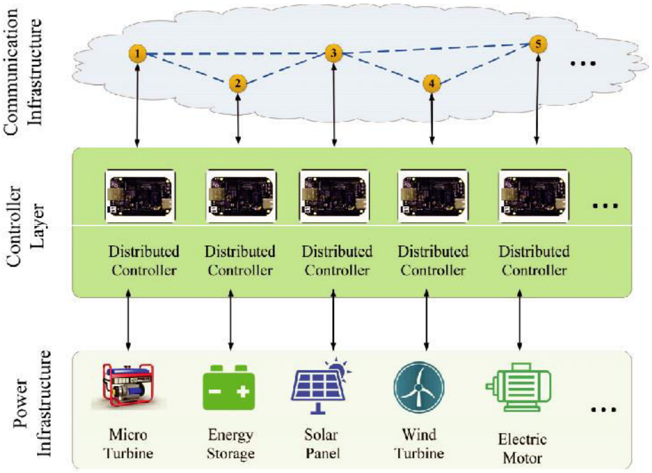


Fig 1: Smart grid architecture with consensus-based applications

The algorithm could coordinate locally to guarantee the important information to be shared in a distributed way. Compared with centralized control framework, which might be subjected to performance limitations, such as computation burden, limited flexibility and scalability, the consensus-based approaches are promising in large-scale coordination problems.

The consensus-based applications require physical operations with the computation, communication and control functionalities realized by a cyber system. Fig. 1 presents a typical smart grid architecture with consensus-based applications from the cyber-physical perspective. The physical devices are embedded with distributed controllers. The distributed controllers acquire measurements from and issue commands to the local devices. To achieve the overall goal of the smart grid, i.e., economics and efficiency of the system operations, the distributed controllers coordinate with neighboring devices through peer to peer communication and share important information over the communication network. Implementations of consensus-based applications could be found in [8]. However, most of the consensus-based distributed approaches assume that distributed controllers behave normally and communicate with neighbors honestly, which may not necessarily be true in real-world scenarios.

Some recent literatures begin to assess the impact of data integrity attacks on consensus-based applications and illustrate data integrity attacks on consensus-based economic dispatch algorithms. In, malicious generation units share false incremental cost information to disturb the convergence of the consensus algorithm and break the balance between the generation and demand. In, malicious generation units inject false generation cost parameters, to increase the total generation cost and decrease the generation efficiency. It introduces a data integrity attack on cooperative control of virtual power plant (VPP). A malicious distributed generator (DG) shares false utilization ratio to mislead other DGs, with the objective to increase its own income. However, the aforementioned attacks cause the imbalance between the generation and demand, which breaks down the normal operation and can be detected easily. An interesting problem is to investigate whether the attacker can increase own benefit without violating physical constraints.

This paper presents efficient electricity theft identification and notification mechanism using modified consensus based algorithm.

- By sending out manipulated local information, attackers mislead the normal devices to achieve a false estimation of the total loads. While the normal devices manage to meet the falsified load condition, the attackers charge/discharge secretly, and make extra benefits while keeping the system stable.
- Attackers do not need global information about system topology or about other buses to launch the attack. Merely relying on the given local information, the attacker could elaborately design false information to share with neighbors, and mislead the system to a false operating point.
- The attacking effect is accumulative. The malicious objective could be accomplished in either one iteration or multiple iterations. Thus, attackers have a choice to design various attacking strategies to achieve the same goal.

II. Consensus Based Distributed Energy Management Algorithm

2.1 Problem Formulation

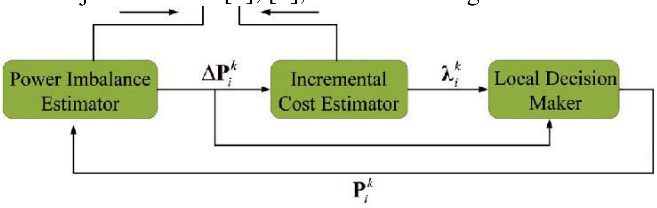
Energy management problem is one of the fundamental problems in power system, which determines the operating point of the power network that minimizes a certain objective, such as generation cost or power loss. In this paper, we use a microgrid consisting of a set of renewable resources. The energy management problem is formulated as an offline optimization problem, to minimize the electricity bill over the time.At every time state, the power generation and load should be balanced . The power commands must be within maximum and minimum limits defined by device characteristics. Constraint states that at every step, the energy stored in the should be within the maximum capacity limit and minimum capacity limit. The storage capacity limits in the form of power commands.

For a given storage device , the dynamic model could be modeled as

- State of charge balance equation: the dynamics of the stored energy between two consecutive time steps.
- Capacity Constraint: the stored energy is bounded by the maximum and minimum capacity of the energy storage device.

2.2 Consensus-based Distributed Approach

As is shown in Fig.1, each device is embedded with a distributed controller. The consensus-based approach is an iterative method, at every iteration , controller performs three major functions [3], [4], as shown in Fig. 2.



The consensus-based distributed approach is summarized as:

- Power imbalance estimator: Each device communicates with neighbors and updates its local power imbalance estimation.
- Incremental cost estimator: According to the economic dispatch criterion, the incremental cost for all devices must be equal to reach the same incremental cost.
- Local decision maker: The local estimations are used to adjust the power commands. The power is moved in the opposite direction of the gradient of the Lagrangian function.

The consensus-based power imbalance estimator enables controller to estimate the actual system power imbalance in a collective sense.The actual system power imbalance the difference between the power and supply. The collective power imbalance estimation at some iteration is the summation of local power imbalance estimation over all devices. If all the controllers follow and share information with the neighbors, then at every iteration, the collective power imbalance estimation equals to the actual system power imbalance. Every term in the summation has its opposite counterpart.

III. DATA INTEGRITY ATTACK MODEL

We consider one of the controllable devices, i.e. a storage device, becomes malicious. Instead of cooperating with other devices to minimize the total electricity bill, the objective of attacker is to follow the most profitable schedule for itself, without breaking down the system.

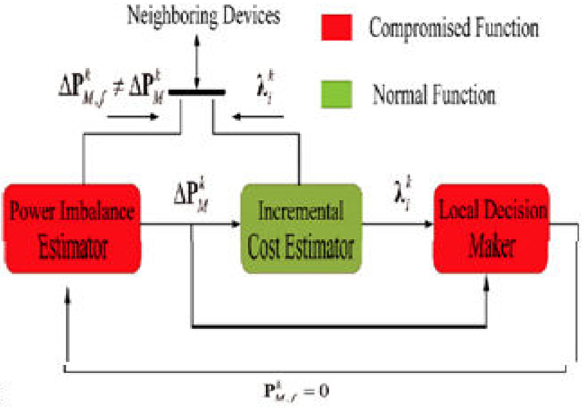
There are two assumptions for the system setup: i) All the devices know electricity price. ii) microgrid buys/sells power from/to the storage devices at the same rate as the electricity price. To fulfill the malicious objective, attacker executes two major steps. The details are discussed below.

3.1 Determining the Most Profitable Schedule

From attacker 's perspective, the most profitable schedule is to maximize the electricity profit by charging and discharging during particular time steps while considering its physical limits.

3.2 Compromising the modified consensus-based update rule

Two functions in the consensus-based update rule are compromised, as shown in Fig.3.



|

3.3 Modules

- User registration and login
- Normal Energy Consuming
- Attack detection (occur on user screen)
- Bill generating
- Sending mail to user

IV. THE MODULES INVOLVED IN THIS PROJECT ARE

4.1 User registration and login

Once user registered sign up page it will directly enter into the login page for validation once validation had completed it will redirected into website.

4.2 Normal Energy Consuming

The grid will send the energy to resources each and every resource consuming the equal energy.

4.3 Attack detection (occur on user screen)

Attack detection technique helps to find the attack detection. If someone has hacked your account alert will be produced to user account. So that we can easily identify account pricing details.

4.4 Bill generating

Process of state estimation helps to find out the normal bill for consuming energy of user with the help of existing records.

4.5 Sending mail to user

The copy of the bill will be produced to the user through mail for the secondary verification process.

V. SYSTEM STUDY

5.1 Existing System

For existing system user cannot get proper report because they couldn't find out where the account has hacked, where the prices advertised to smart meters are compromised by scaling factors(so consumers use the wrong prices)and by corrupted timing information.

5.3 Drawbacks

- Security and privacy cost
- Two way communications can be hacked
- Smart grid is computer based if it is hacked then worst thing will happen

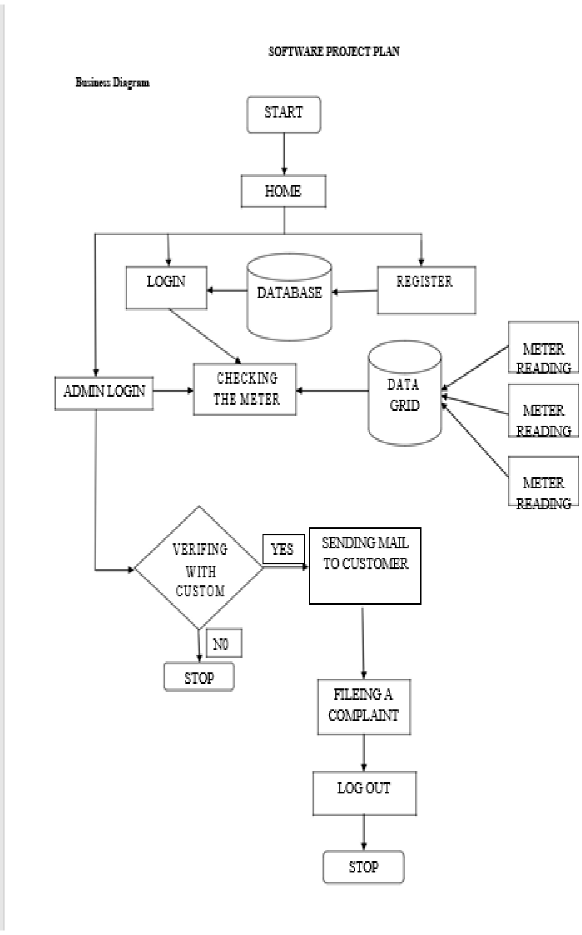
5.4 Proposed System

There are attacks being made by hackers through the internet in the electricity bills to increase or decrease the price of the bill to the users. Now the attacks can be identified and thebills can be checked through the data grid.

The real price of the bill can be identified by the users by themselves through this project.

5.5 Advantages

- Enhanced reliability
- Reduce peak demand
- Multiple, decentralized energy sources
- Lower total energy consuming
- Smarter consumers



VI. Feasibility Study

Feasibility study is the initial design stage of any project, which brings together. The elements of knowledge that indicate if a project is possible or not.

An important outcome of the preliminary investigation is the determination that the system requested is feasible. Feasibility study is carried out to select the best system that meets the performance requirements.

Feasibility study is both necessary and prudent to evaluate the feasibility of the project at the earliest possible time. It involves preliminary investigation of the project and examines whether the designed system will be useful to the organization. Months or years of effort, thousand for millions of money and untold professional embarrassment can be averted if an in-conceived system is recognized early in the definition phase.

The different types of feasibility are: Technical feasibility, Operational feasibility, Economical feasibility.

6.1 Technical Feasibility

Technical Feasibility deals with the hardware as well as software requirements. Technology is not a constraint to type system development. We have to find out whether the necessary technology, the proposed equipment's have the capacity to hold the data, which is used in the project, should be checked to carry out this technical feasibility.

The technical feasibility issues usually raised during the feasibility stage of investigation includes these

- This software is running in windows 2000 Operating System, which can be easily installed.
- The hardware required is Pentium based server.
- The system can be expanded.

6.2 Operational Feasibility

This feasibility test asks if the system will work when it is developed and installed.

Operational feasibility in this project:

- The proposed system offers greater level of user-friendliness.
- The proposed system produces best results and gives high performance. It can be implemented easily. So, this project is operationally feasible.

6.3 Economic Feasibility

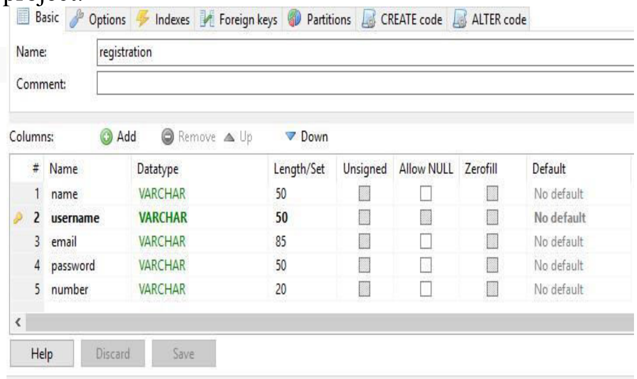
Economic Feasibility deals about the economic impact faced by the organization to implement a new system. Financial benefits must equal or exceed the costs. The cost of conducting a full system, including software and hardware cost for the class of application being considered should be evaluated.

Economic Feasibility in This Project

- The cost to conduct a full system investigation is possible.
- There is no additional manpower requirement.
- There is no additional cost involved in maintaining the proposed system.

VII. Result and Discussion

The following are some of the samples results of our project.



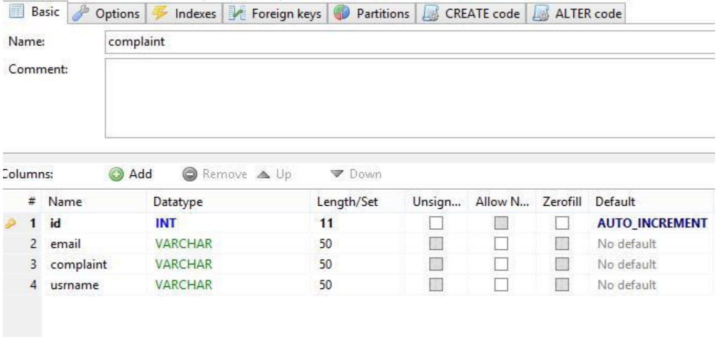
Name: registration

Comment:

Columns:

#	Name	Datatype	Length/Set	Unsigned	Allow NULL	Zerofill	Default
1	name	VARCHAR	50	□	□	□	No default
2	**username**	**VARCHAR**	**50**	□	□	□	**No default**
3	email	VARCHAR	85	□	□	□	No default
4	password	VARCHAR	50	□	□	□	No default
5	number	VARCHAR	20	□	□	□	No default

Fig 1 :Registeration form.



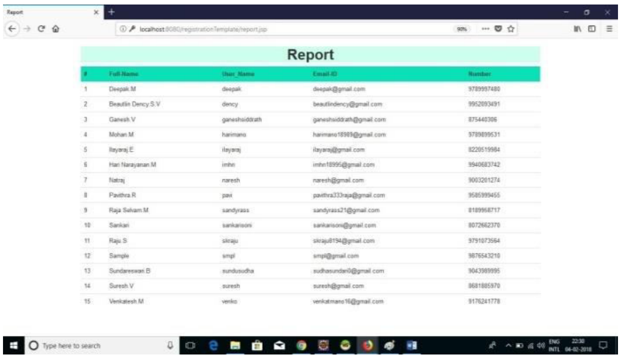
Name: complaint

Comment:

Columns:

#	Name	Datatype	Length/Set	Unsign...	Allow N...	Zerofill	Default
1	**id**	**INT**	**11**	□	□	□	**AUTO_INCREMENT**
2	email	VARCHAR	50	□	□	□	No default
3	complaint	VARCHAR	50	□	□	□	No default
4	usrname	VARCHAR	50	□	□	□	No default

Fig 2 :Bill form



Report

#	Full-Name	User_Name	Email-ID	Number
1	Deepak.M	deepak	deepak@gmail.com	9789997480
2	Beautlin Dency.S.V	dency	beautlindency@gmail.com	9952093491
3	Ganesh.V	ganeshsiddrath	ganeshsiddrath@gmail.com	875440306
4	Mohan.M	harimano	harimano18989@gmail.com	9789899531
5	Ilayaraj.E	ilayaraj	ilayaraj@gmail.com	8220519984
6	Hari Narayanan.M	imhn	imhn18995@gmail.com	9940683742
7	Natraj	naresh	naresh@gmail.com	9003201274
8	Pavithra.R	pavi	pavithra333raja@gmail.com	9585999465
9	Raja Selvam.M	sandyraas	sandyraas21@gmail.com	8189958717
10	Sankari	sankarisoni	sankarisoni@gmail.com	8072662370
11	Raju.S	skraju	skraju8194@gmail.com	9791073564
12	Sample	smpl	smpl@gmail.com	9876543210
13	Sundareswari.B	sundusudha	sudhasundari0@gmail.com	9043989995
14	Suresh.V	suresh	suresh@gmail.com	8681885970
15	Venkatesh.M	venko	venkatmano16@gmail.com	9176241778

Fig 3: Report form

s.no	Test Scenario	Expected Result	Test Result
1	Usemame is available. Full Name. Email ID is valid. Mobile Numberis valid. Password is valid. Confirm passwordmatch.	Registration Successf ul.	Registration Successfu l.
2	Usemame is not available. Full Name. Email ID is valid. Mobile Number is valid. Password is valid. Confirmpasswordmatch.	Usemane not available.	Usemamenot available.
3	Usemame is available. Full Name. Email ID is invalid. Mobile Number is valid. Password is valid. Confirm passwordmatch.	Invalid Email ID.	Invalid Email ID.

VIII. Future Enhancements

An attack-detection algorithm based on the CUSUM technique and evaluates its effectiveness to identify attacks for different controller parameters, and different attack frequencies. Able to identify the trade-off between time of detection, frequency of the attack, and number of false alarms. Moreover, it is possible to define an attack that cannot be detected, but whose effect in the network is low due to the proposed detection method. This detection technique really useful for consumers to find the accurate reports. Whenever the attack has occur consumer will get the alert mail. It's easy to identify where the attacks has occur so that we can easily make complaints.

IX. Conclusion

The theory from sensitivity analysis to understand how previously proposed attacks could be generalized and evaluated in a formal setting. Particularly showed how to find better attacks than previously proposed, and how to design robust control systems that can mitigate a large number of attacks. And also found that the design of the price adjustment mechanism is fundamental in the resiliency of the system. The possible attack strategies that can be achieved by combining attacks to both: sensors and control signals. The models are assumed that the attacker compromised the price signals, but not both. It is clear that if the attacker controls all control signals and all sensor signals then there is nothing we can do, but if the attacker has partial compromise of controllers and sensors, then the defender might still be able to design a robust algorithm that attenuates the attacks.

References

[1] R. Tan, V. B. Krishna, D. K. Y. Yau, and Z. Kalbarczyk, "Impact of integrity attacks on real-time pricing in smart grids," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, Berlin, Germany, 2013, pp. 439–450.

[2] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in Proc. 16th ACM Conf. Comput. Commun. Security, Chicago, IL, USA, 2009, pp. 21–32.

[3] D. Mashima and A. A. Cárdenas, "Evaluating electricity theft detectors in smart grid networks," in Research in Attacks, Intrusions, and Defenses (RAID). Berlin, Germany: Springer-Verlag, 2012, pp. 210–229.

[4] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in Proc. IEEE 1st Smart Grid Commun. Conf. (SmartGridComm), Gaithersburg, MD, USA, 2010, pp. 214–219.

[5] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," IEEE Trans. Autom. Control, vol. 60, no. 4, pp. 1145–1151, Apr. 2015.

[6] L. R. Phillips et al., "Analysis of operations and cyber security policies for a system of cooperating flexible alternating current transmission system," Sandia Nat. Lab., Albuquerque,NM, USA, Tech. Rep. SAND2005-7301, Dec. 2005.

[7] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in Proc. IEEE Power Energy Soc. Gen. Meeting, San Diego, CA, USA, 2011,

[8] pp. 1–6.

[9] M. Vrakopoulou, P. M. Esfahani, K. Margellos, J. Lygeros, and G. Andersson, "Cyber-attacks in the automatic generation control," in Cyber Physical Systems Approach to Smart Electric Power Grid. Berlin, Germany: Springer-Verlag, 2015, pp. 303–328.

[10] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 580–591, Mar.2014.