International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue VI, June - 2020

Protection Engine for Examining Distributed Denial of Service Attack in Computer Networks

R.Lakshmi
(Computer Science and Engineering, Christ the King Engineering College, Coimbatore, Tamil nadu, lakshmivirusiha97@gmail.com)

Abstract— The ever rising attacks on IT infrastructure, especially on networks has become the cause of anxiety for the IT professionals and the people venturing in the cyber world. Distributed denial of service (DDoS) is one of the most indirect security attack on computer networks. Many . Once the DDoS attack initiates, it causes huge overhead to the servers in terms of its processing capability and service delivery. Though, the study and analysis of request packets may help in distinguishing the legitimate users from among the malicious attackers but such detection becomes non-viable due to continuous flooding of packets on servers and eventually leads to denial of service to the authorized users. In the present research, to propose traffic flow and flow count variable based prevention mechanism with the difference in homogeneity. Its simplicity and practical approach facilitates the detection of DDoS attack at the early stage which helps in prevention of the attack and the subsequent damage. Further, simulation result based on different instances of time has been shown on T-value including generation of simple and harmonic homogeneity for observing the real time request difference and gaps.

Index Terms—Convergence analysis, data deception attacks, denial of service (DoS) attacks, distributed state estimation, smart grid

I. INTRODUCTION

WITH the advent of information and communication technology, the legacy power system has been evolving into smart grid (SG), by integrating physical elements of the power network with the computation and communication core to improve the overall automation and management of the grid [1], [2]. In SG, the entire power grid exchanges information via communication networks to support system operation [3]–[7].

However, although the communication networks facilitate the interconnection and interaction of the grid, they also break down an independent physical environment of the traditional power system and lead to vulnerability of SG due to potential cyber attacks [8]–[13].

Indeed, SG represents a large-scale distributed system consisting of many subsystems [14]–[16]. With further advancing SG construction, it is becoming increasingly large in scale.

The traditional centralized state estimation is difficult to meet the real-time and accuracy requirements, thus distributed state estimation is developed [17]–[19]. Distribution state estimation can be treated as a distributed convex optimization problem, which further can be solved by some methods, such as dual decomposition, the augmented Lagrangian method, etc. [20], [21]. Compared with the above existing methods, the alternating direction method of multipliers (ADMMs) is proposed as an attempt to blend the benefits, which include decomposability, higher estimation accuracy, and convergence speed [22].

However, to guarantee a normal operation of a power grid, information exchange must be carried out within and between the subsystems through the communication network, which is susceptible to multi-source cyber attacks and multi type cyber attacks due to network vulnerabilities [23].

Typical cyber-attacks include false data injection (FDI) attacks [24]–[29], denial of service (DoS) attacks [30]–[33], etc. These cyber-attacks inevitably com- promise the performance of distributed state estimation. Therefore, the impact of cyber-attacks on distributed state estimation must be analyzed.

Existing works on cyber-attacks and their effects on distributed state estimation can be classified into two categories, according to whether the distributed state estimation suffers from single type or hybrid cyber-attacks. Most research works focus on the impact of distributed state estimation under a single type of cyber-attacks.

The collectively uniform detectability is proposed to ensure that the error covariance of the covariance intersection-based Kalman consensus filters are uniformly bounded in spite of the absence of cyber-attacks in [34].

A DoS attack against distributed state estimation is studied, which can lead to the blindness of system operators of multiple regional subsystems [35].

A kind of tolerable FDI attacks are constructed, which can bypass the traditional bad data detection (BDD) and degrade the performance of distributed state estimation [36].

An event-based distributed state estimation under FDI attacks is investigated, in which each sensor detects susceptibility of its own data by comput- ing the gap between its data and a given threshold at eachtime step [37].

International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue VI, June - 2020

A distributed attack detection and secure esti- mation problem there is a direct connection between nodes i and j, otherwise "0," and c_{ii} 0.

1) How to develop a novel distributed state estimation method against the simultaneous presence of these two types of attacks is a challenging problem.
2) Hybrid cyber attacks inevitably degrade theperformance of distributed state estimation or even cause nonconvergence of individual local estimators. How to analyze the convergence of distributed state estimation under these two types of attacks is an important problem.

To address these challenges, this paper presents an ADMM-based distributed state estimation method and provides its convergence guarantee under data deception and DoS attacks. The main contributions of this paper include the following.

1) Unlike state estimation and performance analysis of SG under a single type of cyber attacks, an ADMM-based distributed state estimation method is first presented in which regional subsystems are partitioned via the *K*-means method.
2) Considering that individual regional subsystems may suffer from different cyber attacks, the feature models of data deception attacks and DoS attacks are established, and a novel distributed state estimation is then proposed.
3) The convergence of the distributed state estimation method under hybrid cyber attacks is proved theoretically and the relationships between the convergence and algorithm parameters as well as the occurring probability of attacks are established.

This paper is organized as follows. Section II presents an ADMM-based distributed state estimation method of the SG. The distributed state estimation method under hybrid cyber-attacks is investigated in Section III. Section IV proves the convergence of distributed state estimation under hybrid cyber attacks. Simulation results are given in Section V, followed by the conclusions in Section VI.

DISTRIBUTED STATE ESTIMATION OF SMART GRID

A. Regional Partition of Large-Scale SG Based on K-Means

Large-scale SG systems are partitioned [39]–[42] such that distributed state estimation can be performed to enhance the system's ability to withstand the risks. Large-scale system partitioning usually uses graph theory to represent the power grid as a graph based on system structural parameters. Nodes (i.e., power stations, system buses, etc.) are regarded as points,

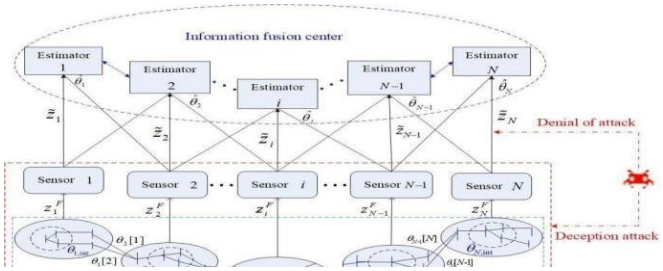


Fig. 1. Block diagram of the distributed state estimation of a multisubsystem power system under the data deception attacks and DoS attacks.

The weight matrix W_L for the connection matrix C_L is further defined as

$$W_L = \begin{cases} w_{i,j},\ c_{i,j} = 1, \text{ and } i * = \\ 1, \quad i = j \end{cases} \tag{2}$$

where $w_{i,j}$ is the connected weight between nodes i and j, $i, j = 1, 2, \ldots, M$, and the diagonal weights are set as 1.

A proper system partition scheme is pursued. That is, individual subsystems after the partition are expected to have similar numbers of nodes, and the connections between subsystems are also minimal. Such a partition scheme can balance the calculation burden of the individual subsystems. If the off-diagonal element in (2) represents the price to be paid for destroying the corresponding connection, e.g., $w_{i,j}$ 0.01 means that the cost to break the connection between nodes i and j is 0.01, based on the *K*-means algorithm [43], the objective function is expressed as

$$J^M = \sum_{i=1}^{M} \sum_{j=1}^{k} w^{ji} - c^{j\,2} \tag{3}$$

where k represents the number of clustering centers, c_j represents the jth center, w_i represents the ith row for W_L, and $w_i{}^j$ belongs to the jth cluster. Furthermore, by minimizing (3) for each node, one can calculate the distance between it and each centroid, and assign it to the nearest cluster, i.e., each node is set as the label number of the corresponding cluster, thus forming the node-cluster incidence vector *ndx* with each element ranging from 1 to k.

Define the partitioned cost function as

$$C_{\text{cost}} = \sum_{i=1}^{M} \sum_{j=1}^{M} w_{i,j} - \text{tr}\, Pi^T W_L Pi \tag{4}$$

where tr[·] represents the trace of matrix; Pi represents the matrix resulting from the index vector *ndx* mapping; and C_{cost} represents the total cost of breaking up the connections after partitioning, the smaller the value, the less the connections damaged.

B. Distributed State Estimation of Smart Grid Based on ADMM

Based on the *K*-means method, the effective partition of large-scale power grid systems can be achieved and the frequency of information exchange between adjacent subsystems can be mitigated, which can reduce the communication

data deception attacks are two popular cyber-attacks for SG. For DoS attacks affecting the data integrity [30], attackers usually use network datagram sending tools [e.g., user datagram protocol (UDP) Flooder 2.0] to send a large number of fake UDP packets to the target devices in a short period of time, which induces the target devices to continuously replay the messages, leading to exhaustion of the network bandwidth.

where ▲ is a diagonal matrix with elements 0 or 1, where 1 represents that the corresponding measurement value is modi- fied, and 0 otherwise, and a_i is the attack vector sophisticatedly designed by attackers, i 1, 2, . . . , N.

To compromise the overall performance of distributed state estimator, the attacker can usually launch multichannel DoS attacks and block the transmission of measurement informa- tion between distributed sensors and the remote estimation unit. In this way, once the attacker successfully blocks the transmission channel, the measurements will be lost. In gen- eral, there are three possible attack scenarios as follows.

1) The attacker fails to block the transmission channel. The measurement is successfully transmitted to the

The communication is finally blocked, so that the normal messages cannot be transmitted. For data deception attacks destroying the data authenticity of the original data, there usually exist two attack patterns, one is the attackers who invade the target devices to inject the false data [47]; another is the attackers who hijack the data packets from the communication channel and manipulate maliciously the original data by using some tools, such as the advanced IP scanner 2.3, Fiddler Web debugger, etc. [48].

A. Modeling of Data Deception and DoS Attacks

A block diagram of distributed state estimation of a multi- subsystem power grid under data deception and DoS attacks is shown in Fig. 1, where N sensors are configured to monitor the operating status of the local grid system and collect the running states of the grid. This measurement information is then transmitted to various remote state estimators via wired/wireless networks. The estimator i (i=1, 2 , . . . , N) calculates the state of each subsystem, respectively. However, when this measurement information is transmitted, it may suffer from data deception and DoS attacks, e.g., the attacker can modify the measurement information z_i as z^F_i of subsystem i; at the same time, the attacker can also block the remote transmission of the measurement signal, assuming that the remote estimator i receives the transmission signal as z_i~.

Considering that the measurement values of the subsystem could be manipulated and modified under the attacks, the measurement model of the subsystem i in (5) can be rewritten as

$$z^F_i = z_i + \blacktriangle a_i = H_i \theta_i + v_i + \blacktriangle a_i \tag{17}$$

attacks occur or not. The compensation z^{comp}_i can be obtained by using the measurement data or the measurement estimation data from the previous sampling instant. Considering that DoS attacks may be continuous, the measurement estimation data is selected to compensate. If each local state estimator is equipped with a buffer, and the measurement estimation data at each sampling instant is saved based on the existing measurement compensation, that is, zk−1, zk−2,..., z1 is stored at the sampling instant k, the remote estimator i can estimator.

2) The attacker can only block part of the channels, leading to partial measurement losses.
3) The attacker will completely block all transmission channels and the measurement will be lost completely.

Considering that a deterministic attack is not only costly, but may also be limited to the security detection of the system. To deceive the operators of the grid system and/or to save the cost, a cunning attacker would intelligently decide to block transmission channels randomly or to hide in the system waiting for the opportunity.

In view of the above analysis, according to the compensation strategy [49], [50], the measurements received by the state estimator after the attacks can be expressed as

$$z_i = \alpha_i z^F_i + (1-\alpha_i) z^{comp}_i \tag{18}$$

where the first term on the right-hand side represents the manipulated measurement values, z^{comp}_i is the compensation of measurement losses and how to obtain is given in the following Remark 1, α_i is a random variable with value of 0 or 1 (i.e., α_i =1 represents that the measurements are successfully transmitted, α_i =0 otherwise) that follows the Bernoulli distribution, and its corresponding probability distribution law satisfies

$$\begin{aligned} \Pr\{\alpha_i = 1\} &= E\{\alpha_i\} = \beta_i \\ \Pr\{\alpha_i = 0\} &= 1 - E\{\alpha_i\} = 1 - \beta_i \end{aligned} \tag{19}$$

always use (1 αi)zk−1 at the sampling instant k to reduce the impact of attacks on the estimated performance.where β_i ∈[0, 1] is a constant, and all random variables α_i(i = 1, 2 , . . . , N) are independent of each other, i.e., each transmission channel independently communicates. Random variables α_i are used to describe the probability whether the measurements from sensor i are successfully transmitted to the local state estimator i. When the attacker launches a DoS attack to block the transmission, the measurements z^F_i will be lost with probability 1−β_i, that is, the larger the β_i, the bigger chance of successful transmission. It should be noted that β_i ∈(0, 1) represents that only part of the measurement information is successfully transmitted to the estimator. Inparticular, if β_i =1, it is an ideal transmission situation, meaning that all measurements are successfully received by the estimator without being attacked during the transmission process; β_i =0 represents an extreme attack situation in which all measurements are lost during the transmission process.

Remark 1: When α_i = 0 (i.e., DoS attacks occur) in (18), the measurement output is compensated by using the second term on the right-hand side of (18) whether data deception When αi 1 (i.e., DoS attacks do not occur) in (18), whether data deception attacks occur or not need be detected. If deception attacks occur, the

the first term does not use the attacked measurements, and the estimated static estimates $\hat{\theta}_{i,\text{quasi}}$ are obtained under the quasi-static conditions of the grid system, and the second term is the attacked estimates, where the attacked estimates $\hat{\theta}^k$ can be calculated by (23). Since the operation state of the power grid under the quasi-static conditions remains almost constant for a period of time, each subsystem model can be contaminated measurements $z^F{}_i$ are discarded and also can be compensated by using different compensation strategies, such as the buffer method [51], [52] and the missing data construction method [53].

Remark 2: The character of measurement losses caused by DoS attacks is described by the Bernoulli distribution [i.e., (19)]. The occurring probability β_i of DoS attacks corresponds to the probability of the measurement losses. Therefore, we can first use network analysis tools (e.g., Ethereal, Airo Peek, etc.) to capture the packets, whether the packets are lost can then be analyzed by its type identification, serial number, time stamp, etc. Furthermore, β_i can be determined by the statistical analysis method. Moreover, there exist some other methods/techniques to describe the character of the measurement losses, e.g., the character measurement losses caused by DoS attacks is described by a finite-state Markov process model [54].

B. Distributed State Estimation Security Framework Under Hybrid Cyber Attacks

Two types of malicious network attacks are present to worsen the performance of distributed state estimation, and even cause no convergence of individual state estimators. By launching a data deception attack, an attacker can inject well-designed malicious data into the measurement data without being detected. Meanwhile, by launching a DoS attack, the attacker tries to block the transmission of the measurement between the sensor and the remote estimator. Therefore, it is extremely important to design a distributed attack detection mechanism and a security estimation framework against these two types of attacks.

If the measurements are under the normal measurement noises, using the ADMM-based distributed state estimation method, the accuracy of state estimation result for each local state estimator can be guaranteed. However, the malicious data deception attack modifies the original measurement, which can escape traditional BDD detection, compromising the estimation results of each estimator. Taking into account the cost of the attacks and the robustness of the various local estimators, it is usually expected that the constructed attack vector a_i is as sparse as possible, to ensure the stealth of the attacks.

In response to this attack, a new distributed attack detection mechanism is designed. First, a new residual is defined as $r_i^k = H_i\hat{\theta}_{i,\text{quasi}} - H_i\hat{\theta}_{i,a}^k$ on each local state estimator, where approxi- mated by the dc model in (5). By using the distributed state estimation method, the state estimation value under the quasi-static conditions of the system can be obtained. According to the anomaly detection method (i.e., $\| z_i - H_i\hat{\theta}_{i,\text{quasi}} \| \le \tau_i$), if no anomaly is detected, this state estimates can be recorded as a reference for the state of grid system. Then, by analyzing the new defined residual, the index function on each local state estimator is defined as

$$f_{i,\text{indicator}}(k) = r_i^k, \quad k \in [k_e - T_e, k_e] \tag{20}$$

where k_{ke} is the end time of the iteration and T represents the iteration steps before the end time. In order to detect the existence of the attacks, a specific threshold τ_i is defined in advance. That is, when the attacks occur, the value of the index function will exceed the threshold, and the local state estimator will trigger an alarm signal. To find a specific threshold, the threshold of the index function is defined as

$$\tau_i = \sup_{a_i=0, v_i*} \| z_i - H_i\hat{\theta}_{i,\text{quasi}} \| \tag{21}$$

where $a_i = 0$represents that subsystem i is not subjected to data deception attacks, and an upper threshold can be obtained based on (21) when the system is running normally (i.e., under quasi-static conditions).

According to (20) and (21), a distributed anomaly detection strategy can be designed as

$$\begin{aligned} &f_{i,\text{indicator}}(k) > \tau_i \Rightarrow \text{ alarm} \\ &f_{i,\text{indicator}}(k) \le \tau_i \Rightarrow \text{ no alarm.} \end{aligned} \tag{22}$$

Remark 3: The real signals fluctuate due to the noise interference, and the detection threshold is set by (21). In fact, this threshold has included the statistical information of the error induced by noise. Therefore, the noise usually cannot trigger the alarm.

Remark 4: The attackers may launch data deception attacks or DoS attacks separately, or two kinds of attacks simultaneously, which is described by (18). This can further be analyzed according to whether α_i is 0 or not.

1) When α_i 0, it means that there certainly exist DoS attacks. Meanwhile, there possibly exist data deception attacks, but the measurements $\tilde{z}_i$ are always compensated by z_i^{comp}. Then $\hat{\theta}^k{}_{i,a}$is calculated by (23), which is further substituted into the index function (20) to judge whether the system is anomaly. Generally, the alarm is not triggered; occasionally, the alarm is triggered. This is because the compensation data are not precise under too long of a continuous DoS attack.
2) When α_i :1, it means that there do not certainly exist DoS attacks. However, it is uncertain whether thereexist data deception attacks or not. Therefore, $\hat{\theta}^k$ is calculated by (23), which is further substituted into the index

International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue VI, June - 2020

TABLE I
NODES CONTAINED IN EACH SUBSYSTEM AFTER PARTITIONING

	Internal nodes	Boundary nodes
subsystem 1	1 2 3 4 5 6 7 8 9 10 11 12 13 14 117	1-4 30 16 15 17 26 19 1-5 30 33 38 37
subsystem 2	103 104 105 106 107 108 109 110 111 112	2-3 100 99 98 94 92 101
subsystem 3	76 78 79 80 82 83 84 85 86 87 88 89 90 91 93 95 96 97 102	3-2 100 99 98 94 92 101 3-4 77 118 75 3-5 77 81 69 68
subsystem 4	18 20 21 22 23 24 25 27 28 29 31 32 71 72 73 74 113 114 115	4-1 30 16 15 17 26 19 4-3 77 118 75 4-5 70 75 34 69
subsystem 5	35 36 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 116	5-1 30 33 38 37 5-3 77 81 69 68 5-4 19 70 75 34 69

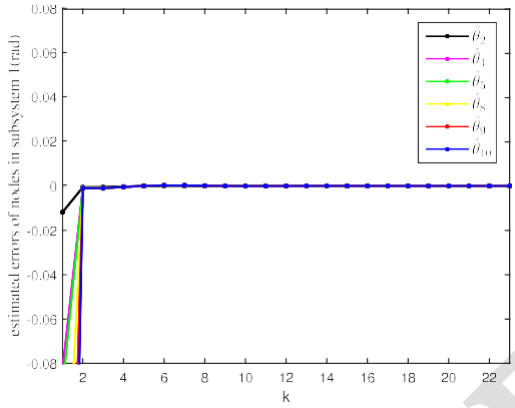


Fig. 4. State estimation errors of several relevant nodes in subsystem 1.

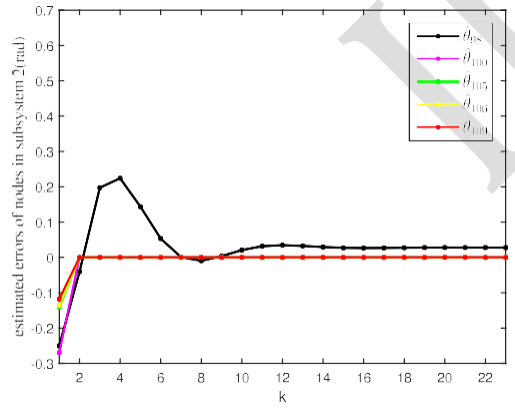


Fig. 5. State estimation errors of several relevant nodes in subsystem 2.

estimation algorithm (12)–(14), with the penalty parameter of $\rho = 10^{3.5}$, state estimation results of several relevant nodes in each subsystem are as shown in Figs. 4–8. The regional estimation error is further shown in Fig. 9.

Figs. 3–9 show that ADMM-based distributed state esti- mation of the grid converges. As the number of recursive iterations increases, the states of individual nodes in each sub- system approaches the true values. Moreover, the convergence speed is also fast enough, with most subsystems converging in 10–14 iterations.

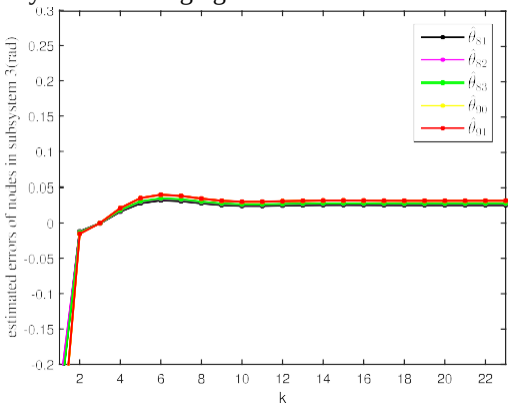


Fig. 6. State estimation errors of several relevant nodes in subsystem 3.

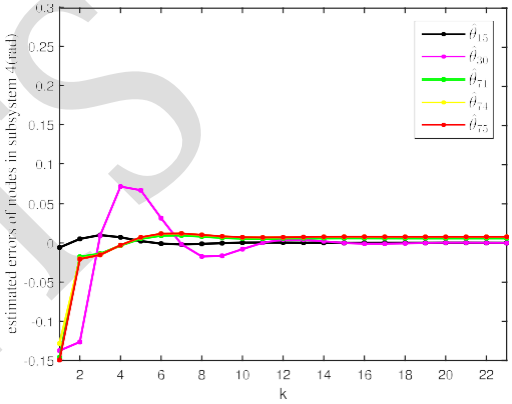


Fig. 7. State estimation errors of several relevant nodes in subsystem 4.

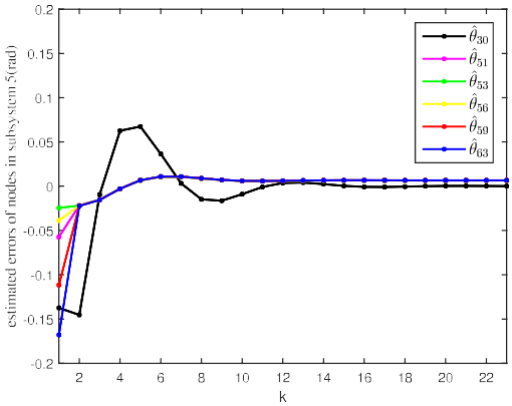


Fig. 8. State estimation errors of several relevant nodes in subsystem 5.

A. Performance Analysis of Distributed State Estimation Under Hybrid Cyber Attacks

International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue VI, June - 2020

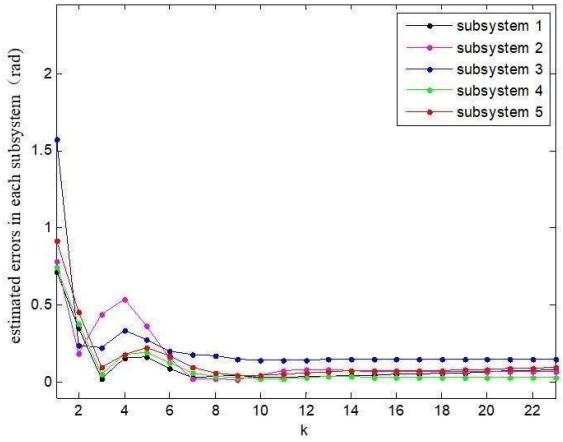


Fig. 9. State estimation errors of individual subsystems.

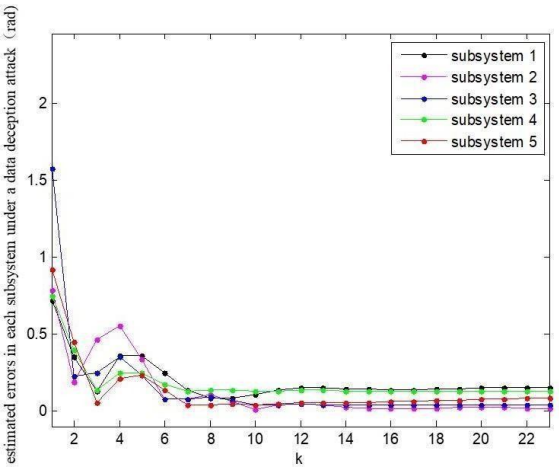


Fig. 11. State estimation errors of individual subsystems under a single data deception attack.

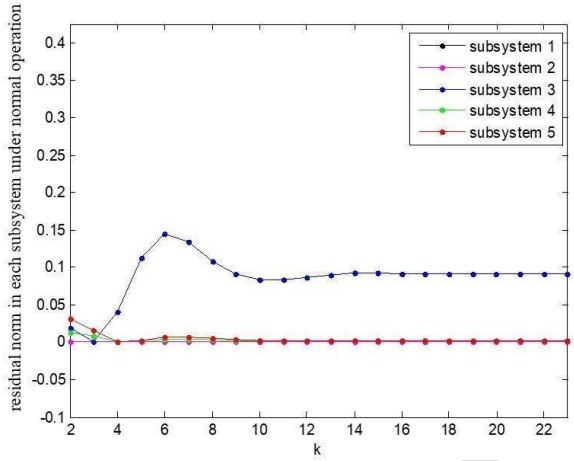


Fig. 10. Residual norms of individual subsystems under normal operation.

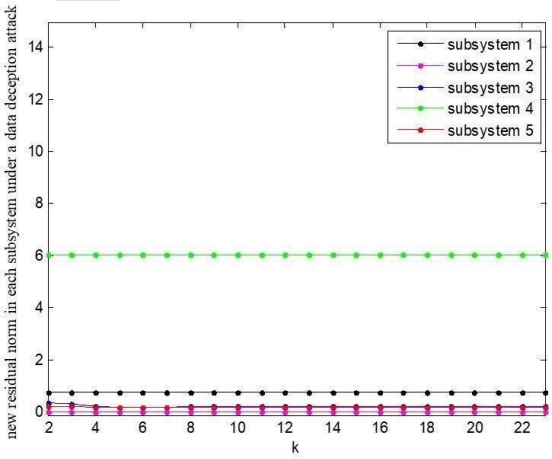


Fig. 12. Residual norms of individual subsystems under a single data deception attack.

measurements are corrupted based on the data deception attack strategy [56]. According to the proposed distributed attack detection mechanism, the residuals of individual subsystems under normal operation of the grid system are shown in Fig. 10. It can be seen that the residuals of individual subsystems are relatively small, which are basically related to measurement noises of individual subsystems. When the system measurement noises are set, the residual upper bound of each subsystem during normal operation (i.e., specific threshold τ_i) can be obtained. Figs. 11 and 12 show the state estimation error and the new residual for each subsystem under single data spoofing attack, respectively. Compared to Fig. 10, Fig. 11 illustrates that single data deception attack does not significantly affect the convergence of distributed state estimation, but will affect the results of the distributed state estimation. Moreover, it is observed from Fig. 12 that the new residual error in subsystem 4 under single data deception attack is much larger than the upper bound set, so that subsystem 4 will trigger an alarm signal, and each local state estimator will respond to the signal.

Next, we will verify the effect of missing data compensator designed for single DoS attack. The probability of DoS attacks for each transmission channel is set as 0.25, i.e., $\beta_i = 0.75$, $i = 1, 2, \ldots, 5$. Figs. 13 and 14 show state estimation errors and residuals of individual subsystems under single DoS attack, respectively. It can be seen from Fig. 13 that DoS attacks will affect the convergence rate of distributed state estimation, and the proposed missing data compensator can well compensate for the missing data, so that the estimation error of each local state estimator is also relatively small. Fig. 14 shows that a single DoS attack hardly changes the upper bound of the residual in each subsystem.

Finally, we verify the distributed detection mechanism and the effect of the missing data compensator under two types of cyber attacks, while the attack conditions remain the same as used in the above studies. Figs. 15 and 16 show the state estimation errors and residuals for individual subsystems under hybrid cyber attacks, respectively. Fig. 15 shows that DoS attacks only affect the convergence rate of distributed state estimation, and each local state estimator still converges, while data deception attacks affect the estimated results of each local state estimator. It can be seen from Fig. 16 that the new residual of subsystem 4 under hybrid cyber attacks is

International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue VI, June - 2020

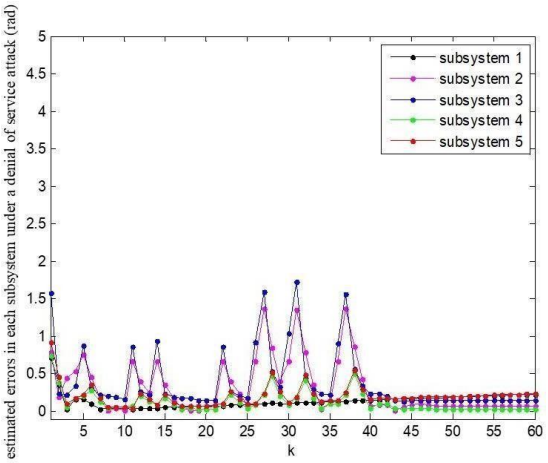


Fig. 13. State estimation errors of individual subsystems under a single DoS attack.

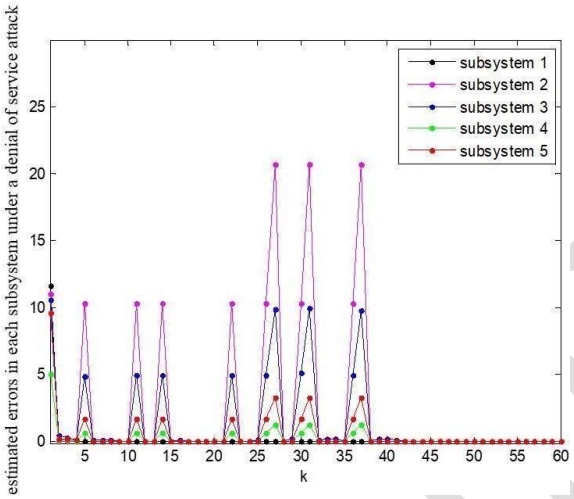


Fig. 14. Residual norms of individual subsystems under a single DoS attack.

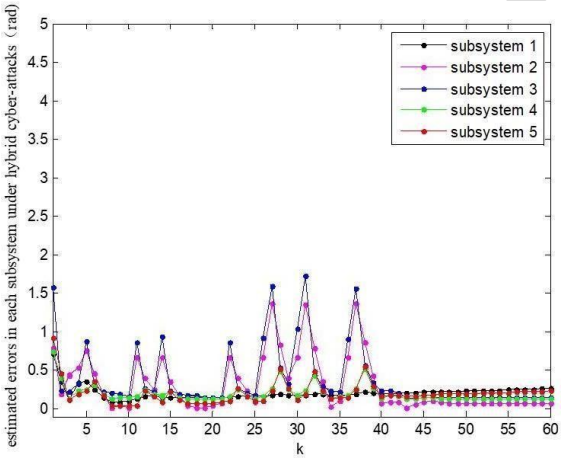


Fig. 15. State estimation errors of individual subsystems under hybrid attacks.

much larger than the upper bound set during the normal operation, which demonstrates the effectiveness of the proposed distributed detection for data deception attacks.

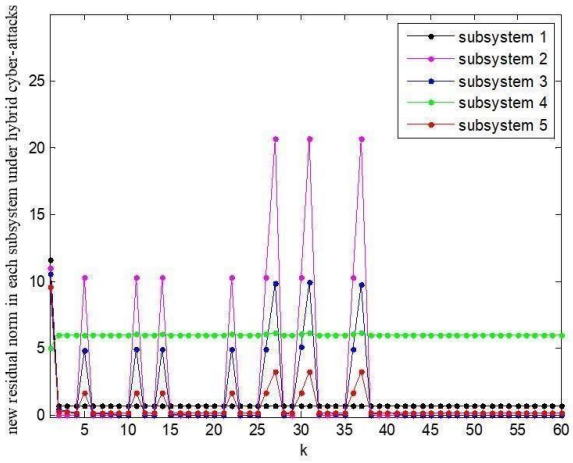
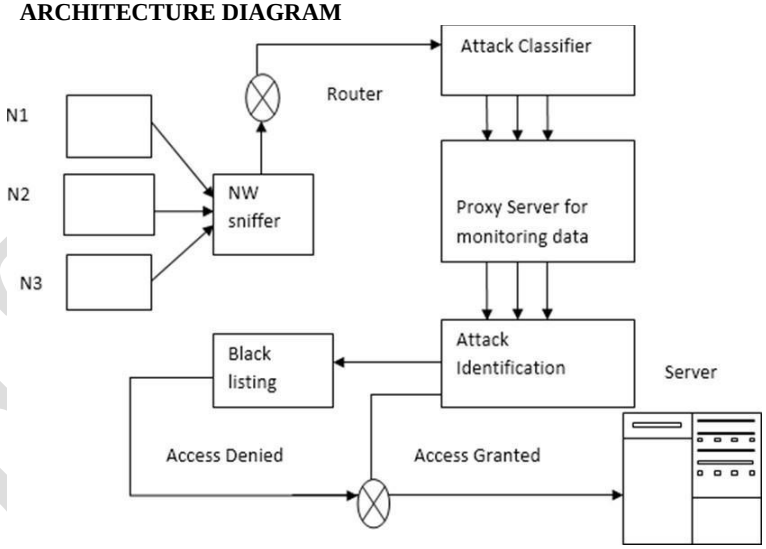


Fig. 16. Residual norms of individual subsystems under hybrid attacks.

ARCHITECTURE DIAGRAM



CONCLUSION

In this research work is proposed a system where the network administrator will observe and analysis various types of attacking tendencies originating from variable source in network. The process basically understand the pattern and behaviour of the hostile circumstances over the network and then it creates the profiles of the attackers based on this pattern analysis, which will protect the network system of the organization by blacklisting the origination of the resource profiling over the network itself thereby assuring the organizational network to be the most secure one in any future probability of network threats from those attackers.

In this work, described some of the previous efforts to measure IDS, and outlined some of the difficulties that have been encountered. to believe that a periodic, comprehensive evaluation of IDSs could be valuable for network managers, information security officers and data managers.

REFERENCES

[1] S. Ciavarella, J.-Y. Joo, and S. Silvestri, "Managing contingencies in smart grids via the Internet of Things," IEEE Trans. Smart Grid, vol. 7, no. 4, pp. 2134– 2141, Jul. 2016.

[2] T. Samad and A. M. Annaswamy, "Controls for smart grids: Architectures and applications, Proc. IEEE, vol. 105, no. 11, pp. 2244–2261, Nov. 2017.

[3] X. Yu and Y. Xue, "Smart grids: A cyber-physical systems perspective," Proc. IEEE, vol. 104, no. 5, pp. 1058–1070, May 2016.

[4] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Neural-network-based output- feedback control under round–Robin scheduling protocols," IEEE Trans. Cybern.

[5] P. Zhou et al., "Toward energy-efficient trust system through watchdog optimization for WSNs," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 613–625, Mar. 2015.

[6] L. Ding, L. Y. Wang, G. Yin, W. X. Zheng, and Q.-L. Han, "Distributed energy management for smart grids with an event-triggered communication scheme," IEEE Trans. Control Syst. Technol., to be published.

[7] C. Peng, J. Li, and M. Fei, "Resilient event-triggering H∞ load frequency control for multi-area spower systems with energy-limited DoS attacks," IEEE Trans. Power Syst., vol. 32, no. 5, pp. 4110–4118, Sep. 2017.

[8] O. Vukovi´c and G. Dán, "Security of fully distributed power system state

estimation: Detection and mitigation of data integrity attacks," IEEE J. Sel. Areas Commun., vol. 32, no. 7, pp. 1500–1508, Jul. 2014.

[9] F. Yang, N. Xia, and Q.-L. Han, "Event-based networked islanding detection for distributed solar PV generation systems," IEEE Trans. Ind. Informat., vol. 13, no. 1, pp. 322–329, Feb. 2016.

[10]R. Fu et al., "Security assessment for cyber physical distribution power system under intrusion attacks," IEEE Access, to be published.