DIRAS: Distributed Image Reconstruction in Adversarial Scenario

Thesis to be submitted in partial fulfillment of the requirements for the degree

of

Dual-degree (B.Tech + M.Tech) in Electrical Engineering with specialization in Signal Processing and Instrumentation

by

Shailesh Mishra
17EE35014

Under the guidance of

Prof. Sanand Dilip Amita Athalye

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Department of Electrical Engineering
Indian Institute of Technology,
Kharagpur
India - 721302

CERTIFICATE

This is to certify that we have examined the thesis entitled **DIRAS: Distributed Image Reconstruction in Adversarial Scenario**, submitted by **Shailesh Mishra** (Roll Number: *17EE35014*) a postgraduate student of **Department of Department of Electrical Engineering** in partial fulfillment for the award of degree of Dual-degree (B.Tech + M.Tech) in Electrical Engineering with specialization in Signal Processing and Instrumentation. We hereby accord our approval of it as a study carried out and presented in a manner required for its acceptance in partial fulfillment for the Post Graduate Degree for which it has been submitted. The thesis has fulfilled all the requirements as per the regulations of the Institute and has reached the standard needed for submission.

[illegible]

Supervisor

Department of Department of Electrical Engineering
Indian Institute of Technology,
Kharagpur

Place: Kharagpur
Date: November 25, 2021

ACKNOWLEDGEMENTS

I would like to thank Prof. Sanand for providing me with this amazing opportunity to collaborate with him where we have been able to develop a distributed system for image reconstruction.
I would also like to thank my parents for their constant support, without which it would have been impossible for me to complete this work.

Shailesh Mishra
IIT Kharagpur
Date: November 25, 2021

ABSTRACT

Cyberphysical Systems (CPSs) have seen wide integration in numerous fields of science and technology because of their ability to acquire and process a large number of data from various sources simultaneously. Among the various types of data processed by CPSs, image is one of the most prevalent. Images are extensively used for improving the processes in healthcare, agriculture, military, etc. and perhaps, can be used in many other sectors of our life. The standard model of CPSs analyzing images consists of a raft of sensors obtaining the image data and a central entity that deploys various algorithms to process the images of the sent by the sensors.

Although the algorithms and learning models developed for processing images have greatly improved the efficacy of CPSs based on images, it has also introduced a new issue of security in CPSs. Images obtained by the CPSs are from various aspects of our life and if they are leaked, then a large amount of sensitive information can be obtained by an attacker. Moreover, if this image data is tampered with by an adversary, then it can lead to wrong analysis. It should be also noted that the cumulative size of the data acquired by numerous sensors is humongous and hence, difficult to be handled by a central entity. The failure of this central entity can lead to the failure of an entire CPS. Therefore, there are multiple issues prevalent in the architecture of existing CPSs that need to be solved.

Therefore, in this research work, we have proposed *DIRAS*, a distributed framework for reconstructing images in a secure manner. Being a distributed system, DIRAS solves the issue of scalability of CPSs. A novel leader-based consensus algorithm has been proposed to regenerate images. DIRAS has been designed to tackle multiple security attacks in the network. Splitting of data has been incorporated into it to enhance the efficiency and privacy of data. A comprehensive description of its implementation has also been provided and the results obtained from the implementation prove that DIRAS is scalable, secure and privacy-preserving. DIRAS has been designed such that it can be incorporated into any CPS that works with matrices.

Keywords: Cyberphysical System (CPS), Image, Matrix Completion, Image Reconstruction, Security, Privacy, Robust Principal Component Analysis (RPCA)

Contents

List of Figures

Chapter 1

Motivation

Cyberphysical Systems (CPSs) combine physical processes, computational processes and communications networks aiming to enhance the overall functioning of systems [4]. CPSs have found great usage in various domains such as power grids, healthcare, supply chain and various other fields. Another sister technology of CPS is the *Internet of Things* (IoT), which connects all the devices over the internet so that the devices can interact with each other to reach a common goal [3]. Around 20 billion IoT devices will be connected in 2022, with that number expected to rise to 41 billion by 2025 [28, 18]. Due to the abundance of data acquired by billions of sensors and the cumulative processing power of the billions of devices, CPS and IoT have revolutionized the way various systems are handled. Along with the IoT, CPSs have played an integral role in improving the efficacy of the existing processes.

CPSs and IoT acquire various types of data, process them and take actions according to the implications obtained from the processing. CPSs acquire and process data such as image, audio, temperature, humidity, voltage and many more. Among all the above-mentioned types of data processed by CPSs, images hold great importance. With the recent advancements in image capturing ability of devices and computer vision [19, 1, 33], images have become an integral form of data in our lives. Recently, analysis of image has become a key component for proper functioning of agriculture [34], medical systems [12], remote sensing [9], robotics [22] and many other fields. Therefore, image data holds great value in various fields.

However, the generation of terabytes of image data by CPS and IoT has made the management of data extremely difficult. The sharing and storage of such a huge amount of data has become a prevalent issue in CPSs, which has been exploited by adversaries extensively. Firstly, in the conventional architecture, CPSs that process images, deploy a central processing unit. Such CPSs have sensors that constantly acquire image data from the surroundings and these sensors send the recorded data to processing units. The processing units analyze the acquired data and direct the actuators to take required actions. A centralized architecture is not scalable, i.e., the processing unit won't be able to handle the increase in number of sensors. With the steep rise in application of CPS in various domains, this scenario is imminent. Secondly, if the processing unit fails or is compromised, then the whole framework would fall. Therefore, there's the issue of *single point of failure*. Next, the images, acquired by the sensors from their surroundings, contain sensitive information. Consider sensors deployed in a hospital or a military base. If compromised, such images can lead to fatal consequences. Lastly, the communication channel is also vulnerable, i.e., an adversary can sniff packets from the packets that are being shared between the sensor and the computing unit which is a classic example of the man in the middle (MITM) attack [31]. If this attack is successful, then the attacker can easily tamper with the image. This can lead to false data injection attacks [25]. Such an attack would alter the image which can lead to grave consequences. For example consider the wrong analysis of an image related to a patient due to this attack. In another scenario, an adversary can execute a denial of service (DoS) [24] attack, where the connection to a specific node (the computing unit) is completely blocked by the adversary. Here, the attacker sends a large volumes of data to the victim node, which prevents the victim from having any contact with the honest nodes in the network. Therefore, there are numerous issues that exist in the frameworks that involve communication of images from sensors to computing units in CPSs.

To overcome the above-mentioned issues, we propose *DIRAS*, a distributed and robust solution for reconstructing images in CPSs. DIRAS reconstructs images in a distributed manner which can be further used for analysis. DIRAS consists of multiple nodes for computation (which have been called as monitor nodes) that mitigates the issue of centralization, and thus, the issue of single point of failure. In the case of DIRAS, the sensors split the images into chunks and distribute it to the sensors. Splitting of data improves the privacy of data. DIRAS deploys an efficient, random consensus algorithm along with robust principal component analysis (RPCA) [7] for image reconstruction, even in the case of false data injection attack. DIRAS incorporates numerous design schemas to mitigate other various kinds of attacks.

Overall, DIRAS provides a novel solution to reconstruct images of sensors that can improve the performance of existing systems greatly. The major contributions of this work are:

1. A novel distributed framework consisting of sensor nodes and monitor nodes to reconstruct images. It deploys RPCA and matrix completion [21] to improve the robustness of image reconstruction.

2. A light-weight, randomized leader selection algorithm for reaching a consensus among the monitor nodes.

3. An efficient data splitting mechanism by sensors to enhance data privacy and reducing the overheads.

4. Evaluations based on implementation of communication network and image reconstruction which prove the scalability and robustness of the framework.

5. Analysis of privacy and security provided by the framework which prove its better performance over classical centralized models.

Rest of the report has been organized as follows: Section 2 outlines the relevant research that has been conducted in this field. Section 3 provides necessary background knowledge for this research. Section 4 elucidates the design of the system, various algorithms used and the mechanisms deployed. Section 5 discusses the implementation of the developed system. Section 6 describes the results from the implementation and compares the proposed model with the existing models. Section 7 elaborates on the implications obtained from the evaluations and the performance of the framework against various attacks. Section 8 outlines the work that needs to be done in the future. Section 9 concludes the report.

Chapter 2

Literature Review

The work that has been presented in this report spans three different research fields which are: security in CPSs, distributed optimizations and image reconstruction. Here, we study the existing work that has been done in these three fields.

2.1 Security in CPSs

Numerous research works have addressed the security issues that exist in CPSs. In [29], the authors have presented control-theoretic approaches to cyberphysical security. First of all, the models of CPS, monitors and attacks have been described. *Detectability* and *identifiability* of attacks for these models have been defined. Then, they discuss the detection and identification limitations from system and graph-theoretic perspectives. They have also discussed monitor design problem and provided a case study on coordinated attacks against power networks. They have used power systems networks and water networks as example for study in the paper. In [32], the authors have proposed two algorithms for state reconstruction from sensor measurements which are corrupted with sparse attack. In [17], malicious state attacks in a remote state estimation has been considered. Here, a smart sensor node transmits data to a remote estimator equipped with a false data detector. The authors have presented an optimal linear deception attack on sensor data where the adversary can successfully inject data and remain undetected by the false data detector. In [14], the authors have proposed a technique for exact reconstruction of the discrete state of a switching system, when only the continuous output is accessible and the discrete output is not available. They have also investigated the scenario where the continuous input and output signal is adulterated by malicious attacks. All these works have presented formidable solutions for attacks.

2.2 Distributed Optimizations

In [39], the authors elaoborate on various distributed optimization algorithms. In distributed optimization of multi-agent systems, the agents collaborate with each other to minimize a global function which is the sum of local objective functions. In [2], the authors have presented a decentralized technique to solve the equation $Ax = B$ in the case of network of agents. In [27], the authors have provided an overview of distributed methods for optimization in networked systems. A distributed architecture can help to overcome the issues of scalability, single point of failure and privacy breaches that exist in the case of a centralised model.

In addition, in the case of distributed computing, there are multiple algorithms that have been proposed to reach consensus. First of all, there is Paxos [23] which presents an algorithm where a proposer proposes a value and a common value is accepted by an acceptor. Paxos is used for message sharing where the nodes want to reach a common point. A recent technology that has also received great attention is *blockchain*. Bitcoin [26] is the most famous cryptocurrency and the most widespread application of blockchain. Bitcoin deploys the Proof-of-Work (PoW) to reach a consensus. Here, the nodes solve a computationally expensive problem to become the miner. The miner is the node in the blockchain that adds a new block to Bitcoin. Although the application of Paxos and PoW is different, there is one similarity between these two algorithms. They work on the basis of a leader selection who executes the main task of maintaining the framework. This idea has also been used in DIRAS to reach a consensus.

2.3 Image reconstruction

Image reconstruction has received great attention recently. It has been used extensively in the field of tomography [37]. Image reconstruction methods are being used for reconstructing 3D images from various projections of the image. The work done in [36] discusses proposes machine learning algorithms for image reconstruction in tomography. In [5], the authors have presented the application of deep learning algorithms for fluorescence image reconstruction. The auhtors in [35] have proposed a deep learning algorithm for tomographic image reconstruction.

All the methods proposed for image reconstruction are executed by powerful machines (personal computers) at a particular location. Such a framework cannot be used in CPS because the devices are computationally less powerful. DIRAS, the solution that we have proposed here, considers first of all the security in CPS and tries to mitigate the effects of attacks. Next, DIRAS is a distributed framework and uses an algorithm which is inspired from the work in [26]. Moreover, the distributed optimization using Least Squares Solution, as presented in [27], provides a completely distributed solution but the solution provided by this is not accurate enough. The matrix generated after this optimization has each element equal to the element of the actual matrix divided by the total number of elements (the element will be normalized). Thus, although the system will reach a consensus, the deviation will still be very high. Due to this reason, we have deployed a leader-based algorithm that helps in reaching consensus quickly and regenerating images fast. DIRAS uses RPCA and matrix completion as its core component for reconstructing mmatrices. In the next section, we describe these two technologies.

Chapter 3

Background

In this section, we describe the technologies which form an integral part of DIRAS. Robust Principal Component Analysis has been used for extracting a low-rank matrix from the matrix that is obtained after collecting the image from other nodes. On the other hand, matrix completion has been used for solving the issue that arises when an adversary simply drops packets and does not allow the packet to reach the destination node. These two algorithms have been elaborated in this section.

3.1 Robust Principal Component Analysis

Robust Principal Component Analysis (RPCA) is the algorithm for obtaining the low rank matrix and the sparse component of the matrix when the matrix is corrupted [7, 38]. It is the modification of the long established Principal Component Analysis (PCA) to make it work even in the case of gross corruption of the data. First of all, we have defined what is PCA and then, elaborate about RPCA.

Suppose we have a data matrix which is the sum of a low rank matrix and a sparse matrix. PCA is the method via which we can obtain the low rank matrix and the sparse component from the data matrix. This is possible only under certain assumptions and can be achieved by solving a convex optimization problem called *Principal Component Pursuit*.

PCA is widely used for data analysis and dimensionality reduction problems. However, its performance reduces greatly when the data is *grossly* corrupted[1]. Therefore, RPCA has been developed for making the process of PCA robust.

[1]Gross errors are the ones which are generally large with respect to the data.

Many RPCA mechanisms have been proposed in literature using multivariate trimming [16], alternating minimization [20], and random sampling techniques [15]. However, these algorithms do not provide a polynomial-time complexity and hence, can be inefficient in case of large matrices. The RPCA described in [7] is the improved version of the other algorithms and yields the low-rank matrix from a highly corrupted matrix.

Hence, in the case of DIRAS, we have used the RPCA described in [7] and we describe the performance of the algorithm in Section 6.

3.2 Matrix Completion

Matrix Completion will be used in DIRAS when RPCA alone will not be able to provide efficient results. This would occur when multiple packets will be unavailable for the node that will reconstruct the image. Therefore, matrix completion is a very important part of DIRAS to improve its security.

In [8], the authors have provided a method for completing a matrix with minimal entries. They have proposed that nuclear-norm minimization subject to data constraints, which is a convex optimization problem, needs to be solved to complete a data matrix. Their results prove that matrix completion provides satisfactory output in case of small noise in the data. The work done by the author in [30] provides a method to complete matrix by minimizing the nuclear norm of the hidden matrix. In [21], the authors have presented a method called OptSpace to improve on the work presented in [8] and [30]. We have also deployed the nuclear-norm minimization technique for matrix completion.

Next, we explain how DIRAS has been designed and how these two technologies mentioned here help in robust image reconstruction.

Chapter 4

System Design

In this section, we describe the architecture of DIRAS and the algorithms deployed in it. DIRAS is a distributed framework for reconstructing images, even in the case of attacks. DIRAS deploys defense mechanisms against false data injection attack, DoS attack and the scenario where the adversary drops a packet. DIRAS also deploys image splitting for improving privacy of information. All the features have been elucidated of DIRAS have been elucidated in this section. First of all, the assumptions made while designing DIRAS have been described. Next, the components of DIRAS have been outlined. Then, the various mechanisms and algorithms used in DIRAS have been explained. Table 4.1 provides the various terminologies used in this section to describe the various components of DIRAS.

4.1 Assumptions

The essential assumptions made while designing DIRAS are as follows: (i) The processing nodes, that reconstruct the image, are connected over a *peer-to-peer* (p2p) network. In other words, all the processing nodes are connected with each other; (ii) The p2p network is synchronous; (iii) All the processing nodes are trusted, i.e., a node that receives data from the monitor does not behave maliciously; (iv) The processing nodes have enough computational power to run algorithms and reconstruct the image; and (v) Sensors have enough computational power to split matrices.

Table 4.1: Definition of the terminologies used

Terminology	**Definition**
S_i	$i-th$ sensor node
SN	Number of sensor nodes
I_i	Image generated by $i-th$ sensor node
$(x_i(I_i), y_i(I_i))$	Coordinates corresponding to the $i-th$ sensor node for the image I_i
M_j	$j-th$ monitor node
MN	Number of monitor nodes
(x_j, y_j)	Coordinates corresponding to the $j-th$ monitor node
Δ	Epoch time (in seconds)
δ	Time (in seconds) a leader waits before reconstructing the image
$C(I_i)$	Set of chunks of the image I_i
$C_j(I_i)$	Chunk of the image I_i sent to the $j-th$ monitor node
I_i_ID	Identifier of the image generated by the sensor
M_j_ID	Identifier of the monitor node
$L(I_i)$	Leader for the image I_i
β_j	Count of the number of images reconstructed by the $j-th$ monitor node

4.2 System Architecture

Here, we discuss the building blocks of DIRAS. Figure 4.1 depicts the high-level architecture of DIRAS.

4.2.1 Sensor Nodes

These are the part of CPSs that acquire the image data from the surroundings. After acquisition of images, the sensor nodes split the images into chunks and send it over to the monitor nodes. Splitting helps in two ways: (i) splitting an image leads to improved privacy because an adversary cannot acquire enough information from chunks of an image; (ii) splitting reduces the bandwidth consumption on a particular communication channel. Furthermore, the sensors can record images from any source

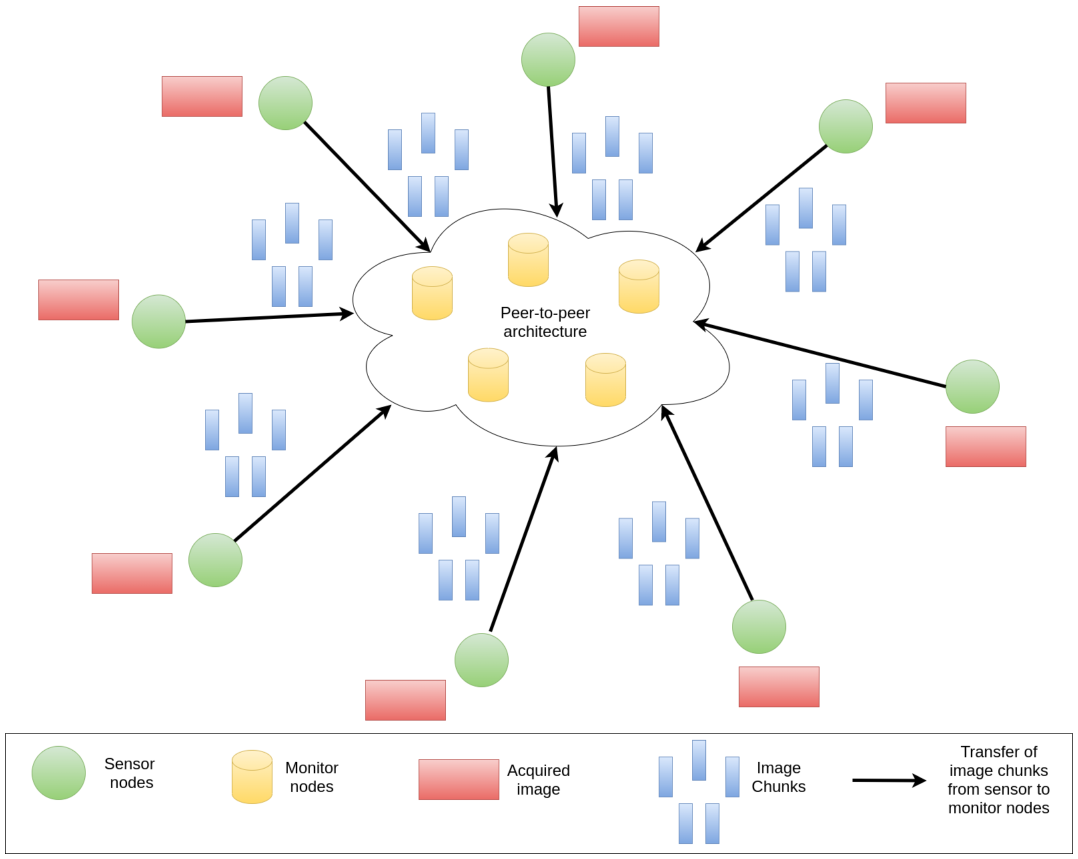
Peer-to-peer architecture
Sensor nodes
Monitor nodes
Acquired image
Image Chunks
Transfer of image chunks from sensor to monitor nodes

Figure 4.1: High level architecture of DIRAS

such as from a factory or a hospital, thus making DIRAS platform independent.

4.2.2 Monitor Nodes

These are the processing units of the CPSs. They are the nodes that receive chunks of acquired images from the sensors and reconstruct the whole images. The images regenerated by the monitor nodes can be used further for other processing and analysis. These analyses are beyond the scope of this work.

4.2.3 Peer to peer(p2p) network

The monitor nodes are connected over a p2p network. This is to ensure that any monitor node can share a packet with any other monitor node. This is a reasonable assumption because considering the advent of the IoT, most of the processing devices around us are connected to each other. Thus, making such an assumption would not make a huge difference to the current architecture.

4.3 Functionality

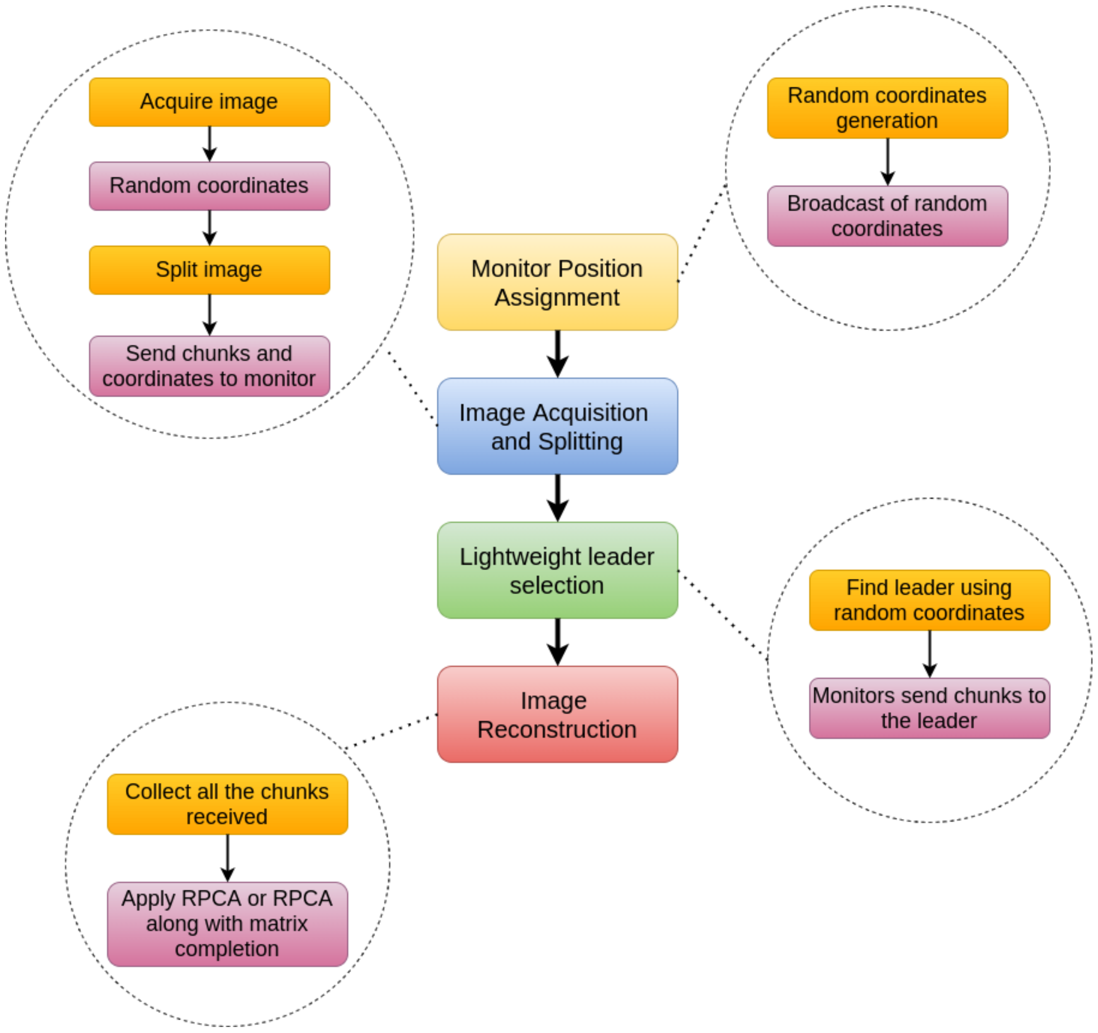
Acquire image
Random coordinates
Split image
Send chunks and coordinates to monitor
Random coordinates generation
Broadcast of random coordinates
Monitor Position Assignment
Image Acquisition and Splitting
Lightweight leader selection
Image Reconstruction
Find leader using random coordinates
Monitors send chunks to the leader
Collect all the chunks received
Apply RPCA or RPCA along with matrix completion

Figure 4.2: Various steps involved in DIRAS

Here, the various design schemas and algorithms used in DIRAS for its functioning, and making it efficient and robust have been described. Figure 4.2 depicts the various functionalities involved in DIRAS. First of all, DIRAS is a distributed framework for reconstructing image. Being a distributed system, the monitor nodes in DIRAS need to reach a consensus for regenerating images efficiently. We do this by using a lightweight consensus algorithm. For each image, a leader is selected randomly who is responsible for aggregating all the chunks of an image and then, reconstructing it. This design ensures lower overhead and does not overburden any particular monitor node. The details of this algorithm have been discussed below.

4.3.1 Monitor Position Assignment

This is an important step in the functioning of DIRAS. In this step, the monitor nodes generate 2-D coordinates (x_j, y_j) with each coordinate being a (pseudo)random integer (from now on we refer a psuedorandom number as a random number). (x_j, y_j) is generated by the monitor nodes for every epoch time Δ. It should be noted that the sensor nodes do not know about the coordinates of the monitor nodes. Thus, changing of the coordinates (x_j, y_j) appears to be superfluous to the design. In spite of this, the monitor nodes keep changing the set of coordinates for each Δ. It is so as to improve the security of DIRAS against DoS attack (explained in the section 7). After generating the coordinates, the monitor nodes broadcast these packets to all other monitor nodes. The structure of the packet sent by a monitor node is $< M_j\_ID, (x_j, y_j) >$.

After receiving the packets from all the monitor nodes, the monitor nodes simply store the coordinates of all other nodes in its memory. The position assignment is an important step for the leader selection.

4.3.2 Image Acquisition and Splitting

This is the task carried out by the sensors of DIRAS. The sensors acquire images from their surroundings continuously. After acquiring an image I_i, a sensor generates a 2-D coordinates $(x_i(I_i), y_i(I_i))$ with each of the coordinates being a random number. The coordinates being a function of I depicts that a sensor node generates unique coordinates for every image acquired. The image acquired by the monitor will have the R, G and B components. Thus, the dimension of the acquired image matrix would be $m \times ntimes3$ (where m is the number of rows in the image and n is the number of columns in the image). Before splitting the image, the R, G and B components are stacked vertically, i.e., the order of the new matrix becomes - $3m \times n$. After stacking the image vertically, a sensor splits the image into chunks row-wise. We have carried out the splitting row-wise but it can be done column-wise (if done column wise, then the stacked matrix would be $m \times 3n$) or by any other way that can be decided by the network operator. After splitting the image, the sensor form packets whose structure is: $< I_i\_ID, M_j\_ID, C_j(I_i), (x_j, y_j) >$.

All the components of the packet have been explained in Table 4.1. The packet depicted here is for a single chunk of image sent by the $i - th$ sensor node to the $j - th$ monitor. After receiving this packet, the monitor nodes select the leader for the image.

4.3.3 Lightweight Random Leader Selection Algorithm

The most important in a distributed system is to reach a *consensus*, i.e., all the nodes in the p2p network should be in the same state. This is a challenge in any distributed system. In the case of DIRAS, we achieve this by selecting a leader for every image. The leader is selected by using a simple method which has been described below.

1. Each monitor node finds the distance between the coordinates generated by every monitor node and the coordinate sent by the sensor node by using the formula: $D_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$.
2. Then, the monitor node evaluate the monitor node in the p2p network that has the minimum D_{ij} for the image.
3. The one with the minimum D_{ij} is the leader for the image.
4. Every other monitor node sends its $C_j(I_i)$ to the leader and the leader can then reconstruct the image whose structure is $< I_i\_ID, M_j\_ID, C_j(I_i) >$.

The leader selection algorithm is not a new concept in distributed systems. It has been used extensively in blockchains [26]. In standard blockchains, the leader (which is called the miner) is chosen on the basis of a cryptographic puzzle. The one who solves the puzzle becomes the miner of a block and adds a block to the blockchain. However, the algorithm used in the case of [26] is resource intensive and requires a lot of time and power. Therefore, we have introduced a lightweight and random algorithm to select a leader for reconstructing an image.

This algorithm appears to be a little centralized with respect to a particular image. But if we consider a long duration of time, this algorithm is decentralized because the leader is selected on the basis of four random coordinates. Thus, if considered honest behavior from all the nodes in the network, this algorithm is decentralized. Another choice would be to design a completely decentralized algorithm where each monitor node reconstructs the image. In this case, after receiving the packet from the sensor node, each monitor node would broadcast the packet to all other nodes in the network. However, this mechanism would increase the overheads greatly making the system very inefficient. Thus, the algorithm in DIRAS, which is distributed with respect to time, provides an optimal distributed solution. We have compared the performance of DIRAS with the above-mentioned decentralized model in section 6. Next, we discuss the reconstruction of the image by a monitor node after it receives all the packet.

4.3.4 Image Reconstruction

After receiving the first packet corresponding to an image from a source, each node starts a timer. This timer is integrated so that a leader does not wait indefinitely for reconstructing an image. Each leader waits for a time δ after receiving the first packet. After the time δ is over, the leader starts the reconstruction process. The leader builds a matrix whose dimension is $3m \times n$. Therefore, the leader first breaks the matrix into 3 matrices of size $m \times n$. After this, it has two paths for reconstruction: (i) *The leader receives all the packets*: In this case, the leader first of all combines all the chunks and then, applies RPCA to extract the low-rank matrix. The low-rank matrix is the image that will be used by other systems for analysis; (ii) *The leader receives some of the packets*: This means that the packet sent by either the monitor node or the sensor node gets dropped. In this case, the leader combines all the chunks and makes the rows equal to zero which it hasn't received. Then, it applies RPCA on the matrix that it gets after combining all the rows. The next step is to apply matrix completion algorithms on the matrix that has been obtained after applying RPCA. The matrix obtained after matrix completion is the reconstructed image that will be used for further analysis.

This is how the whole image reconstruction algorithm works in DIRAS. Next, we discuss load balancing, a mechanism to improve DIRAS.

4.3.5 Improvement in DIRAS: Load Balancing

DIRAS uses a very simple algorithm for selecting the leader which generates the final image. This algorithm uses random numbers which makes it non-deterministic and efficient. However, the randomness also distributes the tasks among the monitor nodes randomly. Therefore, there will be multiple scenarios where one node may have to reconstruct more images than the others. This will induce latency in the functioning of the network because more traffic will be there at some M_j. To prevent this scenario, we have added the feature of load balancing to improve DIRAS. The load balancing algorithm is again a simple yet effective one (we prove is efficacy in the results). Next, we discuss the load balancing algorithm.

Recall that the leader was chosen based on the algorithm:

$$\begin{aligned} L(I_i) = j, \quad \text{s.t.} \quad \min_{j} \quad D_{ij} \\ \text{where} \quad D_{ij} = \sqrt{(x_i(I_i) - x_j)^2 + (y_i(I_i) - y_j)^2}, \quad \text{j} = 1, ..., \mathbf{MN} \end{aligned}$$

, where all the coordinates are random numbers. To mitigate the issue of uneven load distribution, we have introduced β_j, which is the total number of images regenerated by a monitor node. For load balancing, all the monitor nodes keep a track of β_j of all the monitor nodes in the network. After the integration of load balancing, the leader selection algorithm becomes,

$$\begin{aligned} L(I_i) = j, \quad \text{s.t.} \quad \min_{j} \quad F_{ij} \\ F_{ij} = D_{ij} + \beta_j \times \max_{j} \quad D_{ij} \\ \text{where} \quad D_{ij} = \sqrt{(x_i(I_i) - x_j)^2 + (y_i(I_i) - y_j)^2}, \quad \text{j} = 1, ..., \mathbf{MN} \end{aligned}$$

The term $\beta_j \times \max_{j} \quad D_{ij}$ has been added for load balancing. This term ensures that the monitor nodes, which have regenerated more images already, don't have to reconstruct the incoming images. Thus, this load balancing algorithm ensures that the computation burden is distributed evenly.

In the next section, we elaborate on the implementation of DIRAS so as to evaluate its performance.

Chapter 5

Implementation

In this section, we describe the implementation of our system. We have separated the implementation of the system into four parts: (i) communication network; (ii) image reconstruction framework; (iii) load balancing analysis; and (iv) privacy analysis.

5.1 The Communication Network

DIRAS involves sharing of data among monitor nodes and transfer of packets from sensor nodes to the monitor nodes. Therefore, there's a communication network established. The first implementation is done so as to study the scalability of the network, i.e., the performance of the network when the number of sensor nodes and monitor nodes increase. This implementation was done on ns-3 network simulator. First of all, the sensor nodes and monitor nodes were created in the simulator. The monitor-monitor and sensor-monitor connections are established. Then, monitor nodes transfer packets to each other for completing the step of *monitor position assignment*. Then, the sensor nodes generate images (each node generates five images), split the image into chunks and send the chunks to the respective monitor nodes. Lastly, monitor nodes find the leader and send the chunks to the leader. After developing the code for this, the simulator was run for two variations in the network.

5.1.1 Varying Sensor Nodes

In this case, we study the performance of DIRAS with the variation in number of sensors in the network. Here, we have also studied the performance of DIRAS with respect to the standard network architectures:

1. *Centralized model:* There is only one monitor node (server) and the sensor nodes send the whole image to a server. The centralized architecture is inspired from the conventional client-server architecture of network systems.

2. *Decentralized model:* Here, there are multiple monitor nodes and all the monitor nodes reconstruct all the images. This model is inspired from the architecture used in distributed optimization [27]. However, there isn't any optimization running on any node. The decentralization implies that all the monitor nodes reconstruct all the images. In this framework, a sensor node splits an image into chunks and send the chunks to the respective monitor nodes. The monitor nodes, then, broadcast their chunk to all other monitor nodes to ensure that all the monitor nodes reconstruct the image.

The centralized and decentralized models are classical models which form the extreme cases of network systems. On one hand, the centralized model has less overheads but is prone to single point of failure. On the other hand, the decentralized framework has higher overheads but is fault-tolerant. DIRAS falls in the sweet spot of these two extreme cases and aims to provide low overheads and fault-tolerance.

The simulations for this part of implementation have been run with the following parameters: **MN** = 1 for centralized model, and **MN** = 10 for decentralized model and DIRAS; **SN** = n, where n ={10, 15, 25, 40, 50, 75, 100, 125, 150, 175, 200, 225, 250, 300 }; $dimension(I_i) = 100 \times 100 \times 3$; and number of images generated by each sensor = 5.

5.1.2 Varying Monitor Nodes

Here, we study the effect of increasing the number of monitor nodes in DIRAS. The simulations for this part of implementation have been run with the following parameters: **MN** = n; where n ={10, 20, 30, 40, 50, 60, 70, 80, 90, 100 }; **SN** = 100; $dimension(I_i) = 100 \times 100 \times 3$; and number of images generated by each sensor = 5.

We have studied the packet overhead and network delay induced in the network because of the increase in monitor nodes. Recall that a sensor chunks an image according to the number of monitor nodes in the network. Thus, the packet overhead and the latency will increase with the increase in monitor which isn't appropriate for a CPS. However, it should be noted that an increase in chunks implies a decrease in

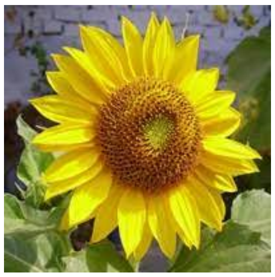
Figure 5.1: Image used for analysis

the information carried by a chunk. Thus, the privacy of data is improved, i.e, if an adversary is able to intercept a chunk, then the adversary would be able to acquire less information when the number of monitor nodes is high. Thus, there is a trade-off between privacy and overheads. Due to this reason, we have also studied quality of privacy provided by DIRAS and quantified it.

It should be noted that there is no step in this implementation where the image of a sensor is polluted. Therefore, in this part of the implementation, we do not intend to study the image reconstruction. Rather we wish to obtain the performance of the network in terms of a communication framework because the implementation described here exactly emulates the packet transfer mechanism as described in the system design. Therefore, this part of the implementation furnishes us with the study of the overheads and delays in the network due to the communication and processing except the reconstruction part.

5.2 The Image Reconstruction Framework

Since DIRAS aims at reconstructing images, it is necessary to study the efficiency of DIRAS in regards to the ability to generate accurate images. In this implementation, we have studied this parameter of performance.

5.2.1 RPCA

In the first part of this implementation, we consider only false data injection attack, and there is no packet drop attack. This implementation has been done in *python-3.8.8* using the *NumPy* module. We have used the image depicted in figure 5.1 (which is a $200 \times 200 \times 3$ matrix), and then, introduce random sparse noise into it. The image with the induced noise is the image that is obtained after the leader obtains all the chunks from all other monitors. The false data injected is a matrix with random entries. The entries of the noise matrix had a maximum value set for its entries. We increased the maximum value of this error and evaluated the performance of the image reconstruction algorithm. Thus, we have emulated the scenario where an adversary adds random noise to any chunk. After obtaining the noisy image, we apply RPCA to it to reduce the sparse noise. This gives us an idea of the degree of noise our reconstruction method can handle. In this study, we have analyzed the performance of RPCA with respect to various image processing denoising algorithms which include: (i) mean blur; (ii) median blur; (iii) Gaussian blur; (iv) bilateral Filter [6]; and (v) Wiener filter[10]. We have studied the performance of the algorithms using the following formula: $Dist = E(M_{reconstructed} - M_{actual})$, where $E(M)$ is the Euclidean norm of matrix M, $M_{reconstructed}$ is the reconstructed matrix after applying the denoising algorithm, and M_{actual} is the actual matrix (the matrix obtained from the figure 5.1). We calculated this for R, G and B components of the image ($Dist_R$, $Dist_G$ and $Dist_B$). Finally, the distance between the actual and reconstructed image is:

$$Distance = \sqrt{\frac{Dist_R^2 + Dist_G^2 + Dist_B^2}{3}}$$

5.2.2 RPCA and Matrix Completion

Next, we study the performance of our algorithm in the case where an adversary drops an packet, i.e., the leader does not receive all the packets of a particular image, and noise is also added to the image.. In this case, the leader tries to regenerate the image by using matrix completion algorithm. This part of the implementation has also been done in *python-3.8.8* using the *NumPy* and *cvxpy* modules. To start with this implementation, we used the image in figure 5.1. Next, we add some random noise to the image. This random noise is same as the one described above. Then, we randomly remove some rows of the image. Note that by doing this, we have emulated the exact attack scenario - where an adversary is in the middle of a monitor and a sensor or in the middle of two monitors, and the attacker simply acts as a sink by not allowing the packet to pass to the receiving monitor. If the leader does not receive all the packets corresponding to an image in δ, the leader assumes that the packet has been dropped. First of all, the leader makes all the elements equal to zero for the rows it hasn't received. Then, it applies RPCA to remove the noise from the image. In the final step, the leader applies matrix completion algorithm to obtain the rows of the image that it hasn't received. This implementation helps us to study the efficiency of our image reconstruction algorithm in case of the combined attack of addition of false data injection and dropping of packets.

5.3 Load Balancing Analysis

Here, we study the performance of the load balancing analysis proposed here. Here, we study the improvement in the leader selection algorithm. Firstly, the normal leader selection algorithm (without the load balancing) was implemented for 10 monitor nodes and 1000 images, i.e., we studied which node is decided as the leader based on the leader selection algorithm for each image. Then, we calculated how many times each monitor node acts as the leader. Next, we implement the leader selection algorithm using the load balancing and evaluate the number of times each node has to act as the leader. This implementation was also done in *python-3.8.8* and gives an understanding of the improvement provided by the load balancing algorithm.

5.4 Privacy Analysis

Here, we have analyzed the privacy provided by DIRAS. DIRAS deploys splitting of images into chunks, which ensures that an attacker cannot acquire a substantial amount of information if the attacker is able to read packets of a communication channel. Therefore, here, we study the variation of amount of information obtained by an adversary with the number of rows of the matrix intercepted. We vary the number of rows of the matrix obtained by the attacker and make the other rows of the matrix equal to zero. Then, we apply matrix completion to obtain the whole matrix from the intercepted rows. From here, we get an understanding of the amount of information revealed by chunks of image. This amount of information revealed is obtained using the Euclidean norm of the matrix obtained by the difference of the actual matrix and the matrix obtained after matrix completion.

These implementations help to study the scalability and ability of DIRAS to reconstruct images in case of adversarial activities. The implications obtained from the implementations have been discussed in the next section.

Chapter 6

Evaluation

In this section, we explain the results that we have obtained from the implementation.

6.1 Communication Network

Here, we describe the performance of network component of DIRAS.

6.1.1 Varying sensor nodes

Here, we vary the number of sensor nodes keeping the number of monitor nodes constant (refer to 5.1.1).

Figure 6.1 depicts the packet overhead in centralized model, DIRAS and decentralized model. Packet overhead depicts the bandwidth consumed by the whole network. As the graph suggests, the packet overhead in the case of decentralized model is very high with respect to the other two, which makes it unsuitable for deployment. Centralized model has the least packet overhead because it doesn't involve any inter-monitor communication (as there is only one monitor node). DIRAS has a packet overhead which is not much higher than the the centralized model.

Figure 6.2 depicts the delay in centralized model, DIRAS and decentralized model. Delay depicts the delay in transmission of packets in the network. The x-axis depicts the number of sensor nodes deployed and the y-axis is the delay in the network. As the graph suggests, the delay in the case of decentralized model is much higher than the other two, which makes it unsuitable for deployment in CPS. Centralized model has the least network delay because it involves only transmission of packets from sensors to a single server. DIRAS has a network delay which is not much higher than the the centralized model.

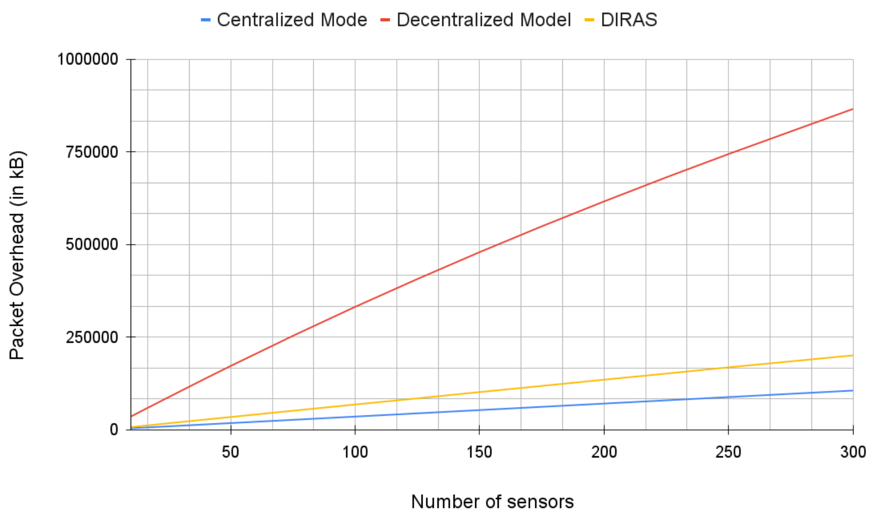

Figure 6.1: Variation in packet overhead with change in number of sensor nodes and comparison with centralized and decentralized models

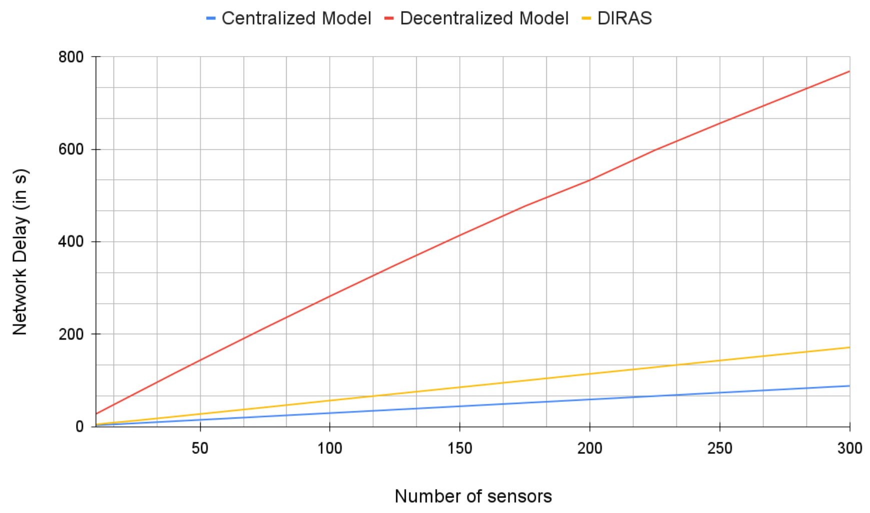

Figure 6.2: Variation in delay with change in number of sensor nodes and comparison with centralized and decentralized models

As the figures 6.1 and 6.2 suggest, DIRAS falls in between the centralized and decentralized models in terms of the performance of the network system.

6.1.2 Varying monitor nodes

Here, we vary the number of monitor nodes keeping the number of sensor nodes constant (refer to 5.1.2).

Figure 6.3 and figure 6.4 depict the packet overhead and network delay in DIRAS with the increase in number of monitor nodes. With the increase in number of monitor nodes, the overhead and delay will also increase and the major increase in the overheads and the delay will be due to the monitor position assignment because the total number of images generated in the network is constant. Thus, as expected, the graphs depict that the overhead and delay increase with increase in the monitor nodes. However, it should be noted that when the number of monitor nodes becomes ten-fold, the packet overhead and the network delay doesn't increase that greatly which is depicted by the lower slopes of the lines. Thus, increasing the number of monitor nodes doesn't greatly affect the performance of the network component. On the other hand, the increase in monitor nodes is beneficial for the network in terms of privacy (this has been discussed later).

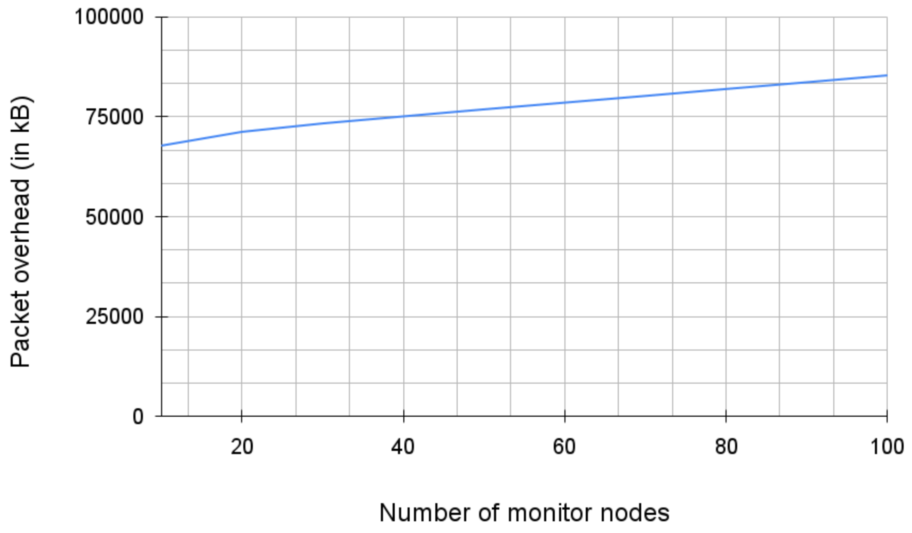

Figure 6.3: Variation in packet overhead with change in number of monitor nodes

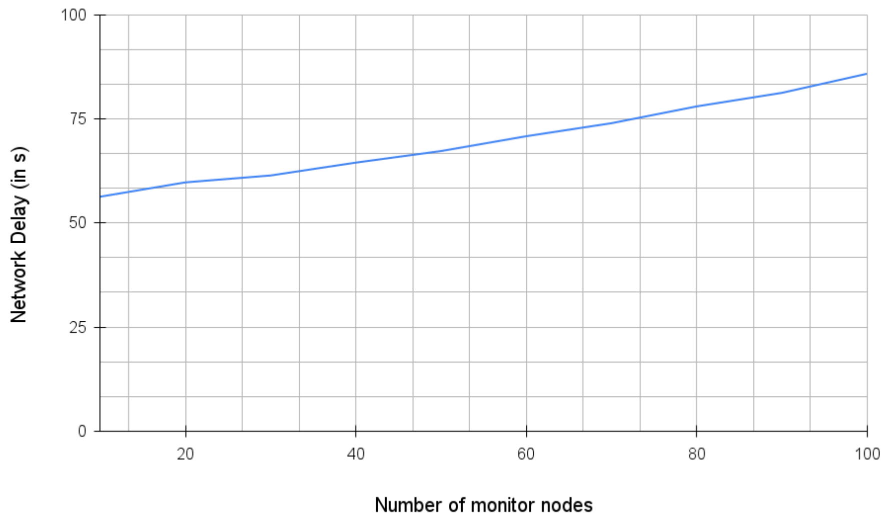

Figure 6.4: Variation in delay with change in number of monitor nodes

6.2 Image Reconstruction Framework

6.2.1 RPCA

Here, we study the performance of the image reconstruction component.

Figure 6.5 depicts the actual image, image with the noise and the image reconstructed from the noisy image after applying RPCA. As the figure depicts, RPCA removes the noise to a great extent. However, there is a certain degree of blurring in the reconstructed image. Therefore, RPCA does not preserve all the features of the image. One reason for this inefficiency is the image that has been used not being a low-rank matrix.

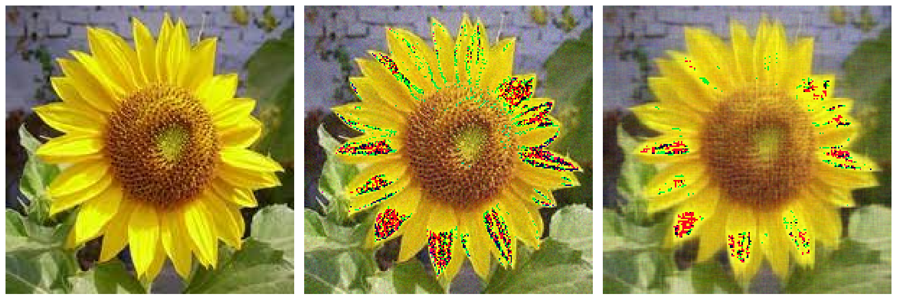

Figure 6.5: (a) Actual Image (b) Image with noise (c) Reconstructed image

Figure 6.6 depicts the performance of RPCA with the increase in magnitude of the noise being added to the image. We have also compared the performance of RPCA with other standard filters. The Euclidean distance between the actual image and the reconstructed image reduces as the error is increased. Thus, all the filters perform better as the magnitude of error increases and RPCA performs better than all of them. However, the reconstructed image obtained from all the filters vary greatly from the actual image.

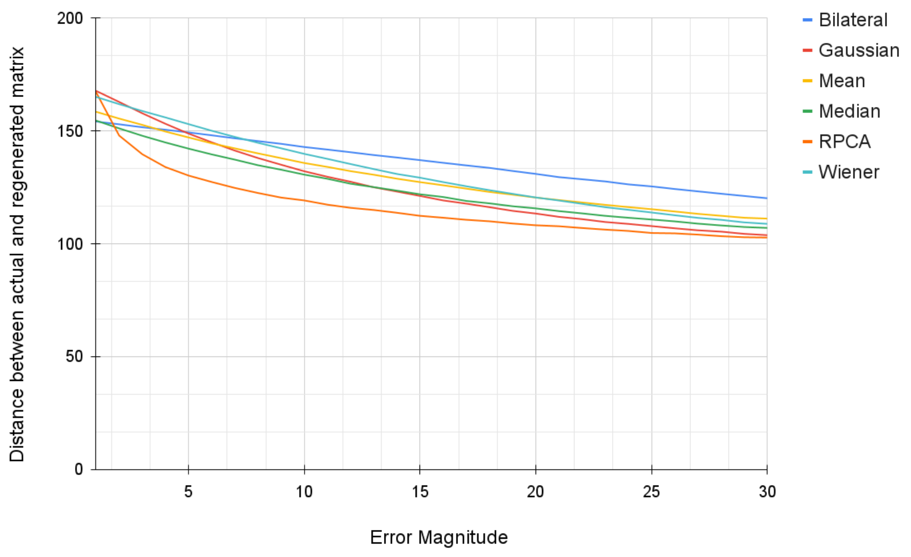

Figure 6.6: Performance of DIRAS in case of false data injection and its comparison with other filters

6.2.2 RPCA and matrix completion

Figure 6.7 depicts the performance of DIRAS in case of packet drop and false data injection. As expected, the Euclidean distance of the reconstructed image and the reconstructed image increases with the increase in number of packets dropped. As the graph suggests, there is a small saturation in the Euclidean distance after 85 rows of the matrix have been dropped.

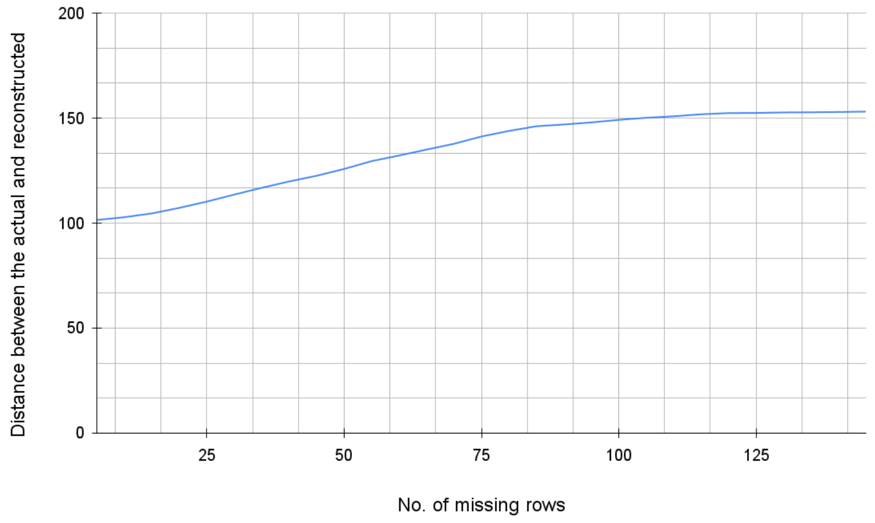

Figure 6.7: Performance of DIRAS in case of packet dropping and false data injection

6.3 Load Balancing Analysis

Figure 6.8 depicts the improvement provided by load balancing. Without the load balancing, some monitors have less computation burden while the others have more. On the other hand, the load balancing algorithm ensures that each of monitor has equal computation burden in terms of reconstructing a whole image.

6.4 Privacy Analysis

Figure 6.9 depicts the amount of information revealed with the number of packets intercepted. It is evident that the Euclidean distance between the actual reconstructed matrix from matrix completion and the actual matrix is quite large when the number of rows intercepted is very small. An adversary does not have a great deal of information until he has intercepted around 500 rows. Thus, DIRAS is resistant to privacy leakage as an attacker would have to get control over numerous channels to get substantial information about the image.

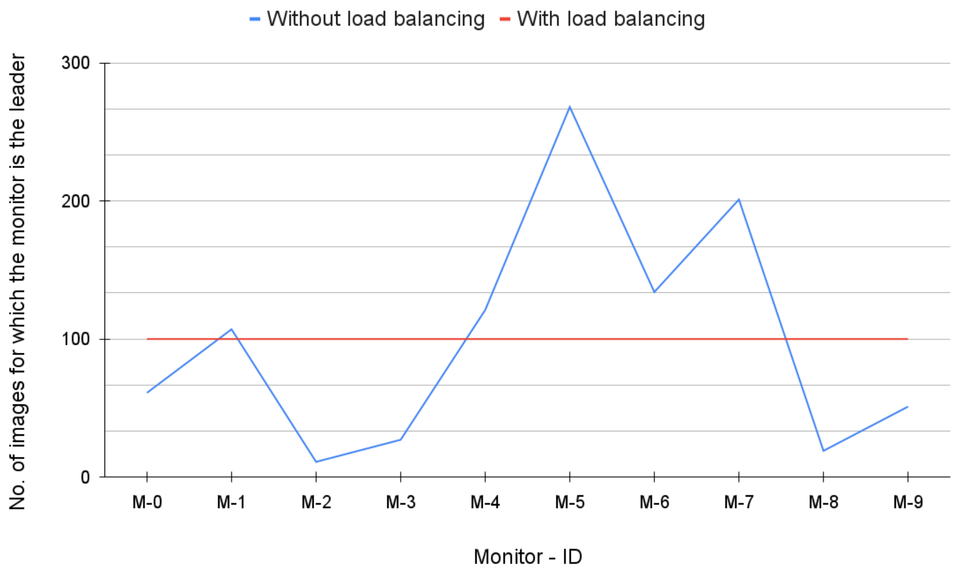

Figure 6.8: Improvement in performance because of load balancing based on the number of images for which each monitor node has been chosen as the leader

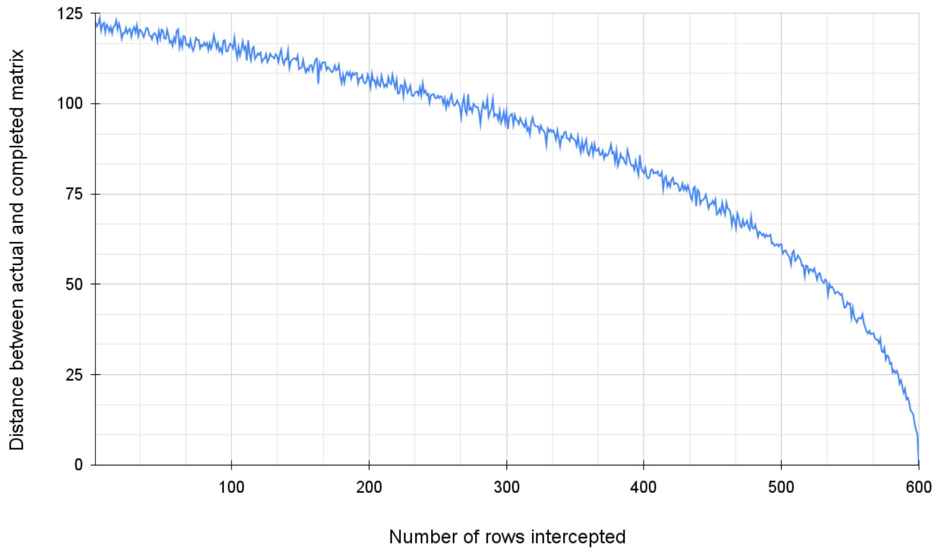

Figure 6.9: Privacy provided by DIRAS based on distance between the actual matrix and the matrix reconstructed after applying matrix completion

Chapter 7

Discussion

In this section, we discuss the various implications provided by the results in Section 6. We have classified this discussion into scalability, privacy and security of DIRAS.

7.1 Scalability Analysis

As results suggest, the overhead and network delay in DIRAS is comparable with the centralized model. Considering the benefits provided by DIRAS in terms of privacy and security, DIRAS can prove to be a better choice over a centralized architecture.

In addition, splitting of data helps in enhancing the scalability of the framework. This is because a sensor node does not have to transfer its entire image, which is generally a large matrix. Such transfer of large matrices would not only bloat the connections of the sensor node but also they will make the communications between monitor nodes slower.

7.2 Privacy Analysis

Splitting of messages has helped us in increasing the privacy of the data. Figure 6.9 suggests that an attacker needs to acquire a large number of rows to gain enough information of an image. The Euclidean norm of the matrix obtained from the difference between the reconstructed and actual matrices is around 90 for 400 rows intercepted. This is difficult for an adversary to achieve. For example, consider a scenario each chunk sent by the sensor has 5 rows. Then, the adversary would need to intercept packets from 80 communication channels, which is very difficult computationally.

Another point that should be noted is the trade-off between bandwidth and privacy. Figure 6.3 and figure 6.4 depict that the bandwidth consumed and delay increase with the increase in the number of monitor nodes. However, with the increase in number of monitor nodes, the size of chunks reduces and thus, the information revealed by each chunk reduces. Thus, the network designer needs to decide the decide the number of monitor nodes based on the requirement of privacy.

Moreover, we have assumed that the adversary uses the same technique used by us for matrix completion. The attacker may use a better matrix completion algorithm for acquiring the entire image.

7.3 Security Analysis

Here, we discuss the various attacks DIRAS defends against and how.

7.3.1 False Data Injection Attack

In this case, the adversary is in between two nodes and tampers with the data within the packet. Note that the adversary can be between a sensor node and a monitor node or two monitor nodes. The adversary changes the data such that the image reconstructed deviates greatly which leads further wrong analysis. We have mitigated the effects of this attack by deploying RPCA that separates the sparse noise from the low-rank matrix. However, as the results depict, the reconstructed matrix has a great deal of blurring and thus, the reconstructed image varies greatly from the actual image. Thus, we may need to improve the algorithm or look for new methods for the same.

7.3.2 Packet Drop Attack

In case of this attack, the attacker is between any two nodes and does not allow packets to pass from source node to destination. We call this the *Packet Drop Attack*. In the case of this attack, the whole image cannot be reconstructed which is really detrimental to the functioning of the systems. DIRAS reduces the effect of this attack by deploying matrix completion algorithm which helps greatly.

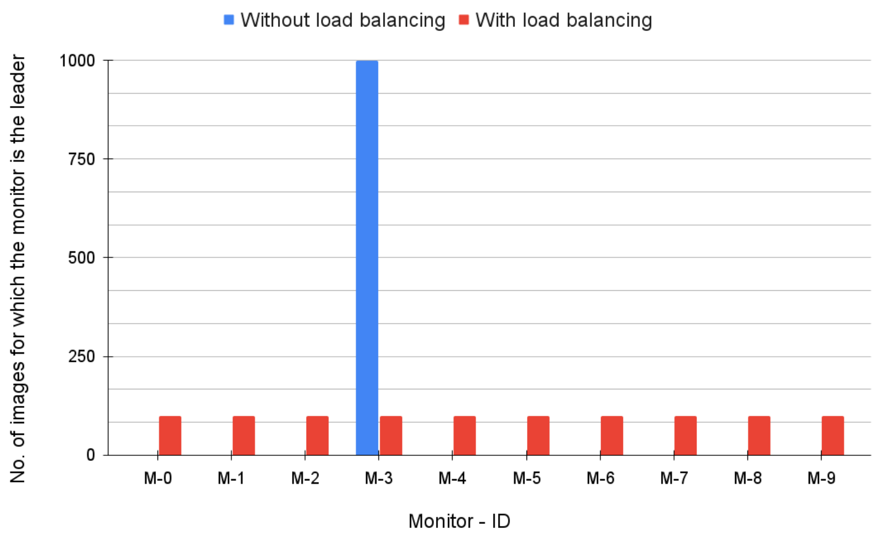

Figure 7.1: Mitigation of effect of DoS attacks by load balancing

7.3.3 Denial of Service (DoS) Attack

This attack is targeted at any particular monitor node. An adversary takes control of a sensor node and generates coordinates which are always close to (x_j, y_j). The $j - th$ monitor node will be selected as the leader each time. Therefore, the $j - th$ monitor node will be sent numerous packets in a very short interval of time and will be blocked from all other communications and functioning. Note that the adversary does not need to know the exact coordinates of a monitor. It can simply keep on generating coordinates which are close to (x_j, y_j). To reduce the effect of this attack, the monitor nodes generate random coordinates for every Δ. This reduces the chances of this attack greatly. However, the attacker may generate images at an extremely quick rate in a given epoch time. To solve this issue, we have proposed load balancing for selecting the leader each image. Figure 7.1 depicts how load balancing helps in countering DoS attack. The attacker sensor generates coordinates very close to monitor with ID $M - 3$. Without load balancing, $M - 3$ has to regenerate all the images. By integrating load balancing, the image reconstruction task is distributed evenly in the network and none of the nodes get blocked.

DIRAS is a distributed, scalable, and improves privacy and security. However, there are improvements that need to be made to DIRAS to enhance its performance. These improvements have been discussed in the next section.

Chapter 8

Future Work

In this section, the work that needs to be done for DIRAS, to make it more robust and pluggable with existing systems has been described. Any or some of these goals can be picked for the upcoming semester:

1. The image quality obtained from RPCA as well as RPCA along with matrix completion is far from the actual image. Thus, one of the research directions could be to design a better algorithm for reconstructing better final images.

2. We have assumed that the monitor nodes are trusted. However, monitors node may act maliciously and this can lead to numerous attacks in the framework. Therefore, the system needs to be designed in such a way that it can reconstruct image even when there's no trust between any two monitor nodes.

3. We have considered a p2p network for the monitor nodes connection where all the monitor nodes are connected. However, all the devices would not be connected with each other due to the geographical distance between them and economic reasons. Devising the protocols for sharing of data and reaching consensus among nodes in such a case could be another research avenue.

4. Another prevalent attack in CPSs which needs to be addressed is the sybil attack [11] where an adversary impersonates another node in the network.

5. There maybe ways to improve privacy of the image data even more. For example, we can use the concept of differential privacy [13] to induce known noise into the chunks of the image.

Chapter 9

Conclusion

The report presents a novel solution for robust distributed image reconstruction, DIRAS. DIRAS integrates various features of security and distributed algorithms to provide an optimal solution. It uses data splitting for improving privacy and reducing the overhead. RPCA and matrix completion algorithms have been used to make the reconstruction process robust. However, the performance of the image reconstruction is not up to the level that the image can be used for analysis. Therefore, in the future, we need devise algorithms such that the image reconstructed has less noise without losing important features of the image. The results presented in Section 6 show the scalability of DIRAS and its ability to reconstruct images. The discussion provided in Section 7 gives a comprehensive view on the implications obtained from the results and the privacy and security analysis of DIRAS. DIRAS takes into account the features of image reconstruction and security of network and data, which makes it a versatile framework for CPS. If the design choices mentioned in Section 8 can be implemented in the future, then the system will be more robust and can emulate the real world scenario more accurately.

Bibliography

[1] A. Al-Kaff, D. Martin, F. Garcia, A. de la Escalera, and J. M. Armingol. Survey of computer vision algorithms and applications for unmanned aerial vehicles. *Expert Systems with Applications*, 92:447–463, 2018.

[2] B. Anderson, S. Mou, A. S. Morse, and U. Helmke. Decentralized gradient algorithm for solution of a linear equation. *arXiv preprint arXiv:1509.04538*, 2015.

[3] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[4] R. Baheti and H. Gill. Cyber-physical systems. *The impact of control technology*, 12(1):161–166, 2011.

[5] C. Belthangady and L. A. Royer. Applications, promises, and pitfalls of deep learning for fluorescence image reconstruction. *Nature methods*, 16(12):1215–1225, 2019.

[6] A. Buades, B. Coll, and J.-M. Morel. A review of image denoising algorithms, with a new one. *Multiscale modeling & simulation*, 4(2):490–530, 2005.

[7] E. J. Candès, X. Li, Y. Ma, and J. Wright. Robust principal component analysis? *Journal of the ACM (JACM)*, 58(3):1–37, 2011.

[8] E. J. Candes and Y. Plan. Matrix completion with noise. *Proceedings of the IEEE*, 98(6):925–936, 2010.

[9] C.-h. Chen. *Signal and image processing for remote sensing.* CRC press, 2012.

[10] J. Chen, J. Benesty, Y. Huang, and S. Doclo. New insights into the noise reduction wiener filter. *IEEE Transactions on audio, speech, and language processing*, 14(4):1218–1234, 2006.

[11] J. R. Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.

[12] G. Dougherty. *Digital image processing for medical applications.* Cambridge University Press, 2009.

[13] C. Dwork. Differential privacy: A survey of results. In *International conference on theory and applications of models of computation*, pages 1–19. Springer, 2008.

[14] G. Fiore, E. De Santis, and M. D. Di Benedetto. Secure mode distinguishability for switching systems subject to sparse attacks. *IFAC-PapersOnLine*, 50(1):9361–9366, 2017.

[15] M. A. Fischler and R. C. Bolles. A paradigm for model fitting with applications to image analysis and automated cartography (reprinted in readings in computer vision, ed. ma fischler,". *Comm. ACM*, 24(6):381–395, 1981.

[16] R. Gnanadesikan and J. R. Kettenring. Robust estimates, residuals, and outlier detection with multiresponse data. *Biometrics*, pages 81–124, 1972.

[17] Z. Guo, D. Shi, K. H. Johansson, and L. Shi. Optimal linear cyber-attack on remote state estimation. *IEEE Transactions on Control of Network Systems*, 4(1):4–13, 2016.

[18] H. Jaidka, N. Sharma, and R. Singh. Evolution of iot to iiot: Applications & challenges. In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.

[19] C. Kanellakis and G. Nikolakopoulos. Survey on computer vision for uavs: Current developments and trends. *Journal of Intelligent & Robotic Systems*, 87(1):141–168, 2017.

[20] Q. Ke and T. Kanade. Robust l/sub 1/norm factorization in the presence of outliers and missing data by alternative convex programming. In *2005 IEEE*

Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), volume 1, pages 739–746. IEEE, 2005.

[21] R. H. Keshavan, A. Montanari, and S. Oh. Matrix completion from a few entries. *IEEE transactions on information theory*, 56(6):2980–2998, 2010.

[22] P. R. G. Kurka and A. A. D. Salazar. Applications of image processing in robotics and instrumentation. *Mechanical Systems and Signal Processing*, 124:142–169, 2019.

[23] L. Lamport et al. Paxos made simple. *ACM Sigact News*, 32(4):18–25, 2001.

[24] L. Liang, K. Zheng, Q. Sheng, and X. Huang. A denial of service attack method for an iot system. In *2016 8th international conference on Information Technology in Medicine and Education (ITME)*, pages 360–364. IEEE, 2016.

[25] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *49th IEEE Conference on Decision and Control (CDC)*, pages 5967–5972. IEEE, 2010.

[26] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[27] A. Nedić and J. Liu. Distributed optimization for control. *Annual Review of Control, Robotics, and Autonomous Systems*, 1:77–103, 2018.

[28] H. Nguyen-An, T. Silverston, T. Yamazaki, and T. Miyoshi. Generating iot traffic in smart home environment. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–2. IEEE, 2020.

[29] F. Pasqualetti, F. Dorfler, and F. Bullo. Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine*, 35(1):110–127, 2015.

[30] B. Recht. A simpler approach to matrix completion. *Journal of Machine Learning Research*, 12(12), 2011.

[31] G. Rong-xiao, T. Ji-wei, W. Bu-hong, and S. Fu-te. Cyber-physical attack threats analysis for uavs from cps perspective. In *2020 International Conference on Computer Engineering and Application (ICCEA)*, pages 259–263. IEEE, 2020.

[32] Y. Shoukry and P. Tabuada. Event-triggered state observers for sparse sensor noise/attacks. *IEEE Transactions on Automatic Control*, 61(8):2079–2091, 2015.

[33] J. Thevenot, M. B. López, and A. Hadid. A survey on computer vision for assistive medical diagnosis from faces. *IEEE journal of biomedical and health informatics*, 22(5):1497–1511, 2017.

[34] A. Vibhute and S. K. Bodhe. Applications of image processing in agriculture: a survey. *International Journal of Computer Applications*, 52(2), 2012.

[35] G. Wang, J. C. Ye, and B. De Man. Deep learning for tomographic image reconstruction. *Nature Machine Intelligence*, 2(12):737–748, 2020.

[36] G. Wang, J. C. Ye, K. Mueller, and J. A. Fessler. Image reconstruction is a new frontier of machine learning. *IEEE transactions on medical imaging*, 37(6):1289–1296, 2018.

[37] W. Wei, B. Zhou, D. Połap, and M. Woźniak. A regional adaptive variational pde model for computed tomography image reconstruction. *Pattern Recognition*, 92:64–81, 2019.

[38] J. Wright, A. Ganesh, S. R. Rao, Y. Peng, and Y. Ma. Robust principal component analysis: Exact recovery of corrupted low-rank matrices via convex optimization. In *NIPS*, volume 58, pages 289–298, 2009.

[39] T. Yang, X. Yi, J. Wu, Y. Yuan, D. Wu, Z. Meng, Y. Hong, H. Wang, Z. Lin, and K. H. Johansson. A survey of distributed optimization. *Annual Reviews in Control*, 47:278–305, 2019.