Verification-based data integrity mechanism in smart grid network

El Yazid Dari*

Faculty of Sciences,
Abdelmalek Essaadi University,
Tetuan, 93020, Morocco
Email: da.elyazid@gmail.com
*Corresponding author

Ahmed Bendahmane

Laboratory of Applied Sciences and Education,
Higher Normal School,
Abdelmalek Essaadi University,
Tetuan, 93150, Morocco
Email: ab.dahmane@gmail.com

Mohamed Essaaidi

College of IT (ENSIAS),
Mohamed V University,
Rabat, 10170, Morocco
Email: Mohamed.Essaaidi@um5.ac.ma

Abstract: The integration of open communication infrastructures and bidirectional communication between smart metres and utilities in smart grids is very important to support vast amounts of data exchange. It also increases the openness and opportunity of resource sharing across smart grid users, which makes the network vulnerable to several cyber-attacks. These cyber-attacks target smart metres data integrity through several known threats. The most known threats are false data injection (FDI) attacks that manipulate, modify or destroy data by some malicious users. Therefore, these attacks make the smart metres behave maliciously to return false data and to sabotage the system functions. In this paper, we propose a new approach to improve the integrity of data generated by smart metres in a smart grid, namely, verification-based data integrity mechanism (VBDIM). The performance of our approach is evaluated through simulation to investigate the effects of collusive smart metres on the correctness of their generated data. The obtained results show that our approach achieves a lower blacklisting error and error-rate, and better performance in terms of overhead and slowdown.

Keywords: smart grid; smart metres; cyber-security; vulnerability; data-integrity.

Reference to this paper should be made as follows: Dari, E.Y., Bendahmane, A. and Essaaidi, M. (2021) 'Verification-based data integrity mechanism in smart grid network', *Int. J. Security and Networks*, Vol. 16, No. 1, pp.1–11.

Biographical notes: El Yazid Dari received the 'DESA' degree in Electrical Engineering from the university Abdelmalek Essaadi of Tetuan. Currently he is working toward his PhD degree with the Information and Telecommunication Systems Group at Abdelmalek Essaadi University. His research interests include the smart grid security, computer sciences and telecommunications.

Ahmed Bendahmane received his PhD in Computer Sciences from Abdelmalek Essaadi University at Information and Telecommunication Systems Laboratory, Faculty of Science, Tetuan, Morocco (2013). His main research interests include distributed systems, security of grid and cloud computing systems, computer networks, intrusion detection and tolerance, and multi-agent systems. He has published a number of refereed research publications in this area.

Mohamed Essaaidi has been the Dean of ENSIAS College of IT Engineering of Mohammed V University in Rabat, Morocco (November 2011–May 2019), a Professor of Electrical and Computer Engineering at Abdelmalek Essaadi University in Tetuan, Morocco (2001–2011) and the past Chairman of the IEEE Morocco Section (2005–2015). He has authored and co-authored seven books and more than 200 papers, and he holds ten patents. He is also an active member of the editorial boards of several international journals. Furthermore, he is the Founder and the General Chair/Co-chair of several IEEE technically sponsored international conferences.

1 Introduction

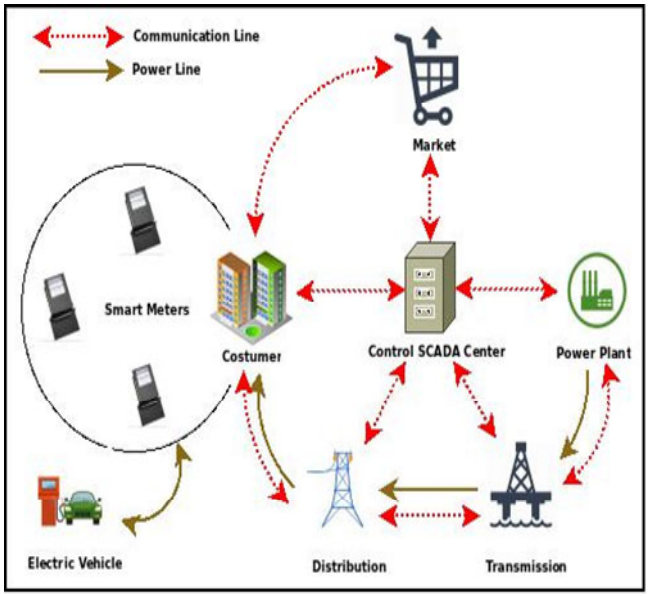
In a smart grid (Figure 1), a large number of users with different applications make it vulnerable to sabotage attacks by data modification or destruction and false data injection as cited in Liu et al. (2011). The smart grid resources manipulation might be sabotaged by injecting false data and by attempting to get favourable results by accessing smart metres' applications and by modifying the generated data. This may have several effects such as decreasing the amount of electricity consumed or changing the price or even causing a blackout. Therefore, the requirements for smart grid security, trust and reliability are really very high despite several existing control and security mechanisms allowing to secure communications and to provide confidentiality, and data integrity. For instance, in order to improve the trustworthiness of the smart grid system it is extremely important to develop some mechanisms that can guarantee the correctness and reliability of data generated by smart metres.

Nowadays, voting techniques are commonly used for sabotage-tolerance as cited in Sarmenta et al. (2002), to deal with the verification of the reliability of job results in many grid systems. Simple voting techniques such as majority voting and m-first voting replicate a job to a number of independent resources and the returned results are checked for a majority decision as cited in Zuev (1998). These techniques are expensive in terms of resource utilisation and thus decrease the performance of grid systems. Other important voting-based techniques using spot-checking as in credibility-based voting with reputation system as cited in Sarmenta et al. (2002) and Sonnek et al. (2007), were proposed to reduce the replication overhead so as to improve the efficiency of resource utilisation.

However, these techniques rely on the assumption that the grid resources behave independently which is not valid where a number of collusive smart metres collectively return the same wrong data. Furthermore, sometimes the decision of voting-based techniques may not be exact as stated in several works (Silaghi et al., 2009; Canon et al., 2011; Araujo et al., 2011; Bendahmane et al., 2010). Therefore, one group of smart metres in a smart grid might develop some form of collective misbehaviour to sabotage the circulated data by returning the same wrong results. In fact, in order to deal with this threat it is necessary to explore the sabotage-tolerant techniques against collusive smart metres in a smart grid.

In this paper, we propose a verification-based data integrity mechanism (VBDIM) to improve the integrity of data generated by smart metres in a smart grid. The mechanism proposed verifies and controls the data generated to prove its correctness and reliability in order to check the effect of false data injection on the correctness of smart grid data. This approach is based on a spot-checking-based technique to improve the credibility-based voting with periodical checking of the data generated by the smart metres, and by sending them a spotter request whose correct data is known. The credibility and trustworthiness of every single smart metre is estimated based on the data it returns. The bottom-line idea behind the proposed approach is to use the result of voting decision instead of that of spot-checking to estimate the credibility of the smart metres. The voting decision is based on the weighted average voting method as stated in Lorczak et al. (1989), while the smart metre credibility, which is considered as a reputation, is used as a weight for it.

Figure 1 Smart grid network (see online version for colours)



The rest of this paper is organised as follows. Section 2 presents a background of voting and credibility techniques, and gives a brief overview of related research work. Section 3 presents the smart grid and the attacks models. Section 4 details the proposed approach for the verification of smart metres data integrity. Section 5 investigates the performance of the proposed technique. Finally, Section 6 presents the main conclusions of this research work.

2 Background and related work

2.1 Sabotage tolerance

Sabotage-tolerance techniques are applied in all kind of distributed computing systems such as MapReduce for desktop grid computing as cited in Moca et al (2011) and Wang and Wei (2011), desktop grids as stated in Domingues et al. (2007), Choi et al. (2010) and Kondo et al. (2007), volunteer computing as cited in Sarmenta et al. (2002) and Son et al. (2008), and peer-to-peer grids as cited in Oliveira et al. (2009) and Zhao et al. (2005). In these systems different administrative domains have conflicting interests. These techniques assume that the computing framework is based on a master-slave model, where a job or a computation is divided into sets of N independent tasks that have the same size.

This model can be explained as a server, the master or the SCADA centre control in our approach that distributes the tasks of an application to a set of computing resources (workers or smart metres). These smart metres return the

corresponding set of results (data in our approach). In sabotage-tolerance techniques, a result error is any result returned by one of a faulty fraction f of the W workers assumed to be malicious. Then, these techniques imply the detection of the smart metres which behave maliciously and return false results with a constant probability s, called the sabotage rate.

Voting-based techniques (replication) are considered among sabotage-tolerance approaches. As examples of these techniques, which are related to our approach, there are m-first voting and credibility-based voting detailed in the subsections below.

2.2 m-first voting

The m-first voting technique, widely used in the real BOINC desktop grid platform, as cited in Watanabe et al. (2009), can bring a low error rate when malicious grid resources are independent from each other. The main idea of this technique is replicating each task (query in our approach) to several computing resources to execute the same task.

The returned results for a specific query are then classified into groups according to their values. The execution of a query is repeated until one of the result groups collects enough m matching results accepted as the best result. This voting method is simple in terms of implementation but it has some flaws that dissipate a lot of resources. Then, before starting the computation, the static degree of redundancy must be specified in advance.

The m-first voting always gathers a fixed number of identical results, without considering the reliability feature of each result. The computing resource reliability may be different and varies dynamically with time; thus, the fixed chosen redundancy value will result in the dissipation of a number of useful computing resources for unnecessary redundant computations as stated in Bendahmane et al. (2015).

2.3 Credibility-based voting technique

The credibility-based sabotage tolerance approach, as cited in Sarmenta et al. (2002), is a way for reducing the acceptance of wrong results as correct ones by using both spot-checking and voting techniques. This approach increases the efficiency of resources utilisation and automatically guarantees balance in term of trade-off between performance and correctness. The main idea of credibility-based voting is that the master estimates the reliability of the workers (i.e., smart metres) based on their behaviours during the computation. It is similar to m-first voting except that the number of replications, m, is not fixed but dynamically determined at the runtime in accordance with some credibility values given to different elements of the grid: worker, result, result group, and task. These credibility values, which represent the reliability rates, are principally based on the number of spot-checks given to workers and their past behaviour.

In order to check the credibility of workers, the master assigns a spotter task to a worker with probability q. If one worker returns a result for the spotter task, which does not match the correct one, the master can score the worker as a saboteur or a malicious one. Therefore, the master may use two policies as stated in Bendahmane et al. (2015):

1 the master may use the backtracking policy to reject all results received from the saboteur because each result might be an inaccurate one

2 the master may use the blacklisting policy to include detected malicious workers into a blacklist to prevent them from returning results or getting other tasks or queries.

The credibility of a worker ω_i, which correctly computed k_i spotters, is an estimate of the probability the worker will return a correct result, and is given by the following equation as cited in Sarmenta et al. (2002):

$$CR = (\omega_i, k_i) = \begin{cases} 1 - \dfrac{f}{1-f} \cdot \dfrac{1}{k_i e} & \text{if } k_i \neq 0 \\ 1 - f & \text{otherwise} \end{cases} \quad (1)$$

where e is the base of the natural logarithm.

The credibility of a result is the conditional probability that the result coming from a worker will be accepted as correct and is equal to the credibility of the worker, which returns this result. The credibility of a result group is the conditional probability that this result is correct.

Ultimately, the credibility of a task is defined as the credibility of the group having the highest credibility as stated in Sarmenta et al. (2002). The final voted results would be accepted by the system only if the task credibility reaches a threshold θ defined by the maximum accepted error for the result. Besides, this approach can mathematically ensure that the error rate will not exceed a given acceptable value.

In the credibility-based sabotage tolerance mechanism, the spot-checking technique is used effectively to detect malicious workers or saboteurs. In contrary, spotter jobs are extra tasks that dissipate the computing systems resources and then deteriorate their performance because they are producing several kinds of spotter tasks requiring extra task computations on trustworthy resources. However, this mechanism works under the assumption that the saboteur never distinguishes spotter tasks form the real ones. This fact also degrades the system performance. If there are a limited number of spotter tasks, a saboteur may easily identify spotter tasks since the same spotter task is frequently allocated to the same saboteur. In this way, a saboteur may return correct results only for spotter tasks to gain a high credibility value and then submits wrong results for the real tasks as stated in Bendahmane et al. (2015).

2.4 Related works

The problem of smart grid integrity attacks is related to several known threats such as false data injection attacks.

These attacks attempt to manipulate, modify or destroy the provided data by some malicious users. Several researchers have addressed these attacks during the last few years.

Liu et al. (2012) give an overview of cyber security and privacy issues in the smart grid. Therefore, authors discuss several potential research fields for understanding of system components and associated cyber-vulnerabilities. Finally, they conclude that almost every aspect related to IT technology in the smart grid has potential vulnerabilities due to inherent security risks in the general IT environment. Another work presented by Gao et al. (2012) they present a systematic review of communication/networking technologies in smart grid, including communication/ networking architecture, different communication technologies that would be employed into this architecture, quality of service (QoS), optimising utilisation of assets, control and management, etc. that have been proposed by other quality researchers.

Yang et al. (2016) have proposed a novel defensive scheme, namely, Gaussian-mixture model-based detection scheme against data integrity attacks. This approach is more efficient and accurate compared to existing schemes when the fluctuation of data is high. This is because it leverages the Gaussian-Mixture model to cluster the historical data and to learn the minimum and maximum values of individual clusters. In addition, this scheme does not require a pre-defined threshold or external knowledge to label historical data, via a combination of both theoretical analysis and simulated experimentation. The obtained results show that this scheme can effectively detect the false injected data in the advanced metering infrastructure (AMI). In addition, these results demonstrate that Gaussian-mixture model-based detection scheme can achieve a higher detection rate, and lower error rate, in comparison with existing schemes based on the min-max model.

A state summation strategy for detecting false data injection attacks and the smart metre integrity problem was also proposed by Li and Wang (2014). This approach is based on the use of two detectors to detect attacks using state variables distributions to detect sparse attacks and to secure smart metres. In this approach the problem was formalised as a hypothetical test of standard normal distribution with empirical data and the effectiveness of the proposed detectors was verified against classical detectors. The main contributions of this work can be summarised in two main points, as stated in Py et al. (2015):

1 For different power systems, two methods are discussed and analysed. The state summation detection (SSD) and single state detector (SiSD) are jointly used at the same time. For large power systems, it is effective to divide it into small or median blocks to defend against false data attacks (FDA).

2 The historical data of a power system can be used to detect FDA. The essence of FDA is discussed in the last experiment which disguises itself as normal running data of power system in accordance with network topology. The more stable and regular the power system is, the more difficult FDA is to hide itself. Also FDA is difficult to successfully implement owing to the need for large information about network configuration and running regularity of the power system. In addition, a spatial-temporal correction based scheme is proposed for detecting false data injection attacks.

Huang et al. (2013) focused on the important security problem of bad data injection attacks in smart grid based on strategies of defenders and attackers. From the defender's perspective, an adaptive cumulative sum test is able to determine the possible existence of adversaries at the control centre as quickly as possible. From the attacker's point of view, independent component analysis is employed for the attackers to make inferences through phasor observations without prior knowledge of the power grid topology. The inferred structural information can be used to launch stealth attacks. The result of simulations successfully demonstrates that the defender can detect real-time malicious data attack within the minimum delay. From the attacker's perspective, they investigated the linear independent component analysis (ICA) technique so that the attacker can perform a stealthy attack without knowledge of the system topology. They demonstrated that the proposed attack can be accomplished by learning the topology structure of the power system and is difficult to detect. Hao et al. (2015) confirmed that the cumulative sum (CUSUM) test-based detection mechanism introduced and is also useful for non-stealth attacks.

Sou et al. (2013) considered a smart grid cyber-security problem analysing the vulnerabilities of electric power networks to false data attacks. This problem is related to a constrained cardinality minimisation problem with a relaxation technique that provides an exact optimal solution to this cardinality minimisation problem. The proposed result is based on a polyhedral combinatorics argument. It is different from well-known results based on mutual coherence and restricted isometric property. One of the main distinctions is that this approach makes an assumption that no bus injections are metered. The current result requires a different assumption that the network is fully measured (i.e., all bus injections and line power flows are metered). Based on that, Hendrickx et al. (2014) proposed an approach that confirms the conjecture by showing that the security index is indeed NP-Hard, and provides an efficient heuristic algorithm for the general NP-hard problem.

3 System model

3.1 System components and architecture for a secure smart grid

The smart grid (Figure 1) is an emerging technology that is revolutionising the conventional electric grid by providing new services based mainly on information and communication technologies (ICT), which is considered to be its main enabler as stated in Hao et al. (2015). This is a

very complex network for energy generation, transmission, distribution and consumption. Besides the different opportunities and advantages offered by ICT, Smart grid suffers from its inherent challenges, especially at the level of cyber-security.

In fact, there are several security attacks that could compromise this system's integrity and more specifically smart metres integrity.

Figure 2 Basic components of a smart grid network (see online version for colours)

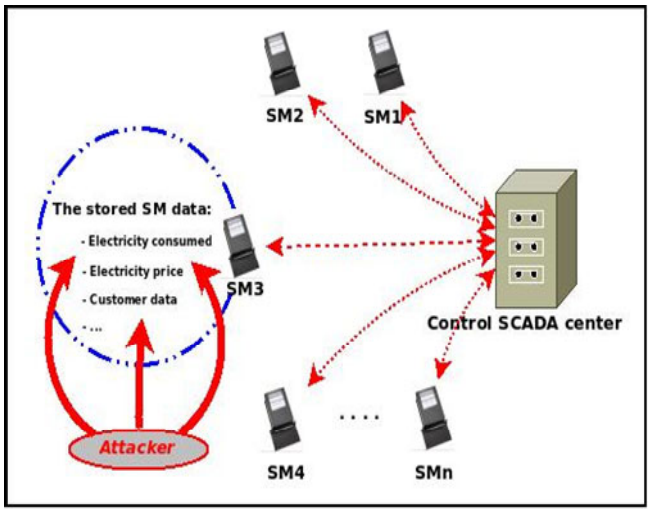


Figure 2 shows the basic components of a smart grid system, which consists of N Smart metres. Each smart metre is connected to a set of local devices or appliances, which are able to communicate with other smart metres via a home area network (HAN). These smart metres analyse and measure data about energy usage, number of appliances, energy pricing, etc., and stores all these data periodically. In addition, these stored data must be returned to a supervisory control and data acquisition (SCADA) centre in order to monitor and control these collected data in real-time, and provide high security information communications between users and utilities.

In smart grid, electricity produced in the power plant, input from distribution substation to a smart metre and then distributed to all appliances (e.g., washing machine, water heater, electric mixer, ...).

The quantity of the energy consumed in a location is calculated by the smart metre, taking into account the price of the energy on the market during the specific time of this consumption. In addition, the HAN can supply and sell extra energy to the power grid in order to benefit from high energy prices in electricity markets that encourage competition among power suppliers as cited in Dari and Essaaidi (2015).

3.2 Attacks model and assumption

In smart grid, malicious attackers or users who can launch security attacks to its infrastructure. In this paper, we focus on smart metres attacks that compromise the provided resources and services by exploiting some of their vulnerabilities. In this attack model, we have an adversary, which can compromise the smart metres, and instruct them to behave maliciously to tamper their data such as the amount of energy consumed, electricity price in the market, etc. and to return wrong data.

We assume that the 'honest' smart metres always produce the same correct data for the same query, whereas the malicious ones may return different wrong data, the number of which does not exceed half of the available smart metres in the entire smart grid. This assumption is eventually required to decide about the correctness of the data sent and to determine which smart metres are malicious and which are honest.

In our grid, we assume that the SCADA control centre sends randomly queries to smart metres to return their data at a time t. The smart metre memory stores both their data at random instances, and all data captured at the SCADA control centre. When a smart metre receives one of these queries, it executes respectively the following tasks:

- *Step 1*: It captures existing data at the same time *t*.
- *Step 2*: It returns this data captured at this time *t* and those stored at the time $t - 1$ (stored in the memory of the smart metre).
- *Step 3*: It stores the data captured at this time *t* in its memory.

The SCADA centre receives the data sent by the smart metres, stores the data captured at time *t*, and checks whether the data captured at instant $t - 1$ is identical to the data already stored.

Several methods have been proposed to verify data-integrity against malicious behaviours attacks. The voting-based techniques are used for sabotage tolerance in various open systems such as grid, cloud and volunteer computing system. In the case of collusion attacks, the credibility-based-voting technique gives good results. Then, we propose, in this paper, to adopt this technique to verify data-integrity in smart grid.

In addition, we assume that all malicious smart metres always collude with one another to return incorrect data.

4 Proposed approach: VBDIM

The new approach we propose, namely, VBDIM is based on a spot-checking-based technique. This approach improves the credibility-based voting (CBV) to achieve a low error-rate with a very low overhead.

Table 1 Verification-based data integrity mechanism algorithm

1	Ld is the list of demands to run
2	LSM is the list of smart metres
3	$R_i = 1 - f$ and $k_i = 0$ for each $SM_i \in LSM$; according to (2)
4	**initialise**( )
5	**while** (there is $d_k \in Ld$ without accepted data) **do**
6	demands scheduling( )
7	data receiving and decision for acceptance( )
8	**end while**
9	**initialise**( )
10	**while** ($SM_i \in LSM$) and (there is demand d_o without accepted data) **do**
11	send d_o to all SMs
12	receive data sent from all SMs and store its
13	**end while**
14	**demands scheduling**( )
15	**while** ($SM_i \in LSM$) and (there is demand $d_k \in Ld$ without accepted data) **do**
16	send d_k to m random SMs
17	**if** SM_i is not blacklisted **then**
18	d_t = a replica of d_k
19	assing d_t to SM_i
20	**end if**
21	**end while**
22	**data receiving and decision for acceptance( )**
23	**while** (there is a running demand) **do**
24	//waiting to receive data from a smart metre SM_i
25	for each d_t executed for a demand d_k do
26	receive a $data_t$ and $data_{t-1}$
27	Comput V_j
28	compute $R(V_j)$ according to (3)
29	compute max($R(V_j)$)
30	**If** $\frac{\max\left(R\left(V_j\right)\right)}{\sum_1^m R_i} > \alpha$ **then**
31	accept V_j^* which represent this maximum
32	update R_i of all SM_j^+ which generate V_j^* according to (6) and (3)
33	**Else**
34	if $NA_i > 0$ then
35	decrement N_{Ai} and R_i and send other replica
36	**else**
37	add all SM_i^- whose generate results different to V_j^* to the blacklist
38	repeat from **25**
39	**end if**
40	**end if**
41	**end for**
42	**end while**

Spot-checking is used in credibility-based voting to periodically check the smart metres, by sending spotter data-queries whose correct data is known, in order to estimate the credibility of each smart metre based on the returned data. The basic idea behind this approach is to check the smart metres without assigning spotter data-queries and to consider the result of voting decision as the one of spot-checking to estimate the credibility without additional operations. This credibility is considered as a reputation, which is used in the VBDIM decision. In our approach, at a time t, SCADA centre sends to the smart metre a query for the stored data, the smart metre captures the data at a time t and returns it with the data captured at time $t - 1$ (stored in the smart metre memory). The SCADA receives these two types of data, the one at the time t and that at $t - 1$, it stores the data at the time t and compares it with that at the time $t - 1$ in order to check if they are identical or they were modified or manipulated.

Table 1 summarises our VBDIM approach. In this algorithm, the smart grid system starts by, sending a d0 query to all smart metres SM_i, receiving their first data, and storing them in SCADA centre in order to initialise all these SM_i (line 4). Then, SCADA centre starts sending a number of queries for smart metres data stored ("Ld" in line 1 of Table 1), to available smart metres ("LSM" in line 2 of Table 1) for paralleled processing. After capturing the data, the smart metre returns the data at the times t and $t - 1$. The generated data will be returned to the SCADA centre control for verification and generate V_j (line 25 to 29). Until all queries are carried out with accepted data (line 10 to 13 of Table 1), the scheduling and receiving processes for each query are repeated.

Let us assume that each query is replicated n times and allocated to several smart metres SM_i, so that a SCADA centre control can collects m different data $data_j$ and compares them with those already stored, where $i = 1, 2, ..., n$ and $j = 1, 2, \ldots, m$. The resulting value of V_j for each data $data_j$ is defined as follow:

$$V_j = \begin{cases} Yes & f\ data_j^t = data_j^{t-1} \\ No & if\ data_j^t \neq data_j^{t-1} \end{cases} \quad (2)$$

The variable V_j is linked to each request j sent by SCADA centre control. Then, V_j is a result of the comparison of the data returned between two instants: t and $t - 1$, of the same smart metre SM_i, and of the same request j. In other words, if data $t - 1$ and datat returned in the two instants are equal, V_j returns the value 'Yes', otherwise, V_j returns the value 'No'.

Each smart metre has its reputation value R_i, which represents the overall computing behaviour. This reputation is collected by a SCADA centre control, which contains the reputation list of all smart metres connected to the smart grid. The reputation is a value in the range between 0 and 1.

According to our approach, the SCADA centre control builds the reputation of each smart metre through its credibility. The credibility represents the likelihood of a particular object of the system to be operating properly as stated in Oliveira et al. (2009). Generally, the credibility

$CR(C_i, A_i, U_i)$ of the smart metre SM_i is computed by passing a spot checking ki times. Since, we consider each query successfully verified and validated by the SCADA centre control using the VBDIM as a passed spotter query. The reputation R_i of any smart metre, which returns the correct data of A_i query and returns the false data of U_i query when blacklisting is used, will be computed using the following equation:

$$R_i = CR(SM_i, A_i m, U_i) = \begin{cases} 1 - \dfrac{f}{1-f} \cdot \dfrac{1}{(A_1 - U_1)e} & \text{if } A_i > U_i \\ 1 - f & \text{if } A_i = U_i \\ \dfrac{f}{1-f} \cdot \dfrac{1}{(U_1 - A_1)e} & \text{if } A_i < U_i \end{cases} \quad (3)$$

where f is the proportion of malicious smart metres and e is the base of the natural logarithm.

In the initial time, each smart metre has $A_0 = U_0 = 0$ and while a smart metre SM_i returns accepted data, the number $A_i - U_i$ increases, then its reputation increases too. In contrast, while it returns unaccepted data, the number $U_i - A_i$ increases, then its reputation decreases.

Increase and decrease of R_i of each smart metre SM_i influences clearly in the voting decision to accept or not accept the returned data by the SM_i for the request j.

In order to make a decision about which data $data_j$ is trustworthy, the SCADA centre control utilises an m-first voting approach based on reputation decision criteria. We define the result reputation $R(V_j)$ of captured data $data_j$ as the summation of reputations of smart metres returning the result V_j of the data-sent $data_j$.

For each result V_j:

$$R(V_j) = \sum_{i=1}^{n} R(V_j, SM_i) R_i \quad (4)$$

where $T(V_j, SM_i)$ is the relationship between the result V_j and the smart metre SM_i, which is computed as follow:

$$T(V_j, SM_i) = \begin{cases} 1 & \text{if } V_j = Yes \\ 0 & \text{if } V_j = No \end{cases} \quad (5)$$

For each query j, all selected smart metres return data to compare with those stored in SCADA control centre memory. After comparison, we have two values of V_j: 'Yes' and 'No', and the reputation of the value 'Yes' is calculated by summation of the R_i of the smart metres returned accepted data multiplied by 1. For $R(V_j)$ of the value 'No' is zero.

The SCADA control centre uses the reputation-based approach for further replications, and uses the reputation value of each smart metre to decide which data are accepted as correct. Moreover, each time the SCADA control centre receives new data $data_j$ which have a value V_j for query replica, it recalculates the result's reputation value $R(V_j)$. We denote α as the desired control threshold ($0 < \alpha < 1$) and we pick the result value with the highest reputation $\max(R(V_j))$ as the best result.

If $\dfrac{\max(R(V_j))}{\sum_1^m R_i} > \alpha$, then the result value which represents this maximum is accepted by the SCADA control centre and is considered to be the correct one (lines 30 to 31 of Table 1).

In addition, the reputation of all smart metres, which generate this result, is updated as follows (line 32 of Table 1):

$$R_i = CR(SM_i, A_i + 1, U_i) \quad (6)$$

In the case where we have unaccepted data, the SCADA decrements the reputation of each smart metre SM_i returning the wrong data as follows (line 35 of Table 1):

$$R_i = CR(SM_i, A_i, U_i + 1) \quad (7)$$

In addition, R_i increase by incrementing A_i by 1 of each smart metres that returns accepted data. Otherwise, R_i decrease by incrementing U_i by 1 for each smart metres SM_i that returns unaccepted data.

In addition, we authorise each smart metre to have an acceptable number of attempts with false results (see simulation setting Section 5.1). In the case where we have false received data $data_j$, they will be destroyed and the SCADA decrements NA_i (NA_i --), while $NA_i > 0$, the erroneous data of the smart metre will be analysed (line 34 to 35 of Table 1), if $NA_i = 0$ the SCADA control centre will be blacklisting the smart metre (line 37 of Table 1).

Finally, it will blacklist the smart metres whose data were not validated by the VBDIM.

Contrarily, where no result reach the level to be accepted as correct one, $\dfrac{\max(R(V_j))}{\sum_1^m R_i} < \alpha$, the SCADA control centre should require another replication of the query until the data are accepted (line 5 to 42 of Table 1).

Moreover, our approach guarantees that the query replicas are not assigned to the same smart metres.

In order to obtain the best performance and prevent the acceptance of wrong data in the presence of low reputed smart metres, we must run several experiments and select the best control threshold α, which should be greater than 0.5 and lower than 1.

5 Performance evaluation

In this section, we evaluate the performance of our approach through simulations of a smart grid system.

The main objective of our simulation is to evaluate the effectiveness of the proposed approach by several performance metrics such as, overhead, slowdown, error rate, honest blacklisting error and malicious blacklisting error.

1 The overhead is defined as the ratio between the total numbers of queries assigned for execution and the original number of queries.

2 Slowdown is defined as the ratio between the running times of computation with and without the use of control mechanism.

3 The error rate is defined as the number of the accepted wrong data divided by the total number of the required data returned at the end of the job of control threshold computation.

4 The honest blacklisting error is defined as the ratio between the number of honest smart metres in the blacklist and the total number of honest smart metres.

5 The malicious blacklisting error is defined as the ratio between the number of malicious smart metres in blacklist and the total number of malicious smart metres.

5.1 Simulation settings

In our simulation, we will run N jobs each with 10,000 independent queries. The job is allocated to 1,000 smart metres and the SCADA control centre which has no knowledge, and no control mechanism about the threat model parameters (i.e., f). In addition, we assume that all smart metres capture and send the same power, and respond only to one query at a time. Furthermore, we assume that all smart metres can collude with each other to generate false data.

Table 2 Units simulation parameters

Notations	*Parameter descriptions*	*Values*
f	Collusive smart metres fraction in the smart grid system	0~0.45
α	Control threshold	0~0.90
N	Number of jobs	5
NA	Number of attempts for a smart metre to return a wrong data	3
m	Number of the testing smart metres	25

In Table 2, we give all the parameters used in the simulations and the values of each parameter. In order to get more consistent and trustworthy results, the simulations for each combination of these parameters were executed 50 times and the average values were computed.

5.2 Results and discussion

5.2.1 Control threshold effect

The choice of the control threshold α is very important to guarantee an optimal level of control. Therefore, we will execute a job for different values of α and collusive smart metres fraction in the smart grid f.

Figure 3 shows the blacklisting error as a function of control threshold α for several values of f. For all values of α, the malicious blacklisting error is always equal to zero. This is due to the credibility decreasing function that decreases the credibility of malicious smart metres, which makes them, less credible in order not to influence the control threshold. Therefore, the blacklisting of malicious smart metres becomes very efficient.

Figure 3 Malicious blacklisting error as a function of control threshold α for various values of f (see online version for colours)

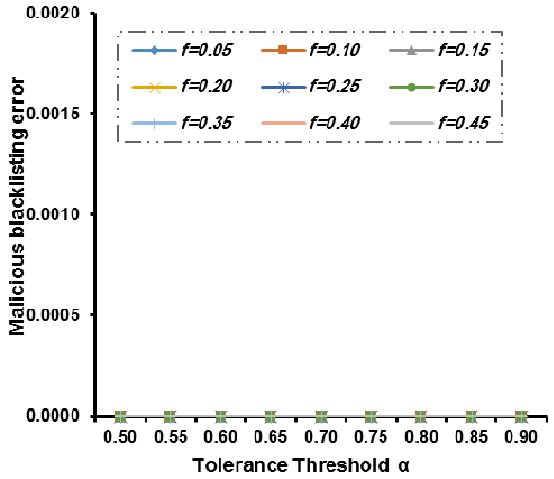


Figure 4 shows that for all values of α, the honest blacklisting error is always equal to zero, except for $\alpha = 0.50$ which also corresponds to a very small error value. Therefore, blacklisting of honest smart metres is avoided in the proposed approach.

Figure 4 Honest blacklisting error as a function of tolerance α for various values of f (see online version for colours)

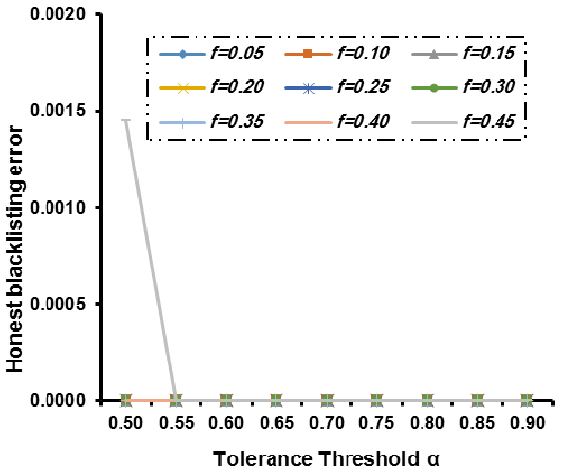


Figure 5 shows the error rate as a function of the control threshold α. For values of α ranging from 0.50 to 0.75, the error rate increases for values of f corresponding to 0.35, 0.40 and 0.45. In the case of low values of α, the malicious smart metres collude each other and can influence the SCADA control centre to accept false data. However, for values of α greater than 0.75, cooperation among honest smart metres is favoured over collusion of malicious ones.

Moreover, the error rate is zero for all f values considered in this simulation.

Figure 5 Error rate as a function of control threshold α for various values of f (see online version for colours)

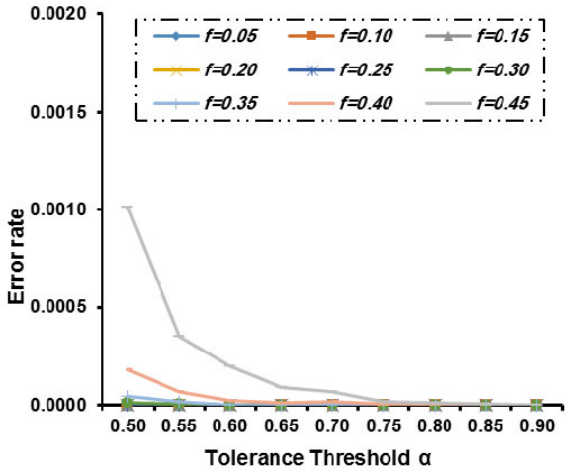
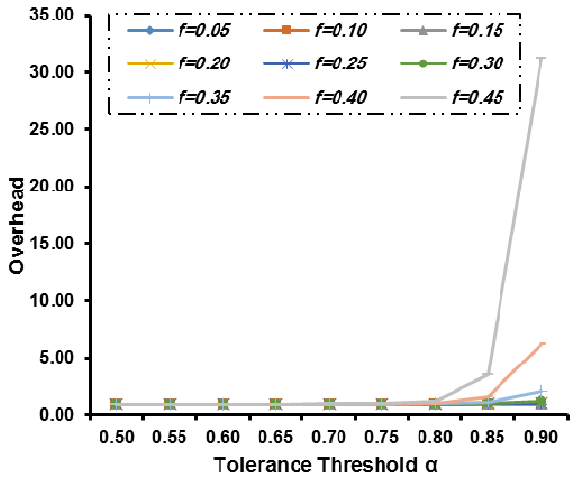


Figure 6 Overhead as a function of tolerance α for various values of f (see online version for colours)

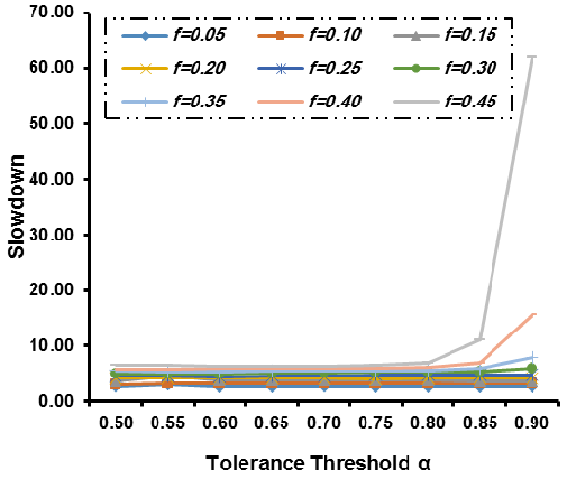


In contrast, Figure 6 shows that the overhead is equal to one for all values of f, except for $f = 0.40$ and 0.45. However, it increases strongly for these last two values of f when $\alpha = 0.85$ and 0.90. This is because to exceed the value $\alpha = 0.85$, the SCADA control centre must obtain 23 honest smart metres from the 25 randomly selected. To this end, the SCADA control centre must send an outstanding number of queries, the fact that makes the overhead very high for both values 0.85 and 0.90

Figure 7 shows that for all values of f considered, the slowdown remains constant for all values of control tolerance, except for $f = 0.40$ when the slowdown increases for the two values $\alpha = 0.85$ and 0.90. For $f = 0.45$ the slowdown increases only for $\alpha = 0.90$, since in order to exceed the value $\alpha = 0.85$, the SCADA control centre must obtain, at least, 23 honest smart metres from the 25 randomly selected. This takes considerable time, the fact that explains the high increase of the slowdown corresponding to these two values of α.

For all the preceding figures, fairly good results accuracy is obtained with errors that are equal or tend to zero for all cases of f between 0.05 and 0.45. In addition, we noticed that the values of the control threshold which gives best results are $\alpha = 0.75$ and 0.80. For these reasons, we consider the value of $\alpha = 0.80$ for the sake of effectiveness as a function of number of jobs.

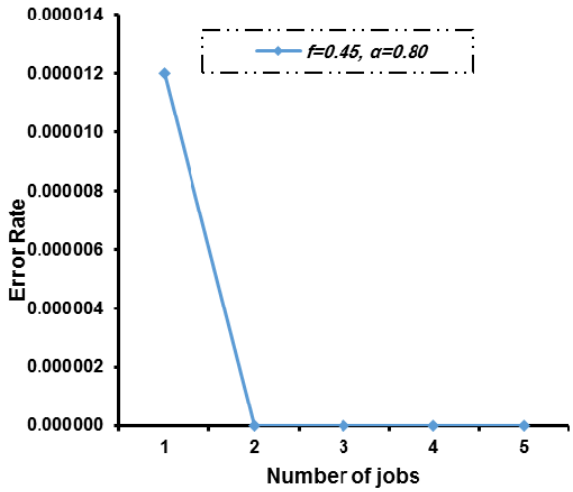
Figure 7 Slowdown as a function of control tolerance α for various values of f (see online version for colours)



5.2.2 *Performance evaluation*

For a better evaluation of the performance of the proposed approach, we compute the error rate, overhead and slowdown for all cases of control threshold in order to compare them with those obtained in five jobs.

Figure 8 Error rate as a function of number of jobs for $f = 0.45$ and $\alpha = 0.80$ (see online version for colours)



From Figure 8, we notice that for the first job, the number of erroneous data accepted by the SCADA control centre is very small in comparison with the total number of data accepted. However, for the following four jobs, the SCADA control centre does not accept any erroneous data thanks to the blacklisting of all malicious smart metres by the SCADA control centre. This is because they have been detected as malicious and then they will no longer be used in the last four jobs.

In a similar manner, Figure 9 shows that the number of queries sent by SCADA control centre is not sufficiently high, compared to the original number in the first job. In addition, the value of overhead decrease to 1, which means that the number of queries sent by SCADA control centre is equal to the number of original queries from the second job, and this remains constant for the rest of jobs, because after the execution of the first job the majority of honest smart metres gain enough reputation. In contrast, the malicious smart metres lose reputation, which in turn makes the data returned from those Smart metres accepted without further replication, so most queries are carried out with only one replica. This is explained by the absence of malicious smart metres in the last four jobs.

Figure 9 Overhead as a function of number of jobs for $f = 0.45$ and $\alpha = 0.80$ (see online version for colours)

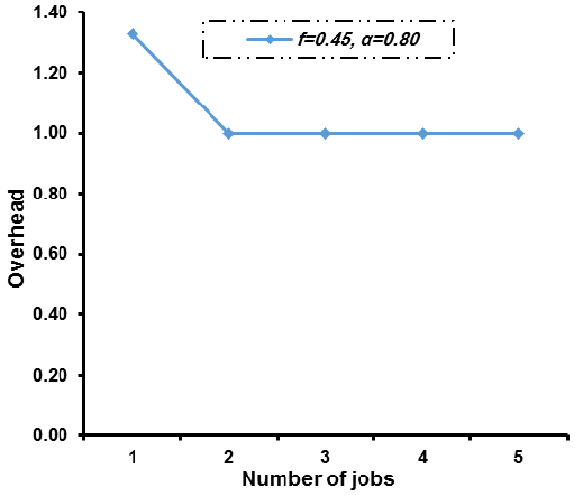
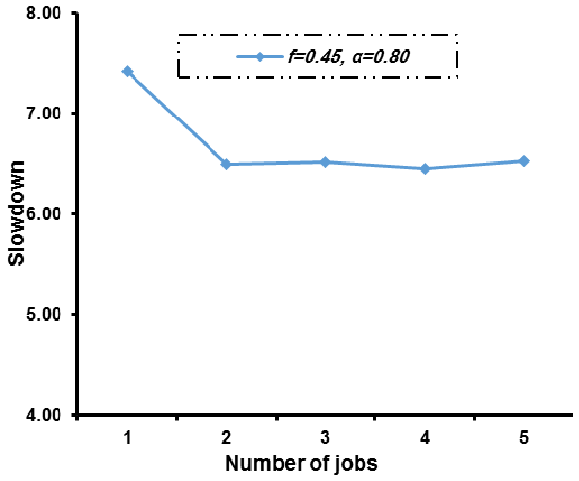


Figure 10 Slowdown as a function of number of jobs for $f = 0.45$ and $\alpha = 0.80$ (see online version for colours)



From Figure 10, the SCADA control centre needs more time to detect the saboteurs smart metres, which explain the high value of slowdown for the first job. However, after detecting of all malicious smart metres and updating of all smart metres reputation, all remaining ones will be honest and need only one replica to return the correct data. That is why we notice that the running time decreases and remains constant in the next four jobs.

6 Conclusions

In this paper, we present a VBDIM (VBDIM) for the control of collusive smart metres in a smart grid. In order to detect all malicious smart metres while maintaining low overhead and high performance, we propose an approach that uses the voting method combined with a reputation technique in the presence of collusion attacks. The voting decision of a query is generated by the reputation values of all the smart metres that participate in the answer of such a query. In addition, our approach can provide a lower error rate with better performance in terms of overhead and slowdown. Our control scheme is able to detect all malicious smart metres and to blacklist them (i.e., the malicious blacklisting error is always null) without blacklisting the honest smart metres.

Moreover, this technique does not make any error in blacklisting the honest smart metres. This is because we allow all smart metres to revise their behaviour in the case they return wrong data, the fact that makes this approach more accurate and more reliable. Therefore, this approach shows the effectiveness of the voting based method with reputation technique to control collusive smart metres, to verify data integrity, and hence improves security within smart grid.

References

Araujo, F., Farinha, J., Domingues, P., Silaghi, G.C. and Kondo, D. (2011) 'A maximum independent set approach for collusion detection in voting pools', *Journal of Parallel and Distributed Computing*, Vol. 71, No. 10, pp.1356–1366.

Bendahmane, A., Essaaidi, M., El Moussaoui, A. and Younes, A. (2010) 'Reputation-based majority voting for malicious grid resources tolerance', *Scalable Computing: Practice and Experience*, Vol. 11, No. 4, pp.385–392.

Bendahmane, A., Essaaidi, M., El Moussaoui, A. and Younes, A. (2015) 'The effectiveness of reputation-based voting for collusion tolerance in large-scale grids', *IEEE Transaction on Dependable and Secure Computing*, Vol. 12, No. 6, pp.665–674.

Canon, L., Jeannot, E., and Weissman, J. (2011) 'A scheduling and certification algorithm for defeating collusion in desktop grids', *31st International Conference on Distributed Computing Systems (ICDCS)*, Minneapolis, pp.343–352.

Choi, S. and Buyya, R. (2010) 'Group-based adaptive result certification mechanism in desktop grids', *Future Generation Computer Systems*, Vol. 26, No 5, pp.776–786.

Dari, E. and Essaaidi, M. (2015) 'An overview of smart grid cyber-security state of the art study', *3rd International Renewable and Sustainable Energy Conference (IRSEC)*, pp.1–7.

Domingues, P., Sousa, B. and Silva, L.M. (2007) 'Sabotage-tolerance and trust management in desktop grid computing', *Future Generation Computer System*, Vol. 23, No. 7, pp.904–912.

Gao, J., Xiao, Y., Liu, J., Liang, W. and Chen, C.L. (2012) 'A survey of communication/networking in smart grids', *Future Generation Computer Systems*, Vol. 28, No. 2, pp.391–404.

Hao, J., Piechocki, R.J. and Chin, W.H. (2015) 'Sparse malicious false data injection attacks and defense mechanism in smart grid', *IEEE Transactions on Industrial Informatics*, Vol. 11, No. 5, pp.1198–1209.

Hendrickx, J.M., Johansson, K.H. and Sandberg, H. (2014) 'Efficient computations of a security index for false data attacks in power networks', *IEEE Transactions on Automatic Control*, Vol. 59, No. 12, pp.3194–3208.

Huang, Y., Esmalifalak, M., Nguyen, H., Zheng, R., Han, Z. and Li, H. (2013) 'Bad data injection in smart grid: attack and defense mechanisms', *Communications Magazine*, IEEE, Vol. 51, No. 1, pp.27–33.

Kondo, D., Araujo, F., Malecot, P., Domingues, P., Silva, L.M., Fedak, G. and Cappello, F. (2007) 'Characterizing result errors in internet desktop grids', in *Euro-Par 2007, Parallel Processing, 13th International Euro-Par Conference*, Springer, France, *Proceedings of LNCS*, Vol. 4641, pp.361–371.

Li, Y. and Wang, Y. (2014) 'State summation for detecting false data attack on smart grid', *International Journal of Electrical Power and Energy Systems*, Vol. 57, pp.156–163, https://doi.org/10.1016/j.ijepes.2013.11.057.

Liu, J., Xiao, Y., Li, S., Liang, W. and Chen, C.L. (2012) 'Cyber security and privacy issues in smart grids', *IEEE Communications Surveys and Tutorials*, Vol. 14, No. 4, pp 981-997.

Liu, Y., Ning, P. and Reiter, M. (2011) 'False data injection attacks against state estimation in electric power grids', *CCS'09: Proceedings of the 16th ACM conference on Computer and Communications Security*, pp.21–32.

Lorczak, P.R., Caglayan, A.K. and Eckhardt, D.E. (1989) 'A theoretical investigation of generalized voters for redundant systems', in the *19th International Symposium on Fault-Tolerant Computing*, Chicago, pp.444–451.

Moca, M., Silaghi, G.C. and Fedak, G. (2011) 'Distributed results checking for MapReduce in volunteer computing', *IEEE International Symposium on Parallel and Distributed Processing Workshops and PhD Forum (IPDPSW)*, pp.1847–1854.

Oliveira, A.C., Sampaio, L., Fernandes, S.F. and Brasileiro, F. (2009) 'Adaptive sabotage-tolerant scheduling for peer-to-peer grids', *Fourth Latin-American Symposium on Dependable Computing (LADC2009)*, IEEE Computer Society, Joao Pessoa, pp.25–32.

Py, C., Yang, S., McCann, J.A., Lin, J. and Yang, X. (2015) 'Detection of false data injection attacks in smart -grid systems', *IEEE Communication Magazine*, Vol. 53, No. 2, pp.206–213.

Sarmenta, L.F.G. (2002) 'Sabotage-tolerance mechanisms for volunteer computing systems', *Future Generation Computer Systems*, Vol. 18, No. 4, pp.561–572.

Silaghi, G.C., Araujo, F., Silva, L.M., Domingues, P. and Arenas, A.E. (2009) 'Defeating colluding nodes in desktop grid computing platforms', *Journal of Grid Computing*, Vol. 7, No. 4, pp.555–573.

Son, H.N., Fukushi, M., Xiaohong, J. and Horiguchi, S. (2008) 'Efficient scheduling schemes for sabotage-tolerance in volunteer computing systems', *International Conference on Advanced Information Networking and Applications (AINA'08)*, pp.652–658.

Sonnek, J.D., Chandra, A. and Weissman, J.B. (2007) 'Adaptive reputation-based scheduling on unreliable distributed infrastructures', *IEEE Trans. Parallel Distrib. Syst.*, Vol. 18, No. 11, pp.1551–1564.

Sou, K.C., Sandberg, H. and Johansson, K.H. (2013) 'On the exact solution to a smart grid cyber-security analysis problem', *IEEE Transactions on Smart Grid*, Vol. 4, No. 2, pp.856–865.

Wang, Y. and Wei, J. (2011) 'VIAF: verification-based integrity assurance framework for MapReduce', *IEEE International Conference on Cloud Computing (CLOUD)*, pp.300–307.

Watanabe, K., Fukushi, M. and Horiguchi, S. (2009) 'Collusion-resistant sabotage-tolerance mechanisms for volunteer computing systems', *IEEE International Conference on e-Business Engineering*, Macau, pp.213–218.

Yang, X., Zhangm, X., Lin, J., Yu, W. and Zhaon, P. (2016) 'A Gaussian-mixture model based detection scheme against data integrity attacks in the smart grid', *25th International Conference on Computer Communication and Networks (ICCCN)*, pp.1–9.

Zhao, S., Lo, V. and GauthierDickey, C. (2005) 'Result verification and trust-based scheduling in peer-to-peer grids', *The 5th IEEE International Conference on Peer-to-Peer Computing (P2P2005)*, IEEE Computer Society, Washington, pp.31–38.

Zuev, Y.A. (1998) 'On the estimation of efficiency of voting procedures', *Theory Probab. Appl.*, Vol. 42, No. 1, pp.73–81.