# A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid

1st Vivek Kumar Singh
*Department of Electrical and Computer Engineering*
*Iowa State University*
Ames, USA
vsingh@iastate.edu

2nd Altay Ozen
*Department of Electrical and Computer Engineering*
*Iowa State University*
Ames, USA
ozeen1@iastate.edu

3rd Manimaran Govindarasu
*Department of Electrical and Computer Engineering*
*Iowa State University*
Ames, USA
gmani@iastate.edu

***Abstract*— Future smart grid capabilities provide assurance to expand the advanced information and communication technologies to evolve into densely interconnected cyber physical system. Remedial Action Scheme (RAS), widely used for wide-area protection, relies on the interconnected networks and data sharing devices, which are exposed to the multitude of vulnerabilities. This paper presents our proposed approach to developing multi-agent based RAS scheme against the system-aware stealthy cyber-attacks. Specifically, we propose the two-level hierarchical architecture which consists of distributed local RAS controllers (RAScs) as local agents, operating at different zones/ areas, which are constantly monitored by an overseer, the central agent. The local controllers receive local and randomly changing outside zonal measurements and cyclically forwards to the overseer. The overseer identifies the corrupted controller using the anomaly detection algorithm which processes the measurements coming from the local controllers, compute measurement errors using local and outside zonal measurements, perform validation checks, and finally detect anomalies based on the two-step verification. Next, as a proof of concept, we have implemented and validated the proposed methodology in cyber physical environment at Iowa State's PowerCyber testbed. We have also implemented the coordinated attack vectors which involve corrupting the local controller and later performing stealthy attacks on the system's generator. We have evaluated its performance during the online testing in terms of detection rate and latency. The experimental results show that it is efficient in detecting different classes of attacks, including ramp and pulse attacks.**

## I. Introduction

The current power grid, consisting of high-space dynamics, is evolving to meet the real-time demand response with higher dependent on intermittent sources of energy like solar and wind. Remedial Action Scheme (RAS), also known as Special Protection Scheme (SPS), provides automated protection during physical disturbances in smart grid [1]. In recent years, there has been drastic proliferations in the number of RAS/SPS implemented in industries because of its ability to accommodate more generation interconnections. It is also considered a less costly alternative to building the expensive transmission lines [2]. Since it relies on interconnected data sharing devices and communication network, it is highly exposed to the multitude of cyber vulnerabilities. NERC has classified the RAS as a critical asset with cyber physical properties and any compromise and degradation in the scheme can affect the reliability and stability of the bulk power system [3]. In recent years, several malicious cybersecurity incidents have been reported targeting the industrial control systems [4]. *Stuxnet worm*, the complex, sophisticated malware, has directly affected more than 100,000 industrial controllers worldwide [5]. It shows how the stealthy malicious attacks can cause more damage while remain undetected as compared to short term attack. The sophisticated malware-based attack on Ukraine's power grid is a similar incident which has caused the shutdown of multiple substations. Furthermore, several remote code vulnerabilities have been issued in the past, e.g., CVE-2017-7494, CVE-2016-7855, CVE-2014-4114 vulnerabilities in windows operating system can allow backdoor access to the attacker [6]. Due to the increased complexity between the interconnected networks and interacting legacy infrastructure, it is difficult to resolve the cyber physical security challenges using the conventional security methods. Therefore, there is a compelling urge to develop a new suite of frameworks and architectures which can resolve security challenges at cyber physical layer.

From a broad perspective, the architecture of the RAS controller (RASc) can be categorized as centralized, de-centralized (distributed) and multi-agent [7]. Most of these protection schemes in the past were implemented in centralized and de-centralized ways [8], [9]. The paper in [8] describes about the centralized RAS (CRAS) implemented in the Southern California Edison (SCE) where it performs an optimal protection, control based on global system information. However, any malfunction in central controller due to malicious cyber activity would lead to a single point of failure with severe system impact. The distributed RAS (DRAS) overcomes the above limitation through the multiple local controllers which are performing localized operations at the substation level. Ross et al. shows how the DRAS can combat denial of service cyber-attacks on the communication devices [9]. However, the proposed scheme may lose their efficiency against the advanced, persistent adversary who can perform stealthy coordinated attacks. Since DRAS operates at local and remote substations, they are more vulnerable to cyber-physical attacks. It also provides increased attack surface due to the multiple controller involvements in the information sharing and collaborative actions. Hence, the multi-agent controllers can provide better promising solutions which can adapt hybrid design of centralized and distributed architecture to provide better synergistic relationship among the agents against stealthy cyber-attacks.

In an earlier effort, we have shown how the system-aware stealthy cyber-attacks can be deployed in a coordinated fashion, targeting the controller and system generator [10]. In this paper, we propose a novel architecture and methodology for detecting the compromised local controller for the distributed RAS using multi-agent system. The proposed architecture consists of local and central agents, where the distributed local agent RAS controllers, operating in the assigned zones, not only perform automated corrective actions but also forwards the system updates to the master agent. The master agent,

designed at the higher level, detects the anomalies based on the local and global measurements and eventually identify the compromised controller based on the majority vote. We have applied the Moving Target Defense (MTD) based strategy of sending random measurements in developing the anomaly detection methodology. As a proof of concept, we have implemented the proposed architecture through the experimental set-up and tested in real-time. Additionally, we have also evaluated its performance in terms of latency and detection rate for different classes of attacks to demonstrate its effectiveness. The remainder of the section is organized as follows: section 2 talks about the overview of RAS and multi-agent applications in RAS. Section 3 describes the attack vectors implemented on the testbed. Section 4 provides the detailed discussions on the proposed architecture and anomaly detection methodology. Section 5 provides the experimental set-up and case study on IEEE 39 system. Section 6 provides insight into the factors that affects the performance in terms of latency and accuracy rate. Section 5 provides the clear conclusion of our work.

## II. Overview and Related Works

Remedial Action Scheme (RAS) detects the physical disturbances like line outages, generator outages and later performs corrective actions like generation shedding, load shedding and other defined actions to maintain the system's stability and reliability. The multi-agent system (MAS) has emerged as a new paradigm for better reliability and control. It consists of intelligent agents which can work autonomously and perform consensus-based decisions [11]. There exists the limited works which address the multi-agent based applications and its security in the context of RAS. The papers [12], [13] talks about the multi-agent framework for wide area controllers from the broader perspective. It emphasizes on the intelligent coordination of local and central agents to enhance the robustness. Liu et al. shows how the three-level hierarchical structure for MAS can prevent voltage instability [14]. The papers presented in [9], [15] advocate the use of agent-based decentralized protection scheme for detecting severe attacks assuming secure communication and trustworthiness among agents. While considering advanced persistent threat (APT), it is not obvious to assume that all the agents are trustworthy. The smart attacker can compromise the security of agents to jeopardize the protection scheme. This paper presents one-step ahead scenario where the attacker compromises the local protection agents to inject data integrity attack on the generator to create physical impact. Based on the smartly assigning limited functionality to the agents and applying MTD based random strategy for the measurement updates, it is possible to detect the compromised controllers and cyber-physical attacks. Pappa et al. shows how the MTD based IP-hopping technique can mitigate cyber-attacks in SCADA environment [16]. In this work, we are applying the similar strategy of dynamically changing measurements, instead of IP addresses, to detect the anomalies.

### A. Generation Rejection Remedial Action Scheme

Based on the corrective actions, RAS can be classified into different types like load shedding, generation based etc. In this paper, we have considered the generation rejection-based RAS, which sheds generation to prevent the thermal overloading as shown in fig. 1. Initially, it is in an armed stage, and collects the system data at regular intervals in terms of relays status, line flows and power output of the generator. During a line outage, the RASc is triggered/activated, it checks the operational transfer capability (OTC) of the other adjacent lines directly connected to the generator. If the current line flows exceed its maximum operational transfer capability (OTC_max) limit, it performs corrective action by shedding the generation to prevent the thermal overloading in other adjacent lines. It is to be noted that we have considered the thermal overload limit while computing the OTC_max, other factors like voltage and angular stabilities are ignored in this case. The OTC_max limit for each transmission line is provided through the predefined action table for the different line contingencies. Apart from the generation shedding, it is also allowed to restore the generation once the fault/contingency is cleared.

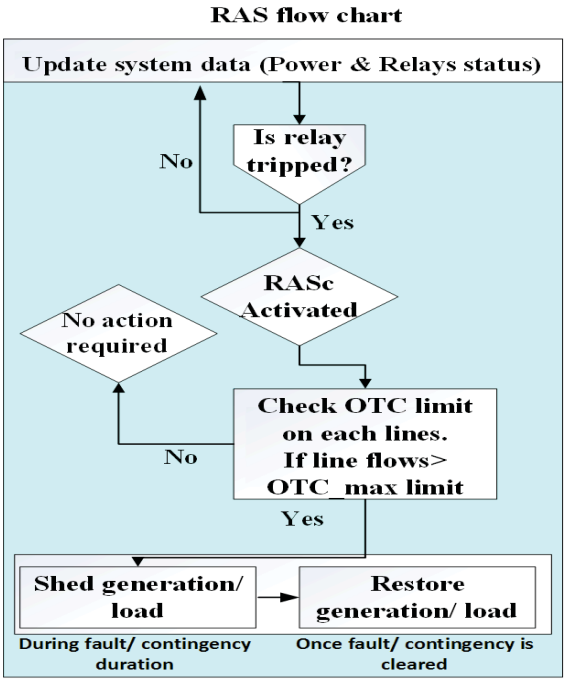


Fig. 1. Remedial Action Scheme (RAS) flow chart.

## III. Cyber Attack Vectors

This subsection talks about the brief overview of the system-aware stealthy cyber-attacks targeting the RASc, as discussed in [10]. The main two objectives of the attack are 1) perform severe impact on the physical system and 2) disguise its malicious action from getting detected by the operator. In this work, we are assuming that the attacker is able to successfully install the malware in one of the local RAScs using any opening like USB drive, emails or other social engineering skills. Once the malware is installed, it provides backdoor access which can be exploited by the attacker in multiple ways. In this case, the attacker disables the original program running for the controller and executes the malicious program/script which was transferred earlier to the affected controller from the attacker. The malicious script performs two functions. First, it initiates the cyber-attack on the generator. Specifically, we consider two attack models, (pulse, ramp attacks) as mathematically represented in equations 1 and 2. Second, it replays the historical measurements which show the system is stable with a

motive to disguise the attack as benign operation. Since the RASc is not allowed to operate during the normal condition, the transmission line is tripped maliciously to remain in a stealthy mode, before executing attacks on generator. Normally, there are multiple reasons when line can be out especially during line faults and maintenance issues. Since we have considered the system to be stable for N-1 contingency, the single line outage does not involve any emergency or critical situation. In general, the proposed coordinate attack vectors include install malware on local controller, trip the line maliciously and finally execute the data integrity attacks (pulse, ramp) on generator while sending fake measurements to the operator. More details are provided in [10].

### A. Pulse Attack

This attack vector involves periodically changing the input control signal by adding the pulse attack parameter, $\lambda_{pulse}$, for a small interval ($t_1$) and retaining back the original input for the remaining interval ($T$- $t_1$) for the given time-period, ($T$).

### B. Ramp Attack

This attack vector involves adding a time varying ramp signal to the input control signal based on a ramp signal parameter, $\lambda_{ramp}$.

$$P_{pulse} = \begin{bmatrix} P_i(1+\lambda_{pulse}) & (t = t_1) \\ P_i & (t = T - t_1) \end{bmatrix} \quad (1)$$

$$P_{ramp} = P_i + \lambda_{ramp} * t \quad (2)$$

## IV. Proposed Architecture and Methodology

### A. Proposed Multi-Agents based Hierarchical Architecture

In this paper, we propose the MAS based hierarchical architecture for the RAS scheme where the large power system network is divided into different zones and each controller (RASc), working as a local agent, is in charge of the decision making process for the assigned zone. In general, we are proposing local agents based distributed Remedial Action Scheme, which is constantly monitored in a centralized manner by the central agent to detect the compromised agent. Fig. 2 shows the overview of the proposed architecture. The overseer, the central agent operating at the control center, collects system information from the RASc, operating at substations. Each RASc is the local agent which is responsible for monitoring and protection of the associated zone independently. It checks the local measurements coming from the zone sensors (relays, PMUs) and performs corrective actions through the actuators (MW, MVAR control) as required during disturbances. The state information provided by the local sensors in the specific zone, as shown by dark arrow, includes the relay and generator power measurements of the specific zone. Apart from the local measurements, each controller is also collecting the other (outside) zone's measurements from their corresponding sensors through the client-server communication, as represented by the colored,

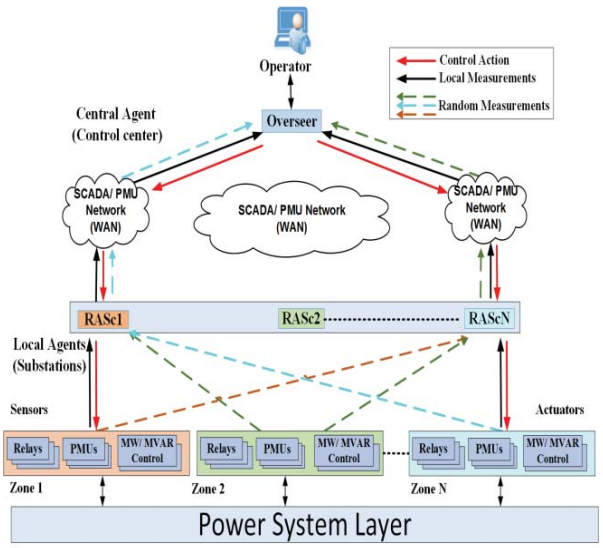


Fig. 2. Overview of the proposed architecture for multi-agent RAS.

$$X(t) = \left\{ x_1(t),\ x_2(t),\ x_3(t),\ x_4(t).....x_{n-1}(t),\ x_n(t) \right\} (1)$$

$$x_i(t) = \left[ x_{li}(t), x_{ri}(t) \right] \quad (2)$$

$$x_{li}(t) = \left[ Pg_{li}(t), Pl_{li}(t), L_{li}(t) \right] \quad (3)$$

$$x_{ri}(t) = rand\left( (x_{l1}(t), x_{l2}(t), x_{l3}(t), .....x_{ln}(t)) \notin x_{li}(t) \right) (4)$$

$$x_{rj}(t) = rand\left( (x_{l1}(t), x_{l2}(t), x_{lj}(t), .....x_{ln}(t)) \notin x_{lj}(t) \right) (5)$$

$$\gamma(t) = \begin{pmatrix} 0, & er <= \delta \\ 1, & er > \delta \end{pmatrix} \quad (6)$$

dotted arrow. The local state measurements from each controller are cyclically forwarded to the overseer, however, other zone's measurements are updated to the overseer in a dynamic, random fashion. Specifically, we have applied the concept of Moving Target Defense (MTD) strategy while sending outside measurement to the overseer. Implying that the outside measurements from each RASc are communicated to the overseer through the random sets of measurements. They are changed in unpredictable, random way in every cycle and since the measurement updates are no more static, the attacker is not able to guess the next update. Furthermore, the outside measurements send from each RASc introduce also redundancy in the system. It provides better visibility of system topology from the local controller's perspective to the overseer. For example, fig. 3 shows the example architecture for RASc2 which collects local zone 2, and other zone's measurement (zone 1 & zone 3), assuming total zones =3, and forward them to the

overseer. At each cycle update from $t_1$ to $t_4$, the RASc2 forwards the local zone 2 measurements, however, outside zone's measurements from zone 2, zone3 are selected randomly during $t_1$ to $t_4$ updates. It can be noted that after a few updates, overseer can completely observe the system topology through the eye of each controller. In this example, overseer can observe the complete system topology (zone1, zone2, zone3) in time $t_1 + t_2$. We have provided the mathematical expressions for the proposed architecture through equation 1 to 5. $X(t)$ represents the total measurements coming to the overseer at a particular instant t, which contains measurements from all controllers. $x_i(t)$ is the measurement update from the controller, RASci, operating at zone i which consists of local measurements, $x_{li}(t)$, and the random measurement, $x_{ri}(t)$, of other zones. The local measurements, $x_{li}(t)$, include the generation output, $Pg_{li}(t)$, line flows, $Pl_{li}(t)$ and lines status $L_{li}(t)$. They are periodically updated to detect zonal system disturbances and provide corrective actions by RASci. The random measurement, $x_{ri}(t)$, includes randomly selecting one of the outside local zonal measurements through the random function, rand( ), such that $x_{ri}(t) \neq x_{li}(t)$ and forwards it to the overseer along with the $x_{li}(t)$. Similarly, $x_{rj}(t)$, in equation 5, represents a random measurement for zone j at instant t which does not include local measurements, $x_{lj}(t)$, of its own zone.

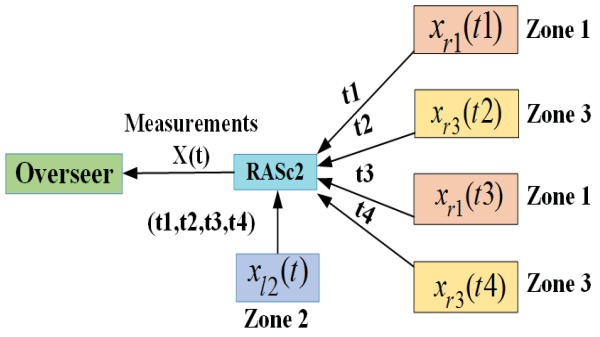


Fig. 3. Example architecture for zone 2 RAS Controller (RASc 2)

**TABLE I. Roles Assigned to Different Agents**

| Roles Assigned | Agents |
|---|---|
| 1) Receive updates from RAScs<br>2) Send Check commands to RASc<br>3) Alert the Operator during cyber attacks | Overseer (Central) |
| 1) Receive System measurements<br>2) Take corrective actions<br>3) Send updates to Overseer | RASc (local) |

Following the hierarchical level, the two-level of agents are performing their own three functions as defined in the action table, Table I. The overseer is allowed to receive updates from the controller, sends checks commands to the controllers during unacceptable measurement errors and alert the operators during cyber-attacks. The local controllers receive local and outside measurements, perform corrective actions to the assigned zones during outages and forward the randomly changing outside measurement to the overseer along with local measurements. The overseer oversees the controllers using an anomaly detection algorithm, making sure that the measurements are accurate and no controller is compromised. In the proposed architecture, agents are not allowed to communicate with each other as the compromised agent can provide false measurements to the others which may trigger the central agent to take corrupt decision.

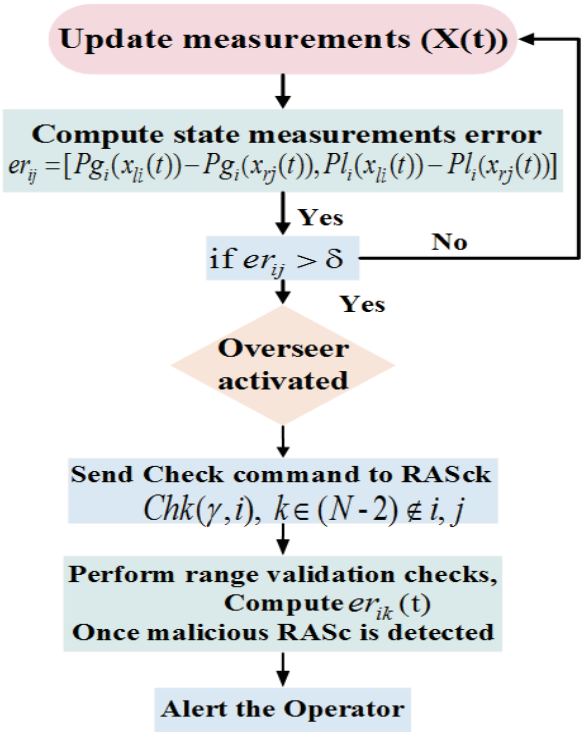


Fig. 4. Anomaly detection methodology to detect the compromised RASc

*B. Proposed Anomaly Detection Algorithm*

Fig. 4 shows the flow chart for the proposed anomaly detection methodology. In this work, we are assuming that the attacker is only modifying the local measurement updates, $x_{li}(t)$, and the integrity of random measurement, $x_{ri}(t)$, is unchanged as it difficult to guess the next update by the attacker. Initially, the overseer is periodically collecting the measurements from all the RAScs, $X(t)$. For each update, it computes the state measurement error, $er_{ij}(t)$, of the generation, $(Pg_i)$, and line flows, $(Pl_i(t))$, from the $i^{th}$ zone, $[Pg_i(x_{li}(t)),\ Pl_i(x_{li}(t))]$ and $j^{th}$ zone, $[Pg_i(x_{rj}(t)), Pl_i(x_{rj}(t))]$ at a particular instant t. For error, $er_{ij}(t)$, i and j represents the local and outside zones at time t. We have defined a parameter δ as the error threshold value to allow the acceptable error as the power system measurements are subjected to the noises and communication delays. When the computed error exceeds the defined threshold, δ, for either the generation or line measurements, the overseer is activated. It sends the check command, $Chk(\gamma, i)$, to the third controller, RASck, where k is selected randomly from the remaining N-2 controllers which are not involved in the error conflict. For $Chk(\gamma, i)$, i is the ith local zone and γ is a binary logic as defined in equation 6. When the $k^{th}$ controller receives the check

command, $Chk(\gamma, i)$, with γ=1, it sends the measurements of ith zone in the next cycle. The overseer performs range validation check by computing the error of the $k^{th}$ controller's (RASck) measurements of the ith zone with local $i^{th}$ controller's (RASci) measurements, as defined by $er_{ik}(t)$, and comparing it to the threshold. If error exceeds the defined threshold, the overseer confirmed that RASci is compromised and send the alert messages to the operator to provide situational awareness. In this process, the overseer is performing two-step verification to make sure that it successfully identifies the compromised RASc. Once the malicious controller is detected, the operator can take corrective actions like turn-off the malicious controller, disabling the router/switch etc.

## V. Experimental Set-up and Case Studies

Fig.5 shows hardware-in-the-loop based experimental set-up for the attack implementation. We have modeled the modified IEEE 39 bus in ePHASORSIM and simulated in the OPAL-RT, real time digital simulator. Fig. 6 shows the topology of the system and it is divided into three different zones or areas where decentralized RAS is implemented for each zone to prevent the thermal overloading during line outages. We have implemented the coordinated attacks on the RASc2 which is collecting measurements from the simulator (fig. 5). The simulator is integrated with two physical relays, as representing line L16-21, L16-24, which are connected to the remote terminal unit (RTU). For successful attack completion, we install the malware, Trojan Horse, written in python script (step1), which provides the backdoor connection to the attacker's computer (step 1). Next, we close the python program running for legitimate RASc and execute the python program for malicious RAS (step 2). Afterwards, the malicious tripping attack is performed by replaying the captured tripping packet on relay 1 which disconnects the line 16-21 to trigger the RAS (step 3). Finally, the attacker initiates the pulse/ ramp attack on the generator 35, while sending false measurement updates of generation to the overseer, running at the control center to hide the malicious action (step 4). Once the attack is successfully performed, we have collected the system data with timestamps from the simulator which is used later for the detection testing.

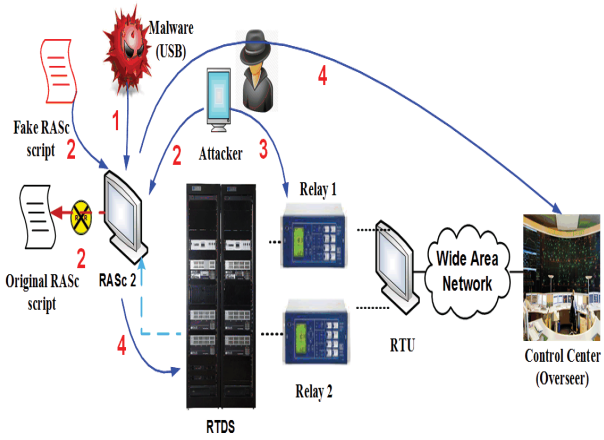


Fig. 5. Experimantal set-up for attack implementation in PowerCyber Lab.

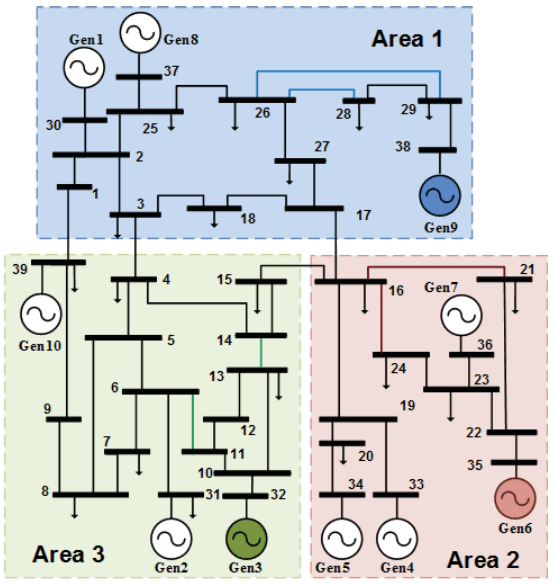


Fig. 6. Decentralized RAS Enabled Modified IEEE 39 Bus System

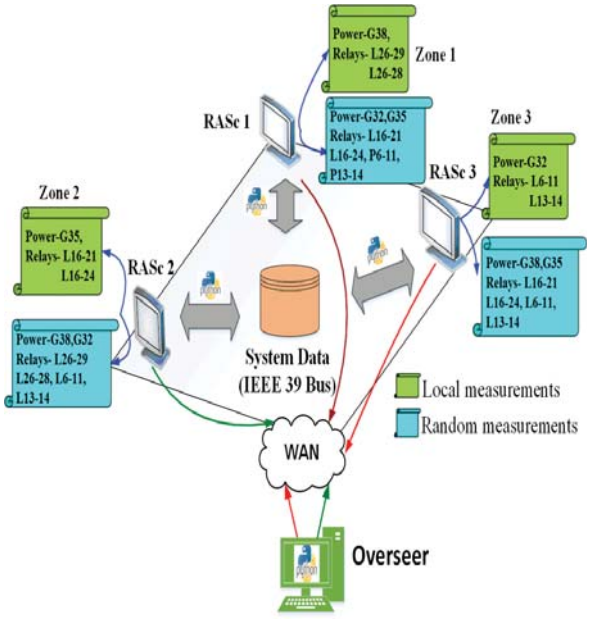


Fig. 7. Online anomaly detection topology for the 3 zones RAS.

Fig. 7 shows the MAS based online anomaly detection topology for 3 zones decentralized RAS where, each controller receives the list of local and random measurements. Each RASc is centrally monitored by the overseer. The RASc2 is operating in the zone 2, which polls the local zone measurements in terms of generator, G35, and line status, L16-21 and L16-24. It also polls the outside zone's measurements from zone 1 and zone 3 in terms of generators, G38, G32, and line statuses, (L26-29, L26-28), (L6-11, L13-L14) as shown in figure. For the detection testing, we develop the MAS using python script where each RASc is sending their measurement updates every 4 second to the overseer as shown in fig. 7. Initially, the system data with timestamps is stored in the python script of each controller, which initiates interaction with the overseer at the same time. The overseer is processing their data to the

online anomaly detection algorithm which is also running in the python script. Once the anomaly is detected, an alert is issued to the operator.

## VI. Results and Discussions

### A. Impact Analysis

Fig. 8 and 9 show the system behavior during the ramp and pulse attacks which are the final attack vectors. In case of ramp attack, as shown in fig. 8 (a, b, c), the malicious tripping was performed on line 16-21 (L16-21) at 78 *sec* (red dot). Pset represents the generator controller input, which is used to shed generation by RASc. PG35 shows the generator output during the attack. Due to successful stealthy attacks, the ramp attack starts at 96.1 *sec*, when attacker slowly ramps down the generator output (PG 35) with $\lambda_{ramp} = -0.03$. During the attack, the attacker is also sending initial false updates of the generator with an intention to hide the disturbances getting detected by the overseer, as shown by a red line, fig. 8 (b). The continuous ramping forces the generation lower than allowable limit during the line contingency. The continuous decrease in the generation level causes significant impact on system frequency. It drives the frequency to deviate from the nominal frequency, 60 Hz, and eventually going below 59.8

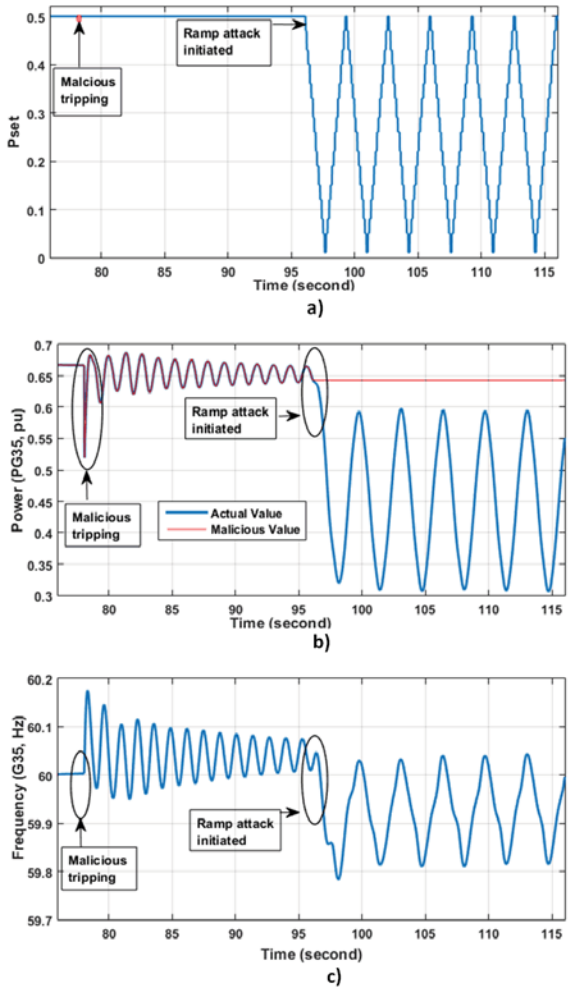


Fig. 8. Pset (a), Power output (b) and Frequency (c) during Ramp attack.

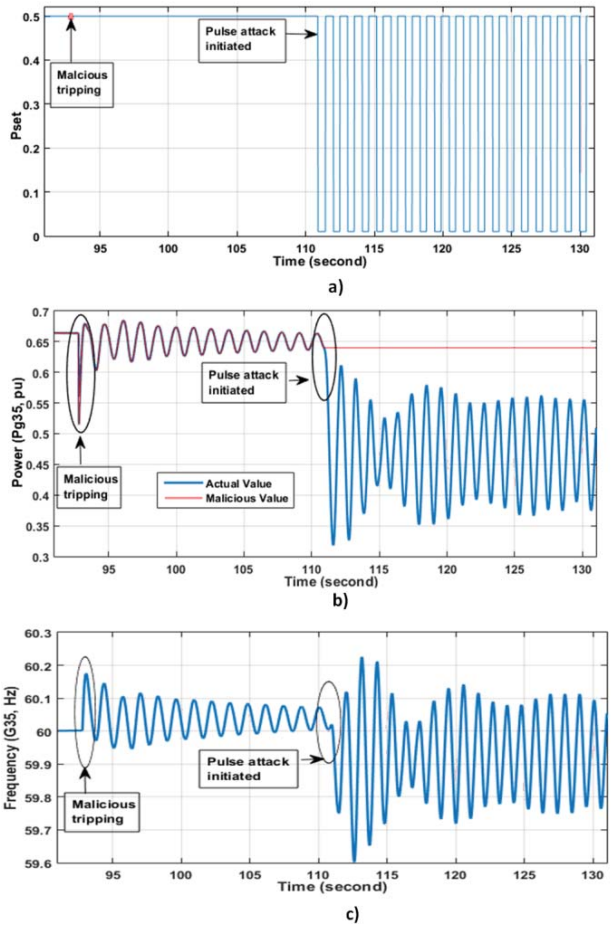


Fig. 9. Pset (a), Power output (b) and Frequency (c) during Pulse attack.

Hz at one point, which may affect the system stability and may cause load shedding. Fig. 9 (a, b, c) represents the pulse attack which is initiated at 111 *sec* after successful stealthy attacks, including the malicious tripping at 92.8 *sec*. During the attack, generation is varied uniformly in a time-period (T) of 1 *sec* with t1 = 0.5, $\lambda_{pulse} = -0.98$ and false updates are sent to the overseer. It should be noted that pulse attack is injecting sharp periodic disturbances causing more and faster oscillation in the system as compared to ramp attack for the given attack period of 20 *sec*. The generator experiences high mechanical stress due to continuous acceleration and deceleration which may damage it permanently.

### B. Performance Evaluation

Fig. 10 and 11 show the online performance of the proposed algorithm in terms of detection cycle and latency during the pulse and ramp attacks. From fig. 10, it can be observed that the number of cycles to detect the attack is similar in both attack vectors for a small detection threshold. However, as we increase the detection threshold from 0.0025 to 0.05, the ramp attack takes higher number of cycles (Nc) as compared to the pulse attack to detect the anomalies. Higher the threshold, it takes longer time for the detection and the difference margin between the two attack cycles keeps increasing as we increase the threshold. Since the pulse attack causes sharp deviation from the initial state, it can be detected much faster than the ramp attack which

gradually pulls down the generation. It is to be noted that cycle is the frequency of measurement updates which can be changed based on system and code execution time. In this work, the measurement is updating every 4 *sec*. Fig. 11 shows the latency involved in detecting the compromised RASc once the measurement error crosses the error threshold for the total 48 cases. We have successfully detected the attacks with average delay of 0.389 and maximum delay of 1.25 cycle. Since it is not dependent on the nature of attacks, we have not plotted it separately for pulse and ramp attacks.

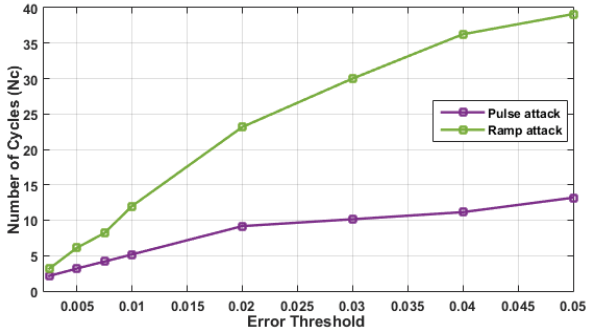


Fig. 10. Detection Cycles for Pulse and Ramp attack

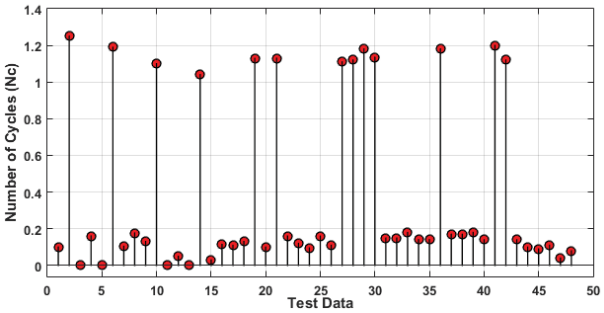


Fig. 11. Latency in term of cycles during Pulse and Ramp attack.

## VII. Conclusion and Future Challenges

In this paper, we propose a two-level hierarchical multi-agent based remedial action scheme which consists of distributed local agents which are periodically monitored by the overseer, the central agent. In this paper, we have provided limited and specific function to agents to avoid vulnerabilities which might be exploited by smart attackers. We have also proposed the anomaly detection methodology based on random measurement updates, inspired by MTD based strategy to detect the stealthy malicious attacks. Initially, we have demonstrated how the sophisticated attackers can perform coordinated attacks which can severe impact on generator through ramp and pulse attacks. Later, we have implemented the proposed architecture along with detection methodology through the experimental set-up and validated through the online testing for different cases. Finally, we have evaluated its performance in terms of detection rate and latency. Based on the performance analysis, it can be concluded that higher detection threshold lead to the significant delay in the anomaly detection. Since system measurements are also subjected to errors and noise, proper tuning of threshold is necessary to make it effective with minimum false alarms. Furthermore, the smaller computed latency during the detection shows its efficiency towards developing attack-resilient protection scheme. The proposed approach hardens the process of performing stealthy attacks and making it more attack-resilient. The potential avenue for the future work will be to perform deeper analysis while considering other factors like communication delay and measurement error as well as developing methodology for the cases where multiple controllers are compromised with other possible attack vectors.

## Acknowledgment

The research is funded in part by the NSF CPS and DOE CEDS research program.

## References

[1] Special Protection Systems (SPS)/ Remedial Action Schemes (RAS): Assessment of Definition, Regional Practices, and Application of Related Standards, NERC Draft committee.

[2] J. McCalley et al., “System Protection Schemes: Limitations, Risks, and Management “, PSERC, Dec. 2010.

[3] NERC, “Security Guideline for the Electrical Sector: Identifying Cyber Critical Assests” June 17, 2010.

[4] Industrial Control System Cyber Emergency Response Team (ICS-CERT), “Monitor (ICS-MM201212)”, January 2012 [Online].

[5] N. Falliere, L. O'Murchu, and E. Chien. W32.stuxnet dossier. Technical report, Symantec, Feb. 2011.

[6] National Vulnerability Database (NVD), National Institute of Standard and Technology (NIST), https://nvd.nist.gov/, [Online].

[7] H. F. Wang, “The “third-category method and multi-agent system theory in power system applications” in Proc. of IEEE Power Engineering Society General Meeting, vol.2, pp. 1042-1043, 2005.

[8] J. Wen, W. H. E. Liu, P. L. Arons and S. K. Pandey, "Evolution Pathway Towards Wide Area Monitoring and Protection—A Real-World Implementation of Centralized RAS System," in *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1506-1513, May 2014.

[9] K. J. Ross, K. M. Hopkinson and M. Pachter, "Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security," in *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 1216-1224, June 2013.

[10] V. Kumar Singh, A. Ozen and M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," *2016 North American Power Symposium (NAPS)*, Denver, CO, 2016, pp. 1-6.

[11] Srinivasan D., Jain L.C. (eds) Innovations in Multi-Agent Systems and Applications - 1. Studies in Computational Intelligence, vol 310. Springer, Berlin, Heidelberg.

[12] H. F. Wang, “The “third-category method and multi-agent system theory in power system applications” in Proc. of IEEE Power Engineering Society General Meeting, vol.2, pp. 1042-1043, 2005.

[13] Lei Luo, Nengling Tai, Guangliang Yang, Wide-area protection research in the smart grid, Energy Procedia, 16 (2012), pp. 1601-1606.

[14] Z. Liu, Z. Chen, C. Liu, H. Sun and Y. Hu, "Multi agent system based wide area protection against cascading events," *2012 10th International Power & Energy Conference (IPEC)*, Ho Chi Minh City, 2012, pp. 445-450.

[15] Pengyuan Wang and M. Govindarasu, "Multi intelligent agent based cyber attack resilient system protection and emergency control," *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Minneapolis, MN, 2016, pp. 1-5.

[16] A. C. Pappa, A. Ashok and M. Govindarasu, "Moving target defense for securing smart grid communications: Architecture, implementation & evaluation," *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, 2017, pp. 1-5.