Trust and Reputation Approach to Smart Grid Security

Omkar Pradhan, Muhammad Awan, *Student Member, IEEE*, Kimberly Newman, *Senior Member, IEEE*,
and Frank Barnes, *Fellow, IEEE*
Department of Electrical, Computer, and Energy Engineering
University of Colorado
Boulder, CO 80309
Omkar.Pradhan@colorado.edu, Muhammad.Awan@colorado.edu,
Kimberly.Newman@colorado.edu,Frank.Barnes@colorado.edu

***Abstract*—The electric grid in the US is aging and needs to be upgraded. Solutions involve the use of equipment with wireless communication capability for monitoring of generation, transmission and distribution. These systems introduce vulnerabilities to attack that can lead to blackouts and damage to equipment. In order to increase the reliability of the power systems, it is important to detect sources of risk at the system and individual level. The approach described in this paper applies trust and reputation management at the home based meter to detect when false reports occur.**

Keywords-smart grid; risks; trust and reputation management; smart meters

I. INTRODUCTION

Smart metering is a critical component of the emerging power grid but there are new vulnerabilities associated with the use of this technology that need to be addressed in a proactive manner as systems are being deployed. Theft of service needs to be detected and mitigated in a timely manner so it does not damage the power delivery to large areas of the grid and potentially cause blackouts. Vulnerabilities in the supervisory control and data acquisition (SCADA) system show that this can occur [1]. Due to these vulnerabilities at the system level, the U.S. Department of Energy (DOE) wants to have "attack resilience" as a primary requirement for the smart grid [2].

Risks need to be determined and prioritized so that appropriate solutions can be formed without violating the privacy of honest users. One approach is to place weights on each layer of the system to reduce vulnerability to attack. Metrics are then applied to determine if the equipment is compromised and acting in a selfish or malicious manner. Appropriate measures are then put in place to limit the impact of the compromised equipment while repair or replacement is dispatched. This method is described in [2]. Another approach is to create infrastructure to evaluate the trustworthiness of a device. This leverages the area of trust and reputation management (TRM) from the social sciences [3] and uses methods from wireless communication deployments to evaluate system component activities. This approach is describe for policy management at the system level in [4] and demonstrates the applicability of trust monitoring for power systems.

The focus of this paper is to evaluate the individual level of trust needed in advanced metering infrastructure (AMI). The reputation of a meter is determined based on reporting of usage versus actual usage that is assessed through capture of load information in the neighborhood as well as supervisory evaluation of meter performance. If the reputation of a meter decreases, then additional supervision is provided to reduce fraud in the system while punitive action is taken to discourage the behavior. The following sections provide detailed descriptions of risks associated with smart grid deployments, discuss TRM methods as they relate to power systems, and provide a simulation with results for the initial evaluation of TRM in AMI equipment. Future directions and conclusions are also provided.

II. SMART GRID OVERVIEW

Restructuring of the power grid is creating opportunities for improvements in generation, transmission, and distribution of energy. The grid is becoming smart so that power companies may now incorporate sensor technologies at all levels to provide the means to auto-balance and prevent large scale faults [5]. Communication with the home is another improvement provided by the smart grid so that consumers within a home area network (HAN) may regulate usage patterns through monitoring of supply costs and scheduling of loads throughout the day. However, the ideal does not always match the reality. Privacy issues are just now being discussed as the power companies are gaining access to a great deal of personal information previously not available for monitoring [6]. Malicious users may also gain access to private information so enhanced security is necessary for the protection of individual usage patterns.

An overview of HAN technologies is provided by Huq and Islam [7]. The basic components of the HAN are the network portal or gateway, the access point or network nodes, the network operating system and network management software, and the endpoints. Communication between these points is possible with Zigbee, Z-Wave, Wifi, HomePlug, and Ethernet. Wireless communication increases risk of theft of information as well as misuse of equipment through corruption of the software. Understanding of the tradeoffs in security versus control of consumption is important as the smart grid is growing. An educated consumer can then determine what deterrents are necessary to maintain privacy while having greater access to information.

III. RISKS IN SMART GRID

Vulnerabilities occur at the system level and individual level. For the power grid, vulnerabilities in SCADA systems need to be understood and mitigated [1] to limit risk at the system level. However, evaluation of system wide vulnerabilities are beyond the scope of this paper. Risks are also present throughout the generation, transmission, and distribution of energy at the component level.

Control systems are extensively used in Electric Grids. For these systems to operate properly, the integrity of the data must be accurate and trustworthy [8]. In this context, trust is used to ensure appropriate users access accurate data using expected protocols and expected devices. It is also assumed the data transmitted to the grid is not modified. False data in a control

978-1-4244-9293-0/11/$26.00 ©2011 IEEE

loop can lead to damage to equipment very quickly since the operating margins for large scale motors are tightly constrained.

Another important asset of smart grids are phasor measurement units (PMUs). Currently there are 200 PMU's installed in the US [9]. PMUs collect and relay data of grid conditions at 60 samples per second as compared to SCADA which collects data every 5 seconds. In a synchrophasor system [10,11] the major components are PMUs, and communication links which send data to local data concentrator for PMUs. The concentrated data is then sent back to the utility owned phasor data concentrator (PDC). This data is used for real-time grid state estimation for planning grid systems. Hence due to the nature of data usage, this data must be transmitted over secure links. Also since the data is used for grid planning and operation, it must be trusted and secure data.

In order to protect the data and communication links in the emerging smart grid, characterization of the types of risks that can occur needs to be performed. Natural events such as snow or strong winds develop over time but malicious attacks aimed at weakening the system occur spontaneously. The worst case scenario is what occurred in the Columbia Electric Grid. Guerrilla attacks occurred on the power grid resulting in substantial supply problems. From 1999-2002 there were between 250-450 attacks on high-tension towers each year that created several isolated regions [12]. These attacks on the power lines and transformers resulted in disruption in electricity as well as mechanical failures in the system. In the approach presented by León et. al. in [12], a two layer wireless sensor network (WSN) is used to monitor the mechanical health of the transmission network. Hot spots in conductors as well as tilt and vibration in towers are monitored using temperature and accelerometers to detect damage due to manmade or natural disasters. However, devices placed on distribution systems to monitor risk are also vulnerable to soft attacks through the communication channel. Unsecured devices can report false information on the status of the infrastructure so protection is necessary for the detection of physical attacks as well as cyber based threats.

Once the characteristics of the equipment are known and the categories of threats with the highest risk and probability of occurrence are determined, algorithms can then be devised to protect the smart grid from vulnerabilities.

IV. Trust and Reputation Management

Types of trust in wireless communication are subjective, context sensitive, and unidirectional [14]. There are two main models which are socio-cognitive and computational. Each of these models involves evaluation of the credibility of the source of information and builds a reputation over time. Implementation of these models is performed at the individual level and system level. For the evaluation of AMI, emphasis is on the individual level to determine malicious and selfish use. At such a level devices in the AMI system are commonly called Smart Meters.

In the socio-cognitive model of trust, there are seven components identified to determine trust. These are willingness, self-confidence, persistence, motivation, disposition, dependence, and competence. The belief-desire-intent (BDI) model of mental states is implemented for this cognitive analysis [15] and a cross-correlation of the seven components is performed to determine trust. Evaluation is rather complex and Fuzzy Cognitive Maps (FCM) have been used to implement this type of model [16,17].

Computational trust models are far less complex to implement than socio-cognitive models. However, it is not clear if they are more robust. They involve the use of game theory and evolution of strategies over the course of multiple interactions. The boundary between trust and credibility is blurred with some approaches used in computational trust implementation since first hand info is better than second hand witnesses.

V. TRM Evaluation for AMI

Automated metering using smart metering devices offers many benefits as well as increased vulnerabilities in the emerging Smart Grid due to the addition of a digital communication layer. The focus of this study is to characterize selfish and malicious reporting of power usage from smart meters installed with individual customers so that the impact of a "bad apple" is minimized. As shown in figure 1, the red houses are reporting bad data and the "patrolman" is dispatched to check the actual values from the smart meters for the detection of fraud. Data from each of the home based AMI devices is sent to the data concentrator unit (DCU). The DCU is a data aggregation device in the AMI system. For the purpose of this study the DCU is assumed to be tamper-proof

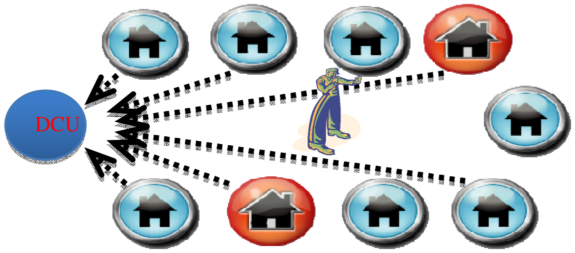

Fig. 1: AMI Trust Evaluation

A mathematical solution is proposed to utilize trust management methodologies to determine when false data is reported.

Let,

- *i = 1,2,…,9* denote house indexes.
- *E(i,t)* is the true electricity usage of house *'i'* at time *'t'*
- *S(i,t)* is the usage reported by 'Smart Meter' of house *'i'* to the DCU at time *'t'*.
- *T(t)* is the total usage of all houses as recorded at the substation at time *'t'*.
- $e(t) = T(t) - \Sigma\, S(i,t)$ is the error seen at the DCU.
- $Me(i,t) = \frac{|E(i,t)-S(i,t)|}{e(t)}$ is the marginal contribution of house *'i'* to the total error. *'Me(i,t)'* is used to correct smart meter data.
- *E(i,t)* is only reported when Agent visits house *'i'*.
  If house 'i' is reporting usage data incorrectly
  $S(i,t) \neq E(i,t)$ for some *' t '*

A. Assumptions

- All the houses are assumed to be serviced by the same distribution substation.
- Total usage of all houses can be measured at the substation and this is tamper proof.

B. Model

- Electrical energy usage data of 9 houses at 5 minute intervals year is used. (yearly)
- The houses are classified as Low, Average & High (3 of each) based on income.

C. The Patrolman

- The patrolman is a hypothetical polling instrument.
- One out of the 9 houses is visited according to a probability distribution.
- The patrolman is able to poll the house visited, for 'true' data along with the 'smart meter' data.
- The Patrolman has access to the following information: *S(i,t)* and *E(i,t)* i.e. usage of house *'i'* reported by 'Smart Meter' installed in house *'i'* and true electrical usage of house *'i'* at time *'t'*.
- A *'mistrust'* table is built for each house from the patrolman's report.
- The mistrust table is used by the patrolman to adapt the probability of visiting houses to prefer those with greater mistrust values.

D. Mistrust Table

Let,

- $MT_t(i)$ is the Mistrust accrued by house 'i' at time 't'.
    - Pseudo code for calculating mistrust:

```
$FOR\ i\ =\ 1\ to\ n$
    $IF\ \ E(i,t) - S\ (i,t) \neq 0$
        $MT_t(i) =\ \delta * MT_{t-1}(i) + 1$
$ELSE$
        $MT_t(i) =\ \delta * MT_{t-1}(i)$

$ENDFOR$
```

- 'δ' is the 'discount factor such that $\delta < 1$. $\delta = 0.5$ in this experiment. Mistrust is discounted so as to allow for a reduction in false reporting by houses.

E. Probability of patrolman visiting a house

- *P(i,t)* is the probability of patrolman visiting house 'i' at time 't'.
- Pseudo code for probability computation:

```
$FOR\ i\ =\ 1\ to\ n$
    $P(i,t) = \frac{MT_t(i)}{\sum_{k=1}^{n} MT_t(k)}$
$ENDFOR$
```

- The form of Probability Density function ensures that: $\sum_{i=1}^{n} P(i,t^*) = 1$

VI. Results

Electrical energy usage data of 9 houses is captured for a year. The houses were divided into three categories based on income (Low, Average and High). Dividing the homes into categories is helpful to determine common usage patterns so that outliers are easier to identify for further evaluation. Over the simulation time frame, 68% of the patrolmen visits are to the high income household and 31% visits are to average income households. Two out of the nine houses in the neighborhood are not reporting their true usage. Initially, the patrolman did not detect the difference in the reported use. However, as shown in figures 2(a) and 2(b) at the highlighted portion, eventually the difference in actual and reported usage is detected and corrected.

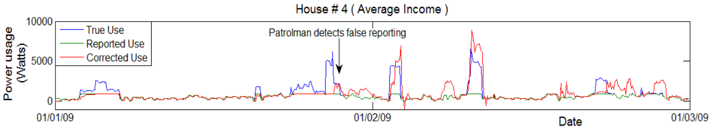

Fig. 2(a) Average Income Household Reported vs. Actual Power Consumption

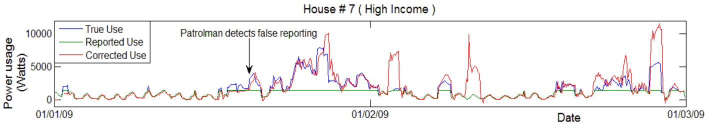

Fig. 2(b) High Income Household Reported vs. Actual Power Consumption

A virtual patrolman is currently in development so the solution is easily portable to a smart metering device. This makes the management of data integrity issues automated with as little human intervention as possible. The solution involves creating categories of homes and using certain characteristics of usage patterns to detect outliers and mathematically apportion the detected error to houses falsely reporting electricity usage data. The categories analyzed here classify houses based on the income and is thus an economic categorization. It is possible to utilize more factors like social, geographic and other information to better classify and categorize households. Such a categorization is commonly used by utilities to help them plan infrastructure for electricity distribution. A higher resolution of usage data now available because of smart metering devices further helps in clustering of customers in categories and this can be used to develop even more accurate models.

In the datasets used in our experiments, houses one, two and three belong to the low income category, houses four, five and six belong to the average income category and the other three are in the high income category. The feasibility of above mentioned approach is proved in figure 3 where the 'standard deviations' of electricity usage is plotted against time for houses belonging to similar category.

Standard deviations of the average income category are plotted over time as shown in figure 3. False usage is reported in house four. Houses five and six converge to standard deviations that are very close to each other within the first five days of the simulation. The standard deviation of house four diverges considerably within the first five days of starting the simulation which shows the validity of the clustering of homes into income categories for evaluation.

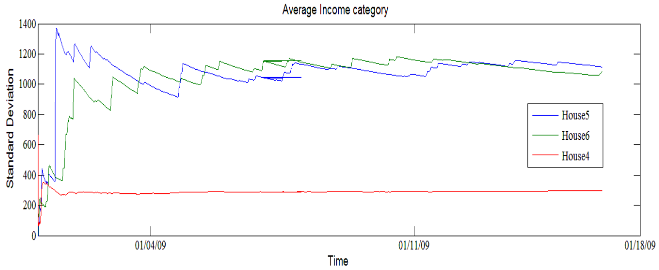

Fig. 3: Usage Comparison of Average Income Homes

VII. Conclusions and Future Directions

Meter tampering is a real possibility in smart grid installations. While securing the hardware and firmware of the metering devices is an obvious first step to reducing the risk of meter tampering, this approach is a good measure to help insulate all involved parties from damage that may be caused by such data tampering attacks.

Such a trust based approach to managing these risks is a good complement to other fail safe measures and needs to be investigated in detail in order to make the AMI as safe and secure as possible.

Future work in this direction involves modeling usage patterns to determine the type of theft that is occurring. In order to achieve this granularity in the TRM algorithm, additional information is required in the model. The system should be capable of quantifying the past behavior of consumers to differentiate between an event where the consumer tampers with the meter and one where the meter is tampered with by a third party miscreant. Another measurement is the social behavior of the consumer that can be quantified to allow for larger variations in routine usage patterns. For example if a consumer goes on vacation leading to a sudden drop in electricity usage, the algorithm should not penalize the user for this change in consumption.

While the type of theft discussed in this analysis is perhaps the most obvious, it is necessary to run such an algorithm against other kinds of electricity thefts as well. This includes scenarios where a large number of houses misreport their usage, or the data read at the substation itself is suspect.

In our present work, these issues are being addressed to provide a comprehensive solution to a more generalized version of this problem.

References

[1] Ten, C., Liu, C., Manimaran, G., “Vulnerability Assessment of Cybersecurity for SCADA Systems,” IEEE Transactions on Power Systems, Vol. 23, No. 4, 2008, pp. 1836-1846.

[2] Hahn, A., and Govindarasu, M., “Smart grid cybersecurity exposure analysis and evaluation framework,” IEEE Power and Energy Society General Meeting, (2010) pp. 1-6.

[3] Sabater, J. and Sierra, C., “Review on computational trust and reputation models,” Artificial Intelligence Review, 24(2005) pp. 33-60.

[4] Fadul, J., Hopkins, K., Sheffield, C., et. al., “Trust Management and Security in the Future Communication-Based “Smart” Electric Power Grid,” Proceedings of the 44th Hawaii International Conference on System Sciences, 2011, pp. 1-10.

[5] C. Wei, “ A Conceptual Framework of Smart Grid”, Power and Energy Engineering Conference (APPEEC), 2010

[6] Doran, K., “Privacy and Smart Grid: When Progress and Privacy Collide,” University of Toledo Law Review, 41(2010) pp. 1-13.

[7] Huq, Z, Islam, S., “Home Area Network Technology Assessment for Demand Response in Smart Grid Environment,” Australasian Universities Power Engineering Conference, 2010, pp. 1-6.

[8] Khurana, H.; Hadley, M.; Ning Lu; Frincke, D.A.; , "Smart-Grid Security Issues," Security & Privacy, IEEE , vol.8, no.1, (2010) pp.81-85.

[9] Corredor, P.H.; Ruiz, M.E.; , "Against All Odds," Power and Energy Magazine, IEEE , vol.9, no.2, (2011) pp.59-66.

[10] Study of Security Attributes of Smart Grid Systems – Current Cyber Security Issue (http://www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf)

[11] Division Environment and Infrastructure TERNA Wind Energy Programme: Energy-policy Framework Conditions for Electricity Markets and Renewable Energies, 21 Country Analyses: Part Colombia (http://www.gtz.de/de/dokumente/en-windenergy-colombia-study-2004.pdf - visited 4-24-11)

[12] Leon, R., Vittal, V., Manimaran, G., “Application of Sensor Network for Secure Electric Energy Infrastructure,” IEEE Transactions on Power Delivery, Vol. 22, No. 2, April 2007, pp. 1021-1028.

[13] Fadul, J., Hopkins, K., Sheffield, C., et. al., “Trust Management and Security in the Future Communication-Based “Smart” Electric Power Grid,” Proceedings of the 44th Hawaii International Conference on System Sciences, 2011, pp. 1-10.

[14] Yu, H., Shen, Z., Miao, C., et.al., “A Survey of Trust and Reputation Management Systems in Wireless Communication,” Proceedings of the IEEE, Vol. 98., No. 10, October 2010, pp. 1755-1772.

[15] A. S. Rao and M. P. Georgeff, “BBDI agents: From theory to practice,”[in Proc. 1st Int. Conf. Multi-Agent Syst., 1995, pp. 312–319.

[16] C. Castelfranchi, R. Falcone, and G. Pezzulo, “BTrust in information sources as a source of trust: A fuzzy approach,[in Proc. 2nd Int. Joint Conf. Autonom. Agents Multi-Agent Syst., 2003, pp. 89–96.

[17] R. Falcone, G. Pezzulo, and C. Castelfranchi, “BA fuzzy approach to a belief-based trust computation,’’ Lecture Notes in Artificial Intelligence. Berlin, Germany: Springer-Verlag, 2003, pp. 73–86.