Malicious Meter Inspection in Smart Grid Using ABSC Algorithm

Laya Chacko[1], Ajeesh S[2], Smita c Thomas[3]

[1]P G Scholar Dept. of CSE, Mount Zion College of Engineering, Pathanamthitta, Kerala, India
[2]Dept. of CSE, Mount Zion College of Engineering, Pathanamthitta, Kerala, India
[3]Research Scholar, Vels University, India

Abstract - *Electricity theft is the problem faced by all countries in the world. Many of the countries loss their faith in antique power systems and switched to smart grid. All countries support the concept of smart grid. The main aim to find the dirty user with scanning and binary search method.*

Key Words: Electricity theft,Scanning method, binary search method, BCGI

1. INTRODUCTION

Smart grid are electrical grid which are the combination of hardware and software. Smart grid users and companies have tool to manage, monitor and respond to the power related issues. Smart grid introduced in many countries such as USA, Japan etc. Traditional power systems are upgraded into digital smart meters. These smart meters are capable of computation, communication and remote control. Smart meter includes a cyber- layer is added to the metering system. It helps the dirty users to apply various ways to steal electricity. Traditional meters affects physical attacks, by directly tapping into power lines. Smart meters can also be influence with cyber-attacks users with minimum level of computer knowledge are able to hack smart meters, with software readily available on the Internet [10]–[12]. Many another works done on electricity theft detection. Major important methods are classification based methods and power based methods. Classification-based methods called grouping methods which applies the extreme learning to analyze user's electricity meter readings. This readings aims to find the users vicarious nature referent to theft electricity. In power based methods which installs extra devices to supervise the meter readings of users.

The proposed electricity theft detection method in the paper is called Adaptive Binary Splitting Check (ABSC) algorithm which test groups of users together and the group size is dynamically during the testing process. The goal of identifying all dirty users within the lowest detection time, a series of inspection methods based on logical binary trees are proposed in papers [14][15]. Recently observe that the electricity theft detection issue, we propose to apply a group testing method to electricity theft detection to locate malicious users.

2. LITERATURE SURVEY

The Binary Coded Grouping-based Inspection (BCGI) algorithm group's users in the NAN based on the binary sequences of identification numbers BCGI groups the users in the NAN. BCGI locate malicious users by only one inspection step works there is a unique malicious user in the NAN. Each inspection box includes inspectors and sub-inspectors. An inspector box which contains a head inspector and several sub inspectors. The head inspector is responsible for finding the presence of dirty users; the sub-inspectors take charges of acquiring the malicious [2] meters exactly.

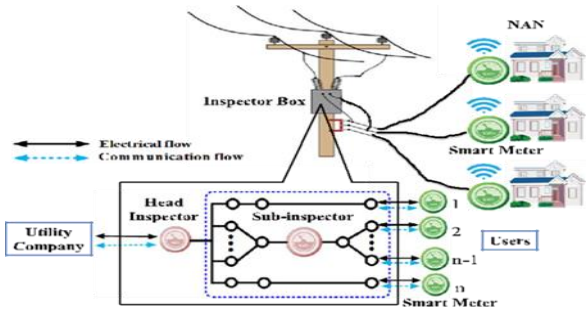

Fig.1: An outline for the malicious meter inspection.

For finding dirty users in shortest detection time, a series of inspection techniques are proposed in papers [14] [15]. The main purpose is to reveal any significant behaviors highly related to electricity theft. Classification based and power based methods are highly expensive because we want to install central observer or inspectors for each user premises.

3. EXISTING SYSTEM

The smart metering system for neighborhood area network are seen on the fig1. Smart meters are installed at each user sites for reporting and recording the electricity consumptions of organizations. Let n be the number of users and u be the set of all users, u= {1, 2....n}. Let V_j and V_j' denotes users' v's reported reading ad genuine electricity usages. V_j and V_j' denotes the users in the NAN as malicious or honest users. If it is malicious, the electricity uptake is less than actual uptake.ie, $V_j < V_j'$ and if it is honest user genuinely reports the electricity report statistics. The inspection box consists of two kinds of inspectors: that is head inspectors and the several inspectors. Head inspectors detects the anomalies and sub-inspectors locating the malicious users. Based on the budgetary constraints of organizations which determines the number of head inspectors and sub-inspector.

Let k denote the entire number of sub inspectors in the inspector box. Then, the set of inspectors can be denoted by I = {0, 1, 2 . . . k}, where inspector 0 shows the head

inspector and inspectors 1, 2. . .k refers as sub-inspectors. Let G_s denote the group of users monitored by inspector s, s ∈ I. Then, for the head inspector, we have G0 =U; and for the sub-inspectors, we have $G_s \subset U, \forall s \in I-\{0\}$. For inspectors s, t ∈ I -{0}, we have $G_0 \cap G_t = G_t$ and $G_s \cap G_t = \emptyset$. For any inspector s∈ I, when it works, it operates as follows:

(1) C_i Measures the total amount of electricity distributed to the users in Gs.

(2) Receiving these users' reported readings.

(3) Calculating the whole amount of stolen electricity of all the users in Gs, which is notated by bi. When an inspector conducts one time of the above operations, it performs one inspection step. Based upon the law of conservation of energy, $b_i = C_i - q - \delta_i$ ----------> (1) $t \in G_s$

Where q_j denotes user t's reported readings, and δ_S represents the total amount of technical losses of the users in G_s.

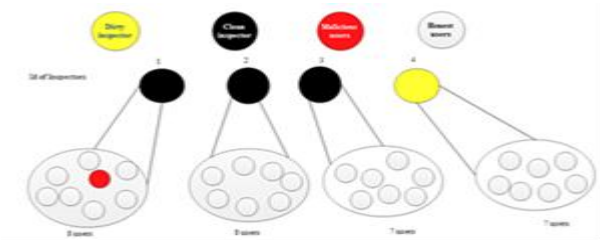

Fig 2: The users are grouped before reading

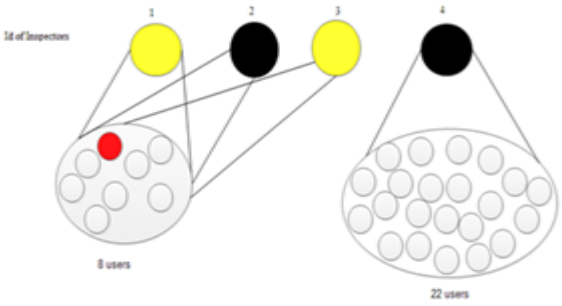

Fig 3: After Reading Anomalies

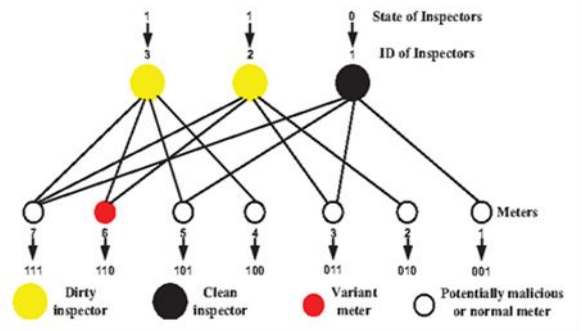

Fig 4: An illustration of the BCGI algorithm

4. PROPOSED SYSTEM

Here the propose system refers the working of ABSC. ABSC used for finding the malicious users from a group. At first set up how the inspector determine whether there are any dirty user among the total group or in the T. Next defines the threshold, notated by ω, to help estimate whether there are reading anomalies among the users being monitored. Specifically, if $P_s \geq \omega$, s ∈ I, the inspector s can conclude that there exist malicious users in G_s.

- If $P_s > \omega$ and there is only one user in Gs, this unique user will be identified as being malicious.
- If $P_s \leq \omega$, all users in G_s will be declared as being honest.
- If $P_s > \omega$ and G_s contains multiple users, we can only conclude that at least one malicious user in G_s. The status of any user in G_s cannot be determined immediately, and more inspection steps need to be further conducted.

Let T denote the set of users whose status ("honest" or "malicious"). Let M denote the set of users in which malicious users are already being identified. Let H denote the set of users in which already identified the honest.

(1) $U = T \cup M \cup H$; (2) $T \cap M = \emptyset$;

(3) $W \cap H = \emptyset$; (4) $M \cap H = \emptyset$.

A total number of at most malicious users in the NAN and the users in M are malicious, we can infer that during the inspection process, the maximum number of malicious users in T that remain to be identified is $\mu - |M|$. Among the users whose status has not been determined, if on average one user out of at least two users is malicious,

i.e., $|T| \geq 2(\mu - |M|) - 1$, ----------> (2)

Scanning method which helps to inspect the users in T one by one merely binary search method which locate the malicious user in [14].

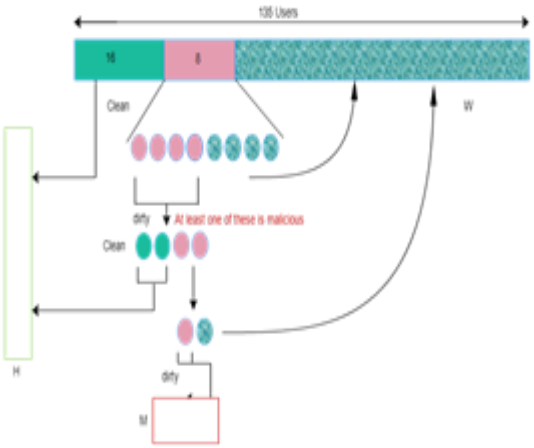

Fig 5: An illustrate the ABSC algorithm

Important feature of ABSC which can adaptively adjust their inspection strategies by dynamically changing the inspection strategies either it can use binary search method or scanning method. Binary search method extract the particular number of users from *T*. Scanning method inspect the Whole user one by one, time consuming and need more inspectors. Major difference between this two is binary search method can inspect as whole rather than inspecting one at a time.

4.1 ADUSTABLE BINARY SPLIT CHECK ALGORITHM

Take: T

Set: M, H

Set T← U, M ← ∅, H ← ∅ //M and H are global.

ABSC (T):

While $P_s > \omega$ do

if $|T| \geq 2(\mu - |M|) - 1$ then

GroupSearch (T);

else

Scan (T);

end if

end while{end ABSC}

Scan (T):

G_i, T ← takeoutUsers(T, 1);

if $P_i > \omega$ then

$M \leftarrow M \cup G_i$;

else

$H \leftarrow H \cup G_i$;

end if

ABSC (T);

{end Scan}

GroupSearch (T);

G_i, T ← takeoutUsers(T, 2α);

if $P_i > \omega$ then

k ← 0;

while $k \leq \alpha$ do

if $|G_i| == 1$ then

$M \leftarrow M \cup G_i$; break;

else

G_i, $G_i`$ ← takeoutUsers(G_i , $|G_2i|$);

if $P_i > \omega$ then

$G_i \leftarrow G_i`$;

$T \leftarrow T \cup G_i$;

else

$G_i \leftarrow G_i`$;

$H \leftarrow H \cup G_i$;

end if

k + +;

end if

end while

else

$H \leftarrow H \cup G_i$;

end if

ABSC (T);

{end GroupSearch};

5. CONCLUSION

In this paper, ABSC algorithm which adaptively adjust the inspection strategies. Average among two users one being malicious we use the binary search method otherwise use the scanning method. ABSC gives out the maximum number of inspection steps. The existing systems uses BCGI algorithm identifying the malicious meter committing electricity theft in neighborhood areas. But BCGI can locate the unique malicious meter if there is one meter becomes malicious in one reporting period. This paper focus on finding electricity theft. In this paper, we assume that once malicious users are located, utility companies disconnect their power accounts immediately and do not restore electricity until malicious users finish paying the whole balance. ABSC algorithm is a more general approach. In near future, smart grid provide customer security, greater number of intelligent devices, the lifetime of power systems and physical security.

REFERENCES

[1] Z. Xiao, Y. Xiao, and D. H. C. Du, "Non-repudiation in neighborhood area networks for smart grid," IEEE Commun. Mag., vol. 51, no. 1,pp. 18–26, Jan. 2013.

[2] X. Xia, W. Liang, Y. Xiao, and M. Zheng, "BCGI: A fast approach to detect malicious meters in

neighborhood area smart grid," in Proc. IEEE Int. Conf. Commun. (ICC), London, U.K, pp. 7228–7233., Jun. 2015

[3] A. H. Nizar, Z. Y. Dong, and Y. Wang, "Power utility nontechnical loss analysis with extreme learning machine method,"IEEE Trans. PowerSyst., vol. 23, no. 3, pp. 946–955, Aug. 2008.

[4] J.Nagi, K. S. Yap, S. K. Tiong, S. K.Ahmed, and A. M. Mohammad"Detection of abnormalities and electricity theft using genetic support Vector machines," in Proc. IEEE Region Conf. TENCON,pp. 1–6. Nov. 2008

[5] J Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad,"Nontechnical loss detection for metered customers in power utility using support vector machines," IEEE Trans. Power Del., vol. 25, no. 2,pp. 1162–1171, Apr. 2010.

[6] C. C. O. Ramos, A. N. de Sousa, J. PPapa, and A. X. Falcao,"A new approach for nontechnical losses detection based on optimum path forest," IEEE Trans. Power Syst., vol. 26, no. 1, pp. 181–189, Feb. 2011.

[7] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity theft detection in AMI using customers' consumption patterns," IEEE Trans. Smart Grid,vol. 7, no. 1, pp. 216–226, May 2016.

[8] R. D.Trevizan et al., "Non-technical losses identification using optimum-path forest and state estimation," in Proc. IEEE Eindhove PowerTech, Eindhoven, The Netherlands, pp. 1–6, Jun./Jul. 2015

[9] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 981–997, 4th Quart., 2012.

[10] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 3,pp. 717–729, Mar. 2014.

[12] C.-H. Lo and N. Ansari, "CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid," IEEE Trans Emerg. Topics Comput., vol. 1, no. 1, pp. 33–44, Jun. 2013.

[13] Z. Xiao, Y. Xiao, and D. H. C. Du, "Exploring malicious meter inspection in neighborhood area smart grids," IEEE Trans. Smart Grid,vol. 4, no. 1, pp. 214–226, Mar 2013.

[14] X. Xia, W. Liang, Y. Xiao, M. Zheng, and Z. Xiao, "A difference comparison-based approach for malicious meter inspection in neighborhood area smart grids," in Proc. IEEE Int. Conf. Commun. (ICC),London, U.K., Jun. 2015, pp. 802–807.

[15] X. Xia, W. Liang, Y. Xiao, and M. Zheng, "Difference comparisonbased malicious meter inspection in neighborhood area networks in smart grid," Comput. J., vol. 60, no. 12, pp. 1852–1870, 2017.