Aerial imagery pile burn detection using deep learning: The FLAME dataset

Nithya Praba C[1], Kalaivani D[2]

[1]*Student, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, India.*

[2]*Associate Professor, Department of Computer Technology, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore, India.*

Corresponding Author: nithistar17@gmail.com

Abstract: Wildfires are one of the costliest and deadliest natural disasters in the US, causing damage to millions of hectares of forest resources and threatening the lives of people and animals. Of particular importance are risks to firefighters and operational forces, which highlights the need for leveraging technology to minimize danger to people and property. FLAME (Fire Luminosity Airborne-based Machine learning Evaluation) offers a dataset of aerial images of fires along with methods for fire detection and segmentation which can help firefighters and researchers to develop optimal fire management strategies. This paper provides a fire image dataset collected by drones during a prescribed burning piled detritus in an Arizona pine forest. The dataset includes video recordings and thermal heatmaps captured by infrared cameras. The captured videos and images are annotated, and labeled frame-wise to help researchers easily apply their fire detection and modeling algorithms. The paper also highlights solutions to two machine learning problems.

Key Words: —W*ild fires, fire detection, firefighters, leveraging techniques.*

I. INTRODUCTION

Wildfires have caused severe damage to forests, wildlife habitats, farms, residential areas, and ecosystems during the past few years. Based on the reports from National Interagency Fire Center (NIFC) in the USA, total number of 51,296 fires burned more than 6,359,641 acres of lands yearly on average from 2010 to 2019 accounting for more than $6 billion in damages [1], [2]. These alarming facts motivate researchers to seek novel solutions for early fire detection and management. In particular, recent advances in aerial monitoring systems can provide first responders and operational forces with more accurate data on fire behavior for enhanced fire management. Traditional approaches to detecting and monitoring fires include stationing personnel in lookout towers or using helicopters or fixed-wing aircraft to surveil fires with visual and infrared imaging.

Manuscript revised June 28, 2022; accepted June 29, 2022. Date of publication June 30, 2022.

This paper available online at www.ijprse.com

ISSN (Online): 2582-7898; SJIF: 5.59

Recent research has suggested Internet of Things (IoT) innovations based on wireless sensor networks but such networks would require further investment and testing before providing practical information. At broader scales, satellite imagery is widely used for assessing fires globally, but typically at relatively coarse resolution and with the availability of repeat images constrained by satellite orbital patterns.

Considering the challenges and issues of these methods, using Unmanned Aerial Vehicles (UAVs) for fire monitoring is gaining more traction in recent years.

UAVs offer new features and convenience including fast deployment, high maneuverability, wider and adjustable viewpoints, and less human intervention. Recent studies investigated the use of UAVs in disaster relief scenarios and operations such as wildfires and floods, particularly as a temporary solution when terrestrial networks fail due to damaged infrastructures, communication problems, or spectrum scarcity.

II. PROPOSED METHODOLOGY

There are a huge number of routing protocols present for sensor networks. First time these routing protocols were presented in an organized way by Al-Karaki and Kamal[1],

this survey covered almost all aspect of routing protocol, classification and architecture. But all these basic protocols have been implemented without the security. Karlof et.al.[7] describe the attacks on different routing protocols and provide the countermeasures, which is the base of the many research.

All these attacks come under active attack. The attacker is also classified as laptop class attacker - mote class attacker and insider attacker - outsider attacker [7]. Most of the outsider attacker can be prevented by link layer security using a *global shared key*, but in the presence of insider attacker or compromised nodes it is ineffective [7]. works. SPINS[13] provides the two generalized mechanism;

SNEP for confidentiality, authenticity, integrity and freshness of data and second μTESLA for authenticated broadcasting, but with the extra over head of buffering messages prior to key disclosure that increase the latency and generating own key chain for every single communication.

LEACH[4] is the first and very popular concept of clustered routing without any security. SecLEACH[11] provides an efficient solution for secure communication in LEACH with the help of *random key pre-distribution* and μTESLA and overcomes some of the attacks. Again, to provide effective solution for secure communication in LEACH, RLEACH[18] has been introduced with improved random key pre-distribution scheme. Some work has been done in secure hierarchical routing protocol; Tubaishat et.al.[16] have described energy efficient hierarchical routing protocol with group key management scheme, but when changing the cluster head all group keys (i.e., inter cluster and intra cluster) have to calculate again, is an overhead associated with this protocol. NHRPA[5] is also an approach towards secure hierarchical routing which provide security under node compromise attack. Quan et.al.[14] offer security against exterior adversary and inner compromised nodes by gene and reputation management tools with extra burden of computation and communication.

All the hierarchical routing protocol has been implemented with the efficiency in mind. If once, we leave the issue of security, there are some other issues exist in clustering protocol like; orphan nodes problem and multihop path (from the cluster head to the base station). In this paper we overwhelmed these two problems.

There are many multipath routing protocols [6], [3] exist, which increase resilience and reliability at the expense of increased energy consumption, traffic generation and overhead of maintaining the alternative paths. In this paper, we overcome these problems with security as a main issue.

Some secure multipath routing protocols have also introduced like; Wenjing Lou[9] has proposed a protocol which is capable of finding multiple node-disjoint paths from the each source node to the common sink(i.e. base station). Parno et al. [12] have implemented a protocol to ensure node-to-node message delivery, even if the sensor network is under active attack. INSENS[2] and SEEM[10] both sent the neighbor information to the base station for computing multipath from source to sink, but in INSENS, BS unicasts the multipath table to each associated nodes and SEEM works as a data centric protocol, which floods the query to the network and the node which satisfies the query will send a request for the routing path to the base station. SEEM justifies the security without using any cryptographic mechanism, unlike INSENS uses cryptography for preventing many attacks.

In this paper, we also use the same mechanism, used in INSENS and SEEM but added the concept of clustering.

III. Sensor Network System Assumption

In the wireless sensor network system lifetime, we follow these assumptions.

3.1 The sensor nodes are randomly

deployed in the network. (2) It is the homogeneous system model where all nodes have similar storage, communication and computation capabilities. (3) BS is secured and possesses a high memory, computation and battery power. (4) Every node has a unique ID, a certificate signed by authority (i.e. base station) and a shared key with the base station. (5) All sensor nodes are static in nature. (6) All sensor nodes are symmetrical, that is same frequency has been used to communicate with each other. (7) Every node has the same energy source that is non-chargeable battery. The sensor node dies as its battery exhausts. (8) In the cluster, there should be only one-hop communication between nodes and cluster head. (9) It is not necessary that the distance between cluster heads and the base station is one-hop. (10) Every sensor node's communication range should be constant and predefined.

IV. Fire segmentation

This section considers the problem of image segmentation for frames labeled as "fire" by the fire classification algorithm presented in Section. Studying the fire segmentation problem is useful for scenarios like detecting small fires. Also, fire segmentation helps fire managers localize different discrete

places of active burning for the purpose of fire monitoring. The goal is to propose an algorithm to find the pile burn segments in each frame and generate relevant masks. These segmentation problems were handled differently in the past using image processing and RGB threshold values to segment different data batches which exhibits relatively high error rates. The goal is to develop an image semantic segmentation to perform a pixel-wise classification for each frame at the pixel level to define a fire mask for the generated output. To accomplish this task, a DCNN model is implemented to predict the label of each pixel based on the imported data. This segmentation problem can be recast as a binary pixel-wise classification problem, where each pixel can take two labels: "fire" and "non-fire" (background). To accomplish the image segmentation task, the fire test dataset from Section is considered as a training dataset. To train a DCNN model, a Ground Truth Mask dataset is required. Different tools and applications such as Labelbox , Django Labeller , LabelImg, MATLAB Image Labeler , GNU Image Manipulation Program (GIMP) , etc are available to perform different types of the manual image segmentation such as pixel labeling, annotation (rectangles, lines, and cuboid) on the Regions Of Interest (ROI) to provide training data for the utilized deep learning model. The MATLAB (TM) Image Labeler is used on 2003 frames to generate the Ground Truth Masks. This subcategory of the FLAME dataset of masks and images is presented in. The implemented image segmentation model is adopted from the U-Net convolutional network developed for biomedical image segmentation. U-Net is an end-to-end technique between the raw images and the segmented masks. A few changes are made to this network to accommodate the FLAME dataset and adapt it to the nature of this problem. The ReLU activation function is changed to Exponential Linear Unit (ELU) of each two-dimensional convolutional layer to obtain more accurate results. The ELU function has a negative outcome smaller than a constant α for the negative input values and it exhibits a smoother behavior than the ReLU function. The structure of the customized U-Net is shown in. The backbone of the U-Net consists of a sequence of up-convolutions and concatenation with high-resolution features from the contracting path.

The size of the input layer is 512 × 512 × 3 designed to match the size of the input's images and three RGB channels. For computational convenience, the RGB values (between 0 and 255) are scaled down by 255 to yield float values between 0 and 1.

Next, it follows the first contracting block including a two-dimensional fully convolutional layers with the ELU activation function, a dropout layer, another same fully convolutional layer, and a two-dimensional max pooling layer. This structure is repeated another three times to shape the left side of the U shape. Next, there are two two-dimensional fully connected layers with a dropout layer in between, the same structure of the left side is repeated for the right side of the U shape to have a symmetric structure for the up-convolution path in each block. Also, there exists a concatenation between the current block and the peer block from the contracting path. Since the pixel-wise segmentation is a binary classification problem, the last layer has the Sigmoid activation function.

The DCNN utilizes a dropout method to avoid the overfitting issue in the FLAME dataset analysis and realize a more efficient regularization noting the small number of ground truth data samples. The utilized loss function is the binary cross entropy similar to. The Adam optimizer is used to find the optimal value of weights for the neurons. The evaluation of the FLAME-trained model with the ground truth data is described in Section. The implemented code for this section is available on GitHub. The detailed explanation for the repository and the code is available on GitHub. This section uses items 9 and 10 from to access the fire images and their ground truth data masks. The user can change the Mode to "Segmentation" in the config.py file to run the fire segmentation code. The user can change all variables such as batch size, number of epochs, number of classes and channels, and training and test sets ratio in the config.py file

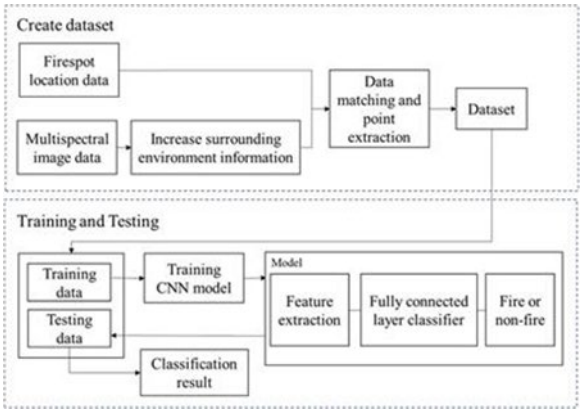

Fig. 1. Pile burn detection using deep learning

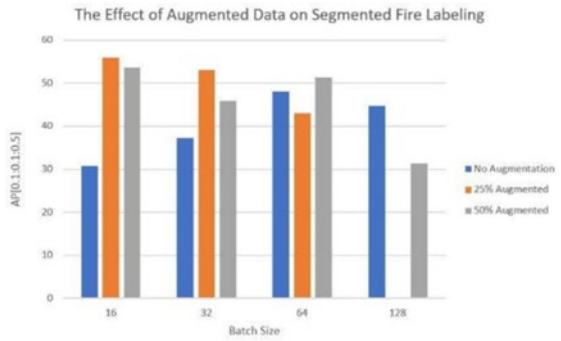

Fig. 2. Graph representation

Any intermediate node who receives the NBR INFO packet will perform following operations: (1) First check the authenticity of the sender node by its certificate. (2) If the sender node *ID* is authenticated, receiver node rebroadcast the packet. (3) If the receiver node again receives the same packet with same *ID*, simply drops the packet. For that every node maintains a table, called *received packet* table.

In this way, it reduces the traffic of the network and save some energy of the node. When the NBR INFO packet reaches to the BS as shown in fig.2, BS will verify the MAC for the integrity and authenticity and encrypts the neighbor information with the *unique shared key* between sender node and the base station. We use MAC which is generated by the data and encrypted by the *unique shared key*, so that no adversary can spoof or manipulate the neighbor information.

V. CONCLUSION

This paper provided the FLAME (Fire Luminosity Airborne-based Machine learning Evaluation) dataset for pile burns in Northern Arizona forest. Two drones were used to collect aerial frames and videos in four different palettes of normal, Fusion, WhiteHot, and GreenHot using normal and thermal cameras. The frames were used in two different applications, in the first challenge, a convolutional neural network was used as a deep learning binary fire classification to label data. In the second approach, a machine learning approach was proposed to extract fire masks from fire labeled data as an image segmentation technique. These exemplary applications show the utility of the FLAME dataset in developing computer tools for fire management and control. Also, FLAME dataset can be used as a benchmark dataset for testing generic image processing algorithms. We provide numerical result for the performance of the proposed two algorithms developed for image classification and detection. We believe that developing more advanced models by the research community can further improve the reported results. Another potential use for this dataset is developing fire classification and detection algorithms by a collective analysis of different imaging modalities including regular and thermal images. Also, researchers can utilize fire segmentation methods to define related networking and monitoring problems, such as optimal task scheduling for a fleet of drones to optimally cover the pile burns in a certain region at shortest time possible.

REFERENCES

[1]. Ahmaed Alkhatib, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Gener.Comput.Syst., Vol.29, no.7, pp.1645-1660, sep.2013.
[2]. kechar Bouabdellah,Houache Noureddine, Sekhri Larbi.” From RFID to the Internet of Things: pervasive networked systems,” vol.30, mar.2006.
[3]. C. Gomathi, B. Shriaarthi, “Research of routing protocol in RFID-based Internet of Things,” vol.1, pp.94-96, Nov.2012.
[4]. Jaime Lkret,Miguel Garcia,” Design aspects of assisted device-to-device communications,” Vol.50,pp. 170-177, Mar, 2012.
[5]. Diwakar chintha, Dr.vishnu vardhan reddy, “Innovative concepts in peer-to-peer and network coding,”vol.47,pp.45-49,Dec.2009.
[6]. E. Elnahrawy and B. Nath. 2003. Cleaning and Querying Noisy Sensors. In Proc. of the 2nd ACM International conference on WSNA’03, pages 78-87.
[7]. Victoria J. Hodge & Jim Austin 2004, a survey of techniques for outlier detection, Artificial Intelligence Review Volume 22, Issue 2, pp 85-126
[8]. Christoph Heinz and Bernhard Seeger. 2006. Statistical Modeling of Sensor Data and its application to Outlier Detection. Technical Report 2006/07, University of Stuttgart; 5. GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze", Stuttgart.