International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Security Assumptions for Ubiquitous Secure Smart Grid Infrastructure using 2 Way Peg Blockchain and Fuzzy Specifications

Md. Shakilur Islam Sarker, Ziaur Rahman, SK. A. Shezan, Md. Selim Hossain , Md. Mahabub Hossain

Abstract: ***The smart grid cyber-physical system and advanced metering infrastructure is an immensely growing term in industrial research based on the electrical power grid system and has uncovered an efficient paradigm for the power generation, transmission, and for the expenditure management as well. These systems allow home area networks and advanced metering infrastructure to communicate bi-directionally. False data injection is a new and climacteric security threat to the power grid to tamper such important data. However, these communication channels that the energy service interfaces provide two-way communication according to the central control unit. Thus, for the security and robustness of the grid, it is critical to separate the false or infected data. The existing protocol on this problem is based on state estimation which is less secure and computationally expensive. In this paper, we propose a 2-way peg blockchain security system by providing a digital signature scheme between home area network device (Smart Meter) and AMI server to get authorization, providing an infected data detection algorithm based on fuzzy rule specification and 2WP based blockchain protocol and finally infected performance reputation updating algorithm by computing the probability distribution of uncouth level to detect the infected or compromised the. We get more efficiency and security by performing a detailed analysis.***

Keywords: 2WP Blockchain, Infected data detection, Rules specifications, Performance reputation updating.

I. INTRODUCTION

A judiciousness of brilliant framework with the advancement of data innovation is to give an exceptionally effective, hearty, exact, solid and secure power conveyance just as strong vitality age and use.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Md. Shakilur Islam Sarker*, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh
Ziaur Rahman, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh
SK. A. Shezan, Scool of Engineering, RMIT University, Melbourne, Australia
Md. Selim Hossain, Md. Selim Hossain, Lecturer in Department of Computer Science and Engineering at KhwajaYunus Ali University, Sirajganj, Bangladesh.
Md. Mahabub Hossain, Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Propelled Meter Infrastructure (AMI) advances have been furnishing quick headway direct association with client's HAN gadget and Control Center (CC). Home Area Network (HAN) may have a few HAN gadgets like savvy meter (SM), versatile device (PDA, Smartphones, etc.), Energy administration interface (ESI). Infusion of False or pernicious information on a brilliant matrix digital-physical framework (CPS) perceived as a climacteric security risk. Cliché False or noxious information discovery entrance, which depends on state estimation (SE) could without much of a stretch be hacked by keen FDI assailants' arms with the information on the framework setup. Existing heritage FDD plots just work with the residuals and framework's inner blunders instead of the malignant information infusion of HAN gadgets like Smart meters and don't assess any further activity to give warning or further cure. Considering CPS security approaches, integrity is considered as the most climacteric requirement. The existing method based on State estimation (SE) is not much secure and accurate to detect the false data and uncouth level of the Phasor data concentrator (PDC) and much computationally expensive and data transfer through traditional medium could be more malicious and less secure for which we use 2-way peg Blockchain. The author proposed an advanced distribution smart meter-oriented recognition technique including authentication approaches based on security and efficiency checks upon rule specification, rather than not only state estimation (SE) and established a blockchain connection between the AMI server and Smart Meter (SM). These methods provide three-stage security approaches and reduce the computational burden from AMI. 2WP blockchain implementation makes the network channel more secure. Our IDD algorithm detects the infected or false data rapidly and provides the running status of smart meter. On the other hand, the PRU algorithm detects the infected PMU for further evaluation.

II. SYSTEM DESIGN

A brilliant lattice arrange is surrounded by SMs, PDCs, Trusted Authority (TA), Two Way Peg (2WP) blockchain and AMI server. As appeared in the "Fig. 1". A brilliant lattice CPS is a completely computerized framework that is fit for cost decrease, accomplishing self-recuperating, better unwavering quality, and productivity. It incorporates wide-region estimation and control framework (WAMCS) which can give high power recognition capacity and controllability on the power matrix.

SM is introduced to client inhabitant or association which records the power utilization and sends approved information to closest PDCwith its comparing compelled gadget. PDC is situated on the local location which gathers the approved information to the AMI server.

It likewise works bi-directionally by communicating information from the AMI server to the SMs. AMI server evaluates the power utilization and total meter information and communicates the value data of intensity and trains the framework on how to work.

The Smart meter played out a solicitation to the Trusted Authority to get the consent and get the authorization to information move to PDCs. PDCs then move every one of the SMs Data to AMI.

In this paper, we consider a polynomial-time foe model that can control SMs and PDC just as ESI correspondence channels. So that authorized users can integrate or modify, inject, eavesdrop, update.

We propose a three-stage security system which includes Digital Signature between SM (PDA, smartphones, notebook, etc.) and AMI server through 2WP blockchain by providing public and private key constrained, then we include a rule-based Infected data detection (IDD) method to detect the false or malicious data.

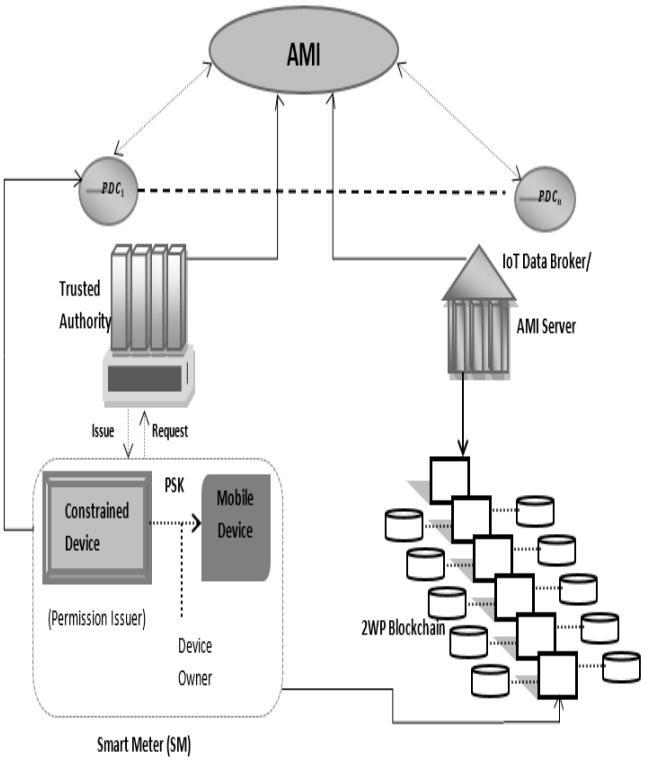

Fig. 1: Proposed Unified Network Model of a Highly Secured Smart Grid System using 2WP Blockchain.

Finally, we assume a Performance reputation updating (PRU) algorithm to find out the infected or compromised PMU to measure the threat level.

III. PROPOSED DIGITAL SIGNATURE MECHANISM

Here to give access or approval during information move, we proposed a computerized mark component which was initially proposed by Fait and Shamir.

To change over the ID plot into advanced mark conspire we supplanted the verifier with a single direction hash work H such SHA-1 or MD5.

Here (HAN SM/HM/PMU etc) devices and AMI server use private and public key pair with a common shared key during (i) Signature generation(Encryption) and (ii) Verification(Decryption) phases.

Now to send message 's' to the HAN (SM/HM/PMU etc) devices, the AMI server runs the following protocol through:

- Protocol I (Signature Generation / Encryption)

Phase 1. Performed encryption method using bitwise XOR operation as $\mathbf{m_1 = s \oplus k_s}$.

Phase 2. Choose a random number $\mathbf{r \in Z_q^*}$ to compute $\mathbf{X = (x_M, y_M) = r.P}$.

Phase 3. Derive x_M to compute $\mathbf{C = H(x_M, m_1)}$.

Table- I: Proposed Digital Signature Mechanism Notation

Notation	Definition
K_{Pr}	Private Key of Entity
K_{Pu}	Public Key of Entity
r	Commitment of Entity
X	Witness of Entity
C	Challenge of Entity
Y	Response of Entity
P	Base Point
k_s	Shared Secret Key
H (.)	One-way Hash function
$\oplus$	XOR operation

Phase 4. Compute $\mathbf{Y = r - C.K_{PrM}}$.

Phase 5. Send encrypted message $\mathbf{m_1}$ with signature (C,Y).

Upon receiving $(\boldsymbol{m_1, C, Y})$ from AMI server does the following:

- Protocol II (Verification / Decryption)

Phase 1.Compute

$$\boldsymbol{X_1 = YP + CK_{PuM} = (x_{M1}, y_{M1})}.$$

Phase 2.Derive $\boldsymbol{x_{M1}}$ and verify $\boldsymbol{H = (x_{M1}, m_1)}$ =? C. If it holds, it accepts that encrypted message.

Phase 3.Obtain original message by decryption using XOR operation as $\boldsymbol{s = m_1 \oplus k_s}$.

A. 2WP Design

To a two-way peg to work these two lockboxes basically, need to have information about each other and have to be able to release funds simultaneously when the lockbox on the other side was seized.

There are a couple of ways for this to work. The simple way to implement a two-way peg is via central exchanges and in this case, we will have a central party that controls both lockboxes on both sides.

The advantage of this is simple but the disadvantage is that we are placing trust in a central party who can if wants to maliciously empty a lockbox in a chain and steal all funds so there is a way to minimize the central trust placed in a central exchange and that is with a federation, so we can implement

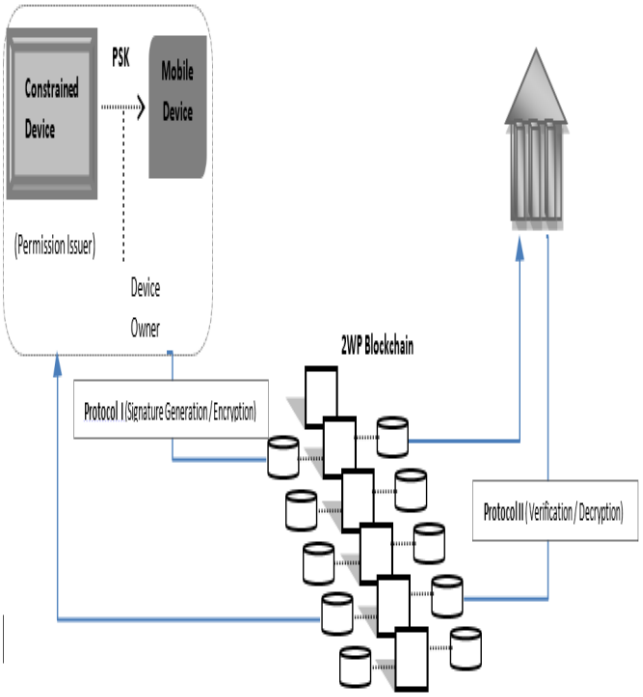

Fig 2: Proposed Digital Signature Mechanism through 2WP Blockchain.

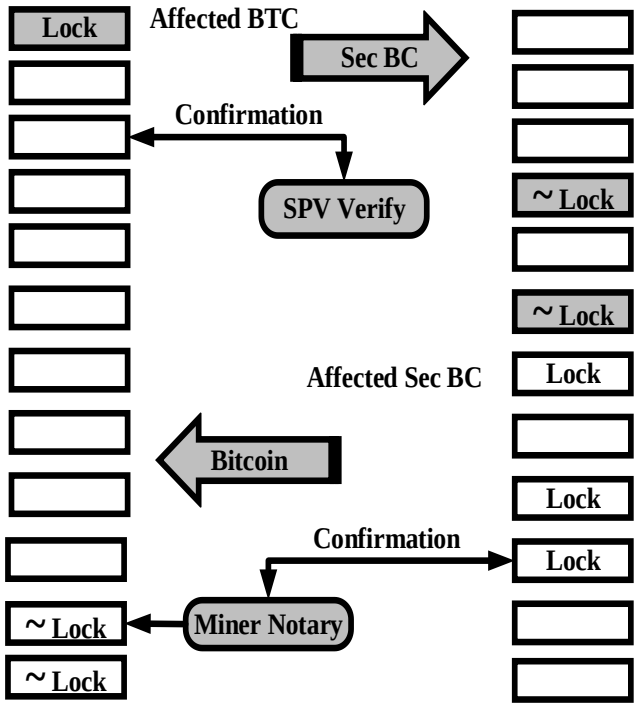

Fig. 3: Sample Transactions to unlock the BTC with Secoin using Proof of Last transaction control (SPV).

the two-way peg via a federated peg where the lockboxes are now being controlled by a group of entities so when I make that transaction across the two chains I now require the lockbox to have n of m signatures to release funds on at least n entities of the Federation need to confirm that this is a valid transaction now the advantage of this is similar to what we have before it can be implemented with any two types of chains without specific protocol upgrades or specific all codes but again we have a centralized trust placed in a group of minimum now there is one more type of two-way peg where the two chains can interact with each other without having a middleman and this is via SPV proofs.

B. SPV Proof

SPV proof stands for simplified payment verification. The SPV proof basically shows that I can prove to you that my transaction is included in a valid block and that miners have created a lot of subsequent blocks on top of it now the SPV proof does not actually say that transaction is consistent with entire blockchain history It doesn't actually check it across check it to be consistent with all previous transactions from the genesis block onwards instead It's doing a proof indirectly and showing that it's member of a block and a lot of miners trust that the block is correct and therefore they have mined on top of it forming the longest chain. SPV gives the 2 critical factors:

- It ensures the transactions are in a block, and
  - It provides attestation (proof of work) that additional blocks are being appended to the chain. By using a two-way peg system with SPV proof we can ensure more security reliability and efficiency than a system that is using a single chain.

C. Proof of Work

Miners in POW chains have the accountability for the growing the chain by repeatedly finding newer blocks. The way of discovering or "mine" for these blocks is by doing a nonstop calculation that requires a lot of processing power.The hash of the block is taken and appended a “nonce” to it. It is a random hexadecimal value. The resultant string is then hashed again. That new hashed value cannot be equal to or more than a predetermined value thatnis called "difficulty." The miners must be keeping on repeatedly altering the value of the nonce until they achieve the required result.If a miner finds a block then they need to present that newly found block to the network along with the nonce. The network can then simply append the two values and hash it to check the validity of the claim.This is the substance of POW:

- It is difficult to solve the possible and finding the exact nonce
- It should not be easy to check whether the nonce is correct or not.

D. Verification of Transaction Singleton Module

Every one of the individuals from the system gain admittance to an irreversible register of all passed and bombed get to demand gives the duty to the two requesters and supplier. Consider the progression where a client bargains his sensor information to an insusceptible security organization. The client bargains the organization access for one month. If the client pulls back access rights on the sidechain level before the managing time is up, the security organization's solicitation access will be fizzled; and as evidence of abuse by the sidechain proprietor, the organization can yield timestamped logs of its bombed access demand.

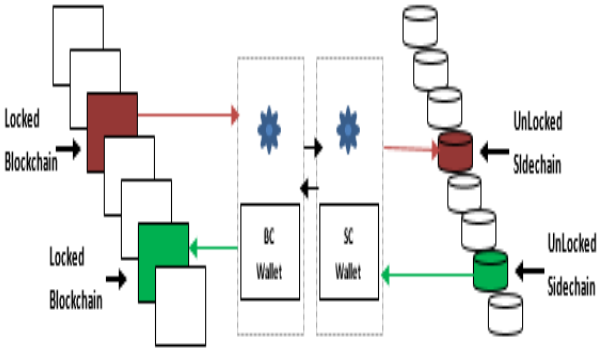

Fig. 4: Bitcoin Transfer singleton Module on 2WP Blockchain.

Algorithm 1 shows the method of accomplishing an individual transaction, X. The public BC all multizonal transactions propagated by each requester are maintained in an individual register. The outcome of the multizonal transactions provides a renown metric for the requester. The connection between passed transactions is established by insertion of the hashing of the PK which will be used by the requester for the subsequent transaction in the 3rd output field of the present transaction. So, the OBM first ensures this by assimilating the hashing of the requester PK in X with the outcome of the former transaction of that requester (lines 1,2). According to this, the requester signature, which is held in the 4th field of X, is accomplished (also called Release) using its PK in X (lines 4,5).In the beginning, the requester sets these outcomes (based on its transactions) in the multizonal transaction. If the provider allows the transaction, then it would increase the outcome by 1.

To defend the chain against nodes those, demand spurious reputation by increasing their outcome before providing them to the provider, in the next step of transaction substantiation, the OBM checks that only one of X's outcome, i.e. either the number of passed transactions (i.e. outcome [0]) or the number of failed transactions (i.e. outcome [1]), is increased only by one. According to this, the request signature is verified using its PK in X. If all steps passed successfully, X is verified.

Algorithm 1 Transaction verification.

Input: Overlay Transaction (X) **Output:** True or False

Requester verification :
1: **if** (hash (X.Requester-PK) = X $_{\uparrow}$.output[2]) **then**
2: **return** False;
3: **else**
4: **if** (X.requester-PK redeem x.requester-signature) **then**
5: **return** False;
6: **end if**
7: **end if**
Ouput validation :
8: **if** (X.output[0] - X $_{\uparrow}$.output[0]) + (X.output[1] - X $_{\uparrow}$.output[1])> 1) **then**
9: **return** False;
10: **end if**
Requestee verification :
11: **if** (X.requestee-PK redeem x.requestee-signature) **then**
12: **return** true;
13: **end if;**

IV. PROPOSED SECURITY MECHANISM

Table- II: Rule Specification Notation

Notation	Definition
G_i^t	The measured value of power generation at generation I and time t.
$\hat{G}_i^t$	Corresponding expected value.
L_i^t	The measured value of the power load.
$\hat{L}_i^t$	Corresponding expected value.
F_i^t	The measured value of the powerline flows (Power flow).
$\hat{F}_i^t$	Corresponding expected value.
$\tau_{min} - \tau_{max}$	Safe Range
τ_G	The safe threshold of Power Generation (PG).
τ_L	The safe threshold of Power Load (PL).
τ_F	The safe threshold of Power Flow (PF).
$\vec{V}_{measured}$	Measured Phasor
$\vec{V}_{ideal}$	Ideal Phasor
$\boldsymbol{E_{rms}}$	RMS of voltage
$\boldsymbol{I_{rms}}$	RMS of current

A. Infected Data Detection (IDD) Method

- Rule Specification

To find out the rule specification is violated or not we perform a binary system, where "0" denotes that the measurement data is relevant and "1" indicates a violation. For instance, "10011100001000" denotes that rules 1,4,5,6,11 are violated. We normalized a Euclidean distance strategy to determine the uncouth level -

$$\boldsymbol{A_l = d^{EuD}(i,j) = \sum_{k=0}^{n-1} y_{i,k} \neq y_{j,k}} \quad (1)$$

Here, $\boldsymbol{d^{EuD}}$= Normalized Euclidean distance of the two sequencesi and j.
where i="00000000000000" which is the baseline. Now let Smart meter,

$$\boldsymbol{SM} = \{\boldsymbol{SM_1}, \boldsymbol{SM_1}, \ldots\ldots, \boldsymbol{SM_N}\};$$

and Set of PMUs, $\boldsymbol{U} = \{\boldsymbol{U_1}, \boldsymbol{U_2}, \ldots\ldots, \boldsymbol{U_N}\};$
Iteration_flag='0' indicates that the procedure don't have to be repeated.
Iteration_flag='1' indicates that the procedure has to be repeated.

- Rules

R1: $\boldsymbol{\left|G_i^t - \hat{G}_i^t\right| \leq \tau_G}$
R2: $\boldsymbol{\tau_{Pmin} \leq G_i^t \leq \tau_{Gmax}}$
R3: $\boldsymbol{\left|L_i^t - -\hat{L}_i^t\right| \leq \tau_L}$
R4: $\boldsymbol{\tau_{Lmin} \leq L_i^T \leq \tau_{Lmax}}$
R5: $\boldsymbol{\left|F_i^t - \hat{F}_i^t\right| \leq \tau_F}$
R6: $\tau_{Fmin} \leq F_i^t \leq \tau_{Fmax}$
R7: Active Power Angle: $\boldsymbol{\Delta\partial < \partial_\Delta}$
R8: Voltage Amplitude: $\boldsymbol{\Delta V < V_\Delta}$
R9: Real Power (MW): $\boldsymbol{\Delta L_{MW} < L_{MW\Delta}}$
R10: Reactive Power (M_{var}) :$\boldsymbol{\Delta L_{Mvar} < L_{Mvar\Delta}}$
R11: Total Vector Error (TVE) :

- TVE=$\frac{|\vec{V}_{measured} - \vec{V}_{ideal}|}{|\vec{V}_{ideal}|}$
- TVE<1% (typically)
- The measured vector could be current or voltage.

- Error: $\vec{V}_{error} = \vec{V}_{measured} - \vec{V}_{ideal}$

R12: Apparent Power (M_{VA}): $P_A = E_{rms}.I_{rms}$

- Reactive Power (P_{Mvar})=$\vec{P}_{VA} - \vec{P}_{MW}$

=Vector difference of apparent and real power

- $P_{VA}^2 = P_{MW}^2 + P_{Mvar}^2; \Delta L_{MVA} < L_{MVA\Delta}$

R13: Frequency (Rate of Frequency)

- Nominal Frequency → 50 and 60 Hz (Settable)
- Operating Frequency → 45 to 65 Hz
- $\Delta f \leq f_{\Delta}$

R14: Phase

- 0^o to 360^o ± 0.5%
- $ABC\ or\ CBA$
- $\Delta P \leq P_{\Delta}$

Each net SM,$SM_i \epsilon SM$determines the cohesive result$R_i^t$of a current piece of measurement data and broadcast the connected SM –

$$SM_i = \{SM_j | SM_j \sim SM_i\}.$$

An example is shown in "**Fig. 4".** Here, by corresponding results of SMs if there is no "1" bit in the result R_i^t then the no false or malicious data is detected over the Smart meter. But if there any results that show "1" bit then SM_ihave to check out how many meters have bit "1" in their cohesive result R_j^t. Therefore, if the result is more than or equal to the quarter of the inter-connected Smart meters (SM) R_j^t then SM_i concludes that $U_i$has

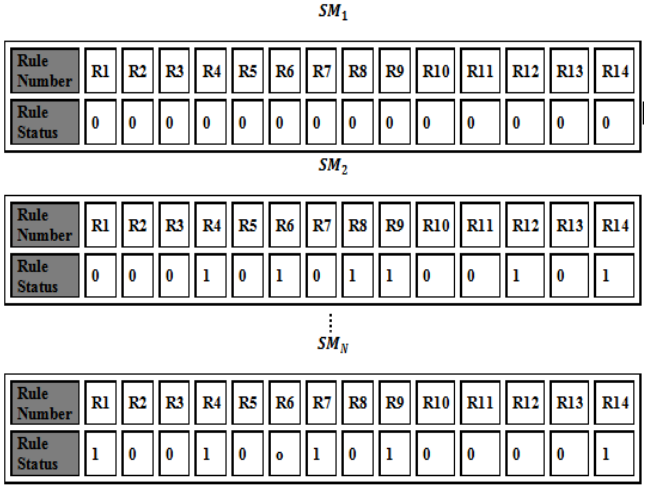

Fig. 5: Sample cohesive results transmitter between SMs.

reported has reported a piece of false measured data, otherwise, $R_i^t$is piloted as dubious. After executing the first procedure by $SM_i \epsilon SM$ the next step is to get determined. If iteration_flag="1", then the process will be repeated to find the further infected or false or malicious data; otherwise the procedure will go to end.

Algorithm 1 IDD Algorithm

1: Initialization: $SM = \{SM_1, SM_1, \ldots\ldots, SM_N\}$, Upperbound=15, Iteration=0, flag='0'

2: Procedure:

3: **for** each smart meter $SM_i \epsilon SM$ **do**

4: ***(I).*** determines the cohesive result R_i^t of current piece of measurement data.

5: ***(II).*** broadcasts the result R_i^t to inter-connected meters $SM_i = \{SM_j | SM_j \sim SM_i\}$.

6: Identifies Infected Data: **If** there is no bit "1" in the result R_i^t **then**

7: ***Output:*** no infected data detected.

8: **Else if** more than or equal to quarter of the meters in SM_i hold bit "0" at the same position in the result R_j^t **then**

9: ***(a). Output:*** infected data detected.

10: ***(b).*** removes SM_i from SM and its connections with other meters.

11: **Else**

12: ***(a).*** keeps R_i^t as dubious result.

13: ***(b).*** Iteration_flag="1".

14: **End if**

15: **End for**

16: Judges the termination criteria: **If** Iteration_flag =="1" and Iteration < Upperbound then

17: ***(a).*** repeats Step 2(**Procedures**).

18: ***(b).*** Iteration= Iteration+1.

19: **Else**

20: Ends the procedure.

21: **End if**

22: **End Procedure**

V. DETERMINATION OF INFECTED PMU

A. Probability Distribution of Uncouth Level

Now, let a random variable A= Uncouth level of a set of measurement data, its value can be either 0 or 1 which is determined by Euclidean distance as mentioned before. The probability density function(PDF) of a stable distribution is –

$$f(x_i|\alpha,\beta,\gamma,\delta_0) = \exp(\beta_i^t - |\gamma t|^{\alpha}(1 - \delta i Sign t\varphi \quad ,(2)$$

Where,

$$= \begin{cases} (|\gamma t|^{1-\gamma} - 1)tan\left(\frac{\pi\alpha}{2}\right) & \alpha \neq 1 \\ -\frac{2}{\pi}\ log|\gamma t| & \alpha = 1 \end{cases};$$

The means value of the stable distribution is-

$\mu = \delta - \beta\gamma\ tan\frac{\pi\alpha}{2}$; $when\ \alpha > 1$ And for ≤ 1, mean is undefined.

B. Maximum Likelihood Estimation (MLE)

To get the exact distribution of A, we estimate the parameters $\alpha, \beta, \gamma, \delta_0$ using MLE. The maximum likelihood estimation scheme for α- stable distribution –

$$l(\vec{\theta}) = \sum_{i=1}^{n} log\ f(x_i|\vec{\theta}) \quad (3)$$

Where $\vec{\theta} = (\alpha, \beta, \gamma, \delta_0)$ and density function $\left(x_i|\overrightarrow{\ }\right)$ θ, Stable sample, $x_i = (x_1, x_2, \ldots, x_n)$. In most cases, it is easier to work with the natural logarithm of the likelihood function by re-writing – $ln\ l(\vec{\theta}) = ln \sum_{i=1}^{n} f(x_i|\vec{\theta}) = \sum_{i=1}^{n} ln\{exp(\beta_i^t - |\gamma t|^{\alpha}(1 - \delta_i Sign(t)\varphi)\}$(4)

Here, $\boldsymbol{\varphi} = \begin{cases} (|\boldsymbol{\gamma t}|^{1-\gamma} - 1)\boldsymbol{tan}\left(\frac{\pi\alpha}{2}\right) & \boldsymbol{\alpha} \neq 1 \\ -\frac{2}{\pi}\, \boldsymbol{log}|\boldsymbol{\gamma t}| & \boldsymbol{\alpha} = 1 \end{cases}$;

Then we have to find the corresponding values of $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}$ *and* $\boldsymbol{\delta_0}$ that maximize

$$\ln \mathcal{L}(\alpha, \beta, \gamma, \delta_0 | x_i = (x_1, x_2, \ldots, x_n)) \qquad (5)$$

Since logarithm is a strictly increasing function, the largest value, if it exists, could be calculated-

$$\begin{cases} \partial\left(\dfrac{\ln \alpha}{\partial\alpha}\right) = 0 \\ \partial\left(\dfrac{\ln \alpha}{\partial\beta}\right) = 0 \\ \partial\left(\dfrac{\ln \alpha}{\partial\gamma}\right) = 0 \\ \partial\left(\dfrac{\ln \alpha}{\partial\delta_0}\right) = 0 \end{cases}$$

That is –

$$g_1(\alpha, \beta, \gamma, \delta_0) = \Psi(\alpha) - \Psi(\alpha + \beta + \gamma + \delta_0) - \frac{1}{n}\sum_{i=1}^{n} \ln x_i = 0$$

$$g_2(\alpha, \beta, \gamma, \delta_0) = \Psi(\beta) - \Psi(\alpha + \beta + \gamma + \delta_0) - \frac{1}{n}\sum_{i=1}^{n} \ln(1 - x_i) = 0$$

$$g_3(\alpha, \beta, \gamma, \delta_0) = \Psi(\gamma) - \Psi(\alpha + \beta + \gamma + \delta_0) - \frac{1}{n}\sum_{i=1}^{n} \ln(2 - x_i) = 0$$

$$g_4(\alpha, \beta, \gamma, \delta_0) = \Psi(\delta_0) - \Psi(\alpha + \beta + \gamma + \delta_0) - \frac{1}{n}\sum_{i=1}^{n} \ln(3 - x_i) = 0$$

Where $\Psi(x)$ is the digamma function defined as –

$$\Psi(x) = \frac{\partial}{\partial x} \ln \Gamma(x) = \frac{\Gamma'(x)}{\Gamma(x)};$$

To find the approximate roots, the parameters $\widehat{\boldsymbol{\theta}} = [\widehat{\alpha}, \widehat{\beta}, \widehat{\gamma}, \widehat{\delta_0}]$ can be iteratively estimated by –

$$\widehat{\theta_{\iota+1}} = \widehat{\theta}_\iota - \frac{g(\widehat{\theta}_\iota)}{J_g(\widehat{\theta}_\iota)} \qquad (6)$$

Where, $\boldsymbol{g} = [g_1, g_2, g_3, g_4]$ and $\boldsymbol{J_g}(\widehat{\theta}_\iota)$ is a 4×4 Jacobian matrix –

$$\begin{bmatrix} \dfrac{\partial g_1}{\partial\alpha} & \dfrac{\partial g_1}{\partial\beta}\dfrac{\partial g_1}{\partial\gamma} & \dfrac{\partial g_1}{\partial\delta_0} \\ \dfrac{\partial g_1}{\partial\alpha} & \dfrac{\partial g_1}{\partial\beta}\dfrac{\partial g_1}{\partial\gamma} & \dfrac{\partial g_1}{\partial\delta_0} \\ \dfrac{\partial g_1}{\partial\alpha} & \dfrac{\partial g_1}{\partial\beta}\dfrac{\partial g_1}{\partial\gamma} & \dfrac{\partial g_1}{\partial\delta_0} \\ \dfrac{\partial g_1}{\partial\alpha} & \dfrac{\partial g_1}{\partial\beta}\dfrac{\partial g_1}{\partial\gamma} & \dfrac{\partial g_1}{\partial\delta_0} \end{bmatrix}$$

VI. PERFORMANCE REPUTATION UPDATING (PRU) ALGORITHM

The Observed Reputation Level of a PMU as –

$$T_{ob} = 1 - \mu = 1 - \ \delta - \beta\gamma\, tan\left(\frac{\pi\alpha}{2}\right);$$

Where $\boldsymbol{\mu} = \boldsymbol{mean} = \ \delta - \beta\gamma\, tan\left(\frac{\pi\alpha}{2}\right)$.

The real-time Overall Reputation Level of a PMU is then defined as –

$$T_{PRU} = \ \omega\,.T_{ob} + \ (1 - \omega)\,.T^{o}_{up}$$

$$= \omega\,.\delta - \beta\gamma\, tan\left(\frac{\pi\alpha}{2}\right) + \ (1 - \omega)\,.\frac{1 + \eta_t\,.{}^{o}_{t}\aleph}{1 + \eta_t\,.{}^{o}_{t}\aleph + \eta_f\,.{}^{o}_{f}\aleph} \qquad (7)$$

Where –

- $\boldsymbol{\omega}$ =Weight defined for the Observed Reputation Level;
- $\boldsymbol{T_{ob}}$= The Observed Reputation;
- $(\mathbf{1} - \boldsymbol{\omega})$ =Impacts of recent performances to the Updating Reputation Level;
- T^{o}_{up} = *The Updating Reputation Level.*
- $\boldsymbol{\eta_t}$ = impacts factor of True data;
- ${}^{o}_{t}\aleph$= Cumulative number of "True" data Observation;
- $\boldsymbol{\eta_f}$ = impacts factor of Infected data;
- ${}^{o}_{f}\aleph$ = Cumulative number of "Infected" data Observation.

Here in the algorithm,

- S^{t}_{f} = *Successive observation of* "Infected" *data*and
- $\boldsymbol{\vartheta}$ = *very small value* = 0.0001.

The PRU algorithm shows that increment 1 when the same behaviour occurs. If infected data is observed, then the impact factor of false data$\boldsymbol{\eta_f}$ will be increased by $\boldsymbol{\eta_f^{t-1}}.\ \boldsymbol{e^{\vartheta}} - \mathbf{1}$, otherwise${}^{o}_{f}\aleph$ = the Cumulative number of "Infected" data Observation will be reset to 0 and the impact factor of false data $\boldsymbol{\eta_f}$will remain unchanged.

- Now it is easy to identify the Infected PMU with real-time updating byexamining the following presumption:

$$\begin{cases} P_0: PMU\ U_j\ is\ compromised, & if\ T^{j}_{PRU} < D_{th} \\ P_1: PMU\ U_j\ is\ not\ compromised, & otherwise \end{cases}$$

Here,$\boldsymbol{D_{th}}$= Detection threshold.

Algorithm 2 : PRU Algorithm

Procedure

Input: $\eta_t\,, {}^{o-1}_{t}\aleph\,, \eta_f\,, {}^{o-1}_{f}\aleph\,, S^{t-1}_{f}\,, \vartheta$

if the Current Observed data is "True" **then**

  ${}^{o}_{t}\aleph \leftarrow {}^{o-1}_{t}\aleph + 1$;

  $S^{t}_{f} \leftarrow 0$;

else

  ${}^{o}_{f}\aleph \leftarrow {}^{o-1}_{f}\aleph + 1$;

  $S^{t}_{f} \leftarrow S^{t-1}_{f} + 1$;

  if $S^{t}_{f} > 1$ **then**

    $\eta_f = \eta_f^{t-1}\,.\,e^{\vartheta}$;

  end if

end if

Compute Updating Reputation level by:

$T^{o}_{up} = \frac{1 + \eta_t\,.{}^{o}_{t}\aleph}{1 + \eta_t\,.{}^{o}_{t}\aleph + \eta_f\,.{}^{o}_{f}\aleph}$

and the Overall Reputation Level by:

$T_{PRU} = \ \omega\,.\delta - \beta\gamma\, tan\left(\frac{\pi\alpha}{2}\right) + \ (1 - \omega)\,.\frac{1 + \eta_t\,.{}^{o}_{t}\aleph}{1 + \eta_t\,.{}^{o}_{t}\aleph + \eta_f\,.{}^{o}_{f}\aleph}$.

Output: T_{PRU} .

end procedure.

VII. INITIAL EVALUATION

A. Network traffic Overhead in Blockchain

In the blockchain, the substantial system traffic over-burden that originates from the various hubs of the systems that partake in the accord calculation. Here we estimated traffic over-burden for the sidechain because the sidechains include with validator hub. In this trial, the pace of access demands rate expected not exactly the information creation exchanges inside the sidechains. Monax is used for business purpose and the risk network aims to be used in a scalable public network. Here, we assumed network traffic has a variable number of nodes in the sidechain and the different number of access requestincoming per minute. Our observation of the experiments is in Figures 5 smaller than the traffic overhead of Monax. High network overload in Monax because the Tendermint consensus engine sending empty blocks to check if a peer is up. In our experiment, we get network traffic with a variable number of nodes in the fellowship network, and a variable amount of access request incoming per minute.

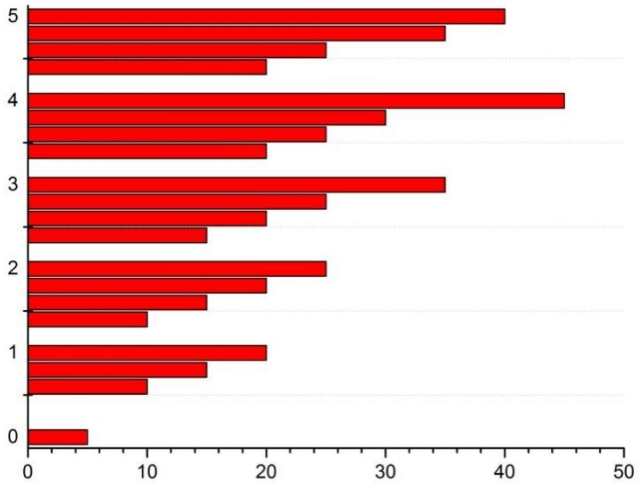

Fig. 6: Network traffic overhead in Monax.

B. Applying the Rules for Fuzzification

In “Fig. 7" we define six inputs and one output which also shown the membership function of the corresponding input and output.

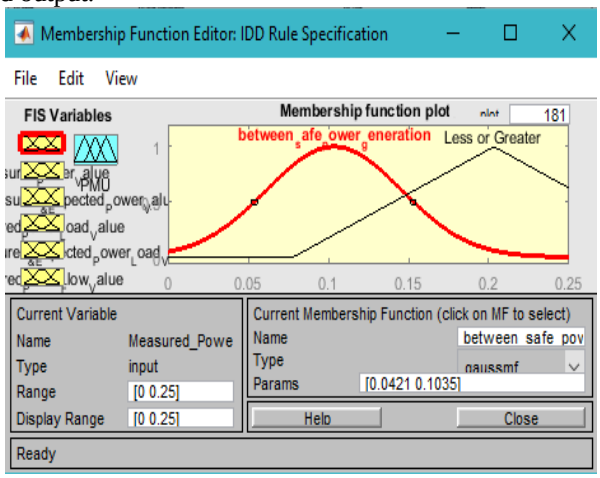

Fig. 7. Considered Input and Output and Membership Function Definition for Fuzzy Inference System.

Then we also view the rules graphical representations and surface view as shown in "Fig. 8 and 9”.

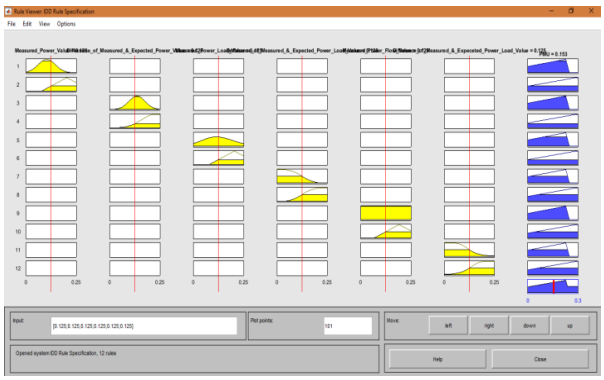

Fig. 8.Behaviour rule specifications according to conditions and surface view.

C. Fuzzification for IDD Algorithm

Then we also simulate the behaviour rule specification results for the IDD algorithm. After defining the membership function we select and specify 3 consequent behaviour rules. Then we also view the rules graphical representations and surface view as shown in "Fig. 10”.

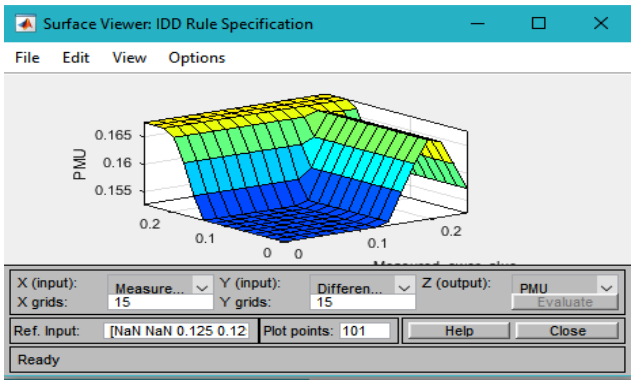

Fig. 9.Behaviour rule specifications according to conditions and surface view.

D. Fuzzification for PRU Algorithm

To find out infected or compromised PMU we simulate behaviour rule specifications results. We define one input with its two membership functions which defined the real-time PMU status according to the threshold and one output also with its two membership functions which defines the GOOD and INFECTED PMU. "Fig. 11” and “Fig. 12”shows the rules graphical and surface view as well.

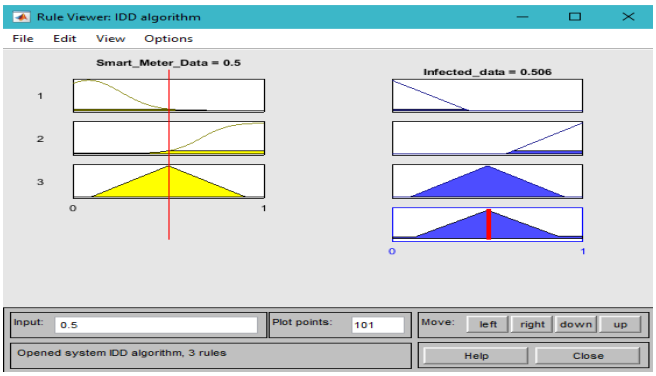

Fig. 10.Behaviour rule specifications graphical view for IDD.

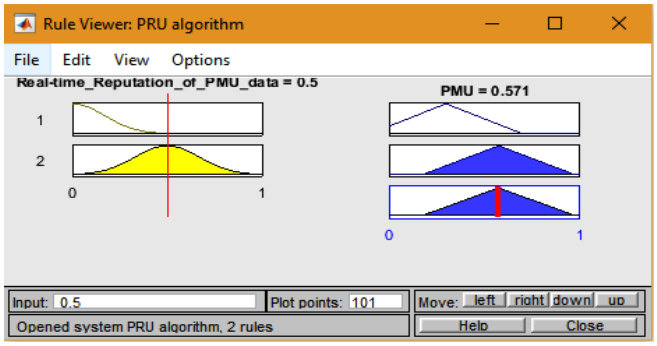

Fig. 11.Behaviour rule specifications graphical view for PRU.

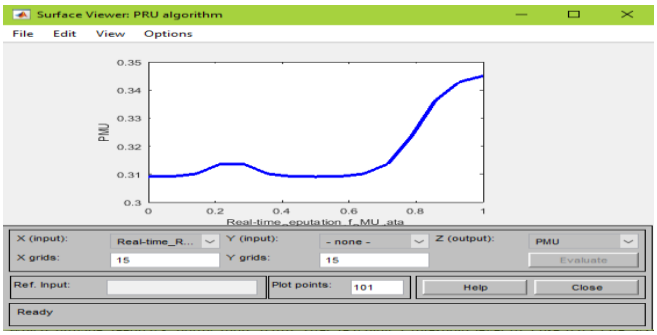

Fig. 12.Behaviour rule specifications according to conditions and surface view.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we proposed a Distributed Authorized Metering Protocols for False Data Detection and Separation for ubiquitous Smart grid infrastructure which is including three-stage security barriers. Signature scheme for remote access and infected or false data detection method in smart grid CPS based on rule behaviour specified by the Fuzzy Interference System (FIS) approaches and reputation system PRU algorithm to detect the infected or compromised PMUs. This provides feedback notification alarm after reaching a threshold level of false data rate. Existing protocols are vulnerable to PDC compromised attack; however, our proposed protocols are to be robust against attacks of this nature. Our future works would include extending the proposed approaches to capture power system faults like an open circuit, short circuit, and voltage disturbance. We will also be conducting experiments to implement our proposal protocols and to evaluate their performance.

REFERENCES

1. Beibei Li, R. L.-K. (December 20, 2016). Distributed Host-based Collaborative Detection for False Data Injection Attacks in Smart Grid Cyber-Physical System. Journal of Parallel and Distributed Computing., 11-20.Binod Vaidya, D. M. (2016, December 15). Secure Communication Mechanism for Ubiquitous Smart Grid Infrastructure. Springer Science+Bussiness Media, LLC 2011, 444-449.
2. Esposito, C., Castiglione, A., F.Palmeri, & M. Ficco. (2015, 12 04). Trust management for distributed heterogeneous systems by using linguistic term sets and hierarchies, aggregation operators and mechanism design. Future Gener. Comput. Sysst.IK. Elissa, “Title of paper if known,” unpublished.
3. Fiat A Shamir A. (1987). How to prove yourself: practical solutions to identification and signature problems. Advances in Cryptology- Proc of Crypto'86.
4. Hyo Jin Jo, I. S. (May 2016). Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems. IEEE Transactions on Smart Grid, Vol. 7, NO. 3.
5. M. E. Baran A. W. Kelley. (1994). State estimation for real-time monitoring of distribution systems. IEEE Trans. Power App. Syst. 9(3), 1601-1609.
6. Liang, G., Zhao, J., Luo, F., Weller, S., & Dong, Z. Y. (2017). A review of false data injection attacks against modern power systems. IEEE Transactions on Smart Grid.
7. Premarathne, U. S., Khalil, I., & Atiquzzaman, M. (2016). Trust-based reliable transmission strategies for smart home energy consumption management in a cognitive radio-based smart grid. Ad Hoc Netw. 41, 15-29.
8. Loise Axon. 2015. Privacy-awareness in Blockchain-based PKI. Retrieved April 12, 2017, from http://goo.gl/3Nv2oK.
9. Marco Conoscenti, Antonio Vetro and Juan C. D. Martin: Blockchain for the Internet of Things: A Systematic Literature Review. In Proceeding of The Third International Symposium on Internet of Things: Systems, Management, and Security (IOTSMS-2016). Agadir.
10. Shezan, S., N. H. Khan, M. T. Anowar, M. H. Delwar, M. D. Islam, M. H. Reduanul, M. M. Hasan and M. A. Kabir (2016). "Fuzzy Logic Implementation with MATLAB for Solar-Wind-Battery-Diesel Hybrid Energy System." Imperial Journal of Interdisciplinary Research (IJIR) 2(5): 574-583.
11. Shafagh Hossein, Anwar Hithnawi, and Simon Duquennoy. 2017. Towards Blockchain-based Auditable Storage and Sharing of IoT Data. arXiv preprint arXiv:1705.08230 (2017).
12. Anwar, A., Mahmood, A. N., & Pickering, M. (2017). Modelling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements. Journal of Computer and System Sciences, 83(1), 58-72.

AUTHORS PROFILE

Md Sakilur Islam Sarkar, received his Bachelor from the Department of Information and Communication Technology (ICT) of MawlanaBhashani Science and Technology University (MBSTU). His research interest includes Smart Grid Security, Cybersecurity, Cryptography, Blockchain, and the Internet of Things.

Ziaur Rahman, is currently a PhD Candidate at RMIT University, Melbourne, and an assistant professor of the Department of ICT, MBSTU, Bangladesh. He was graduated from Shenyang University of Chemical Technology, China, in 2012 and completed Masters in Computer Science from IUT, OIC in 2015. His research interests are Blockchain, IoT, and Cybersecurity.

Shezan Arefin, is the researcher of Electrical and Electronic Engineering dept. of RMIT University, Melbourne, Australia. He was a lecturer of Electrical and Electronics Engineering Dept. of Uttara University, Dhaka, Bangladesh. He received his Master of Engineering degree from University of Malaya, in 2016. Moreover, he received his Bachelor of Engineering degree in Electrical Engineering and Automation from Shenyang University of Chemical Technology, China, in 2013. His research interests are Microgrid, HRES, Solar Energy, Wind Energy etc.

Md. Selim Hossain, Md. Selim Hossain has been working as a Lecturer in Department of Computer Science and Engineering at KhwajaYunus Ali University, Sirajganj, Bangladesh. He completed his B.Sc. degree on Telecommunication and Electronic Engineering from Hajee Mohammad Danesh Science and Technology University, Dinajpur, Bangladesh and M.Sc. (Engg.) on Information and Communication Technology from MawlanaBhashani Science and Technology University, Tangail, Bangladesh. His main research interest is based on IoT, Blockchain, Cryptography and Network Security, Antenna, Algorithm and Software Engineering.

Dr. Md. Mahabub Hossain, Dr. Md. Mahabub Hossain is currently working as an Associate Professor and Head in Department of Electronics and Communication Engineering, Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh. He completed his Ph.D. in Semiconductor and Display Engineering, School of Electronics Engineering, Kyungpook National University, South Korea and M. Sc. in Applied Physics & Electronic Engineering, Rajshahi University and B. Sc. (Honours) in Applied Physics & Electronics, Rajshahi University, Bangladesh.