

Research Article

Artificial Intelligence-Based Wireless Sensor Network Model for Intrusion Detection and Firearms Image Detection in the Conflict Zone

Simon Tooswem Apeh^{1,2}, Lukman Adewale Ajao^{2,3*} , Dominic S. Nyitamen¹, Ciroma L. Wamdeo¹, Robinson Edeh¹

¹Department of Electrical & Electronic Engineering, Nigerian Defence Academy, Kaduna, Nigeria

²Department of Computer Engineering, University of Benin, Benin City, Nigeria

³Department of Computer Engineering, Federal University of Technology, Minna, Nigeria

E-mail: ajao.wale@futminna.edu.ng

Received: 21 May 2024; **Revised:** 15 January 2025; **Accepted:** 20 January 2025

Abstract: The convergence of wireless sensor networks (WSN) and artificial intelligence (AI) for gathering security information about terrorism pattern movement in war zones offers significant advantages. It improves the efficiency of sophisticated machinery in combating terrorists, which is more resilient than humans at the front line through autonomous surveillance. However, the detection of terrorist pattern movement and human-conceived weapons using traditional approaches—through the deployment of gallant soldiers and other anti-terrorist personnel to the conflict zone—is more challenging, which usually results in mass casualties, fatalities, and machinery destruction by ambushing. Therefore, this research aims to develop an architecture for intrusion detection of movement patterns and firearm detection models in war zones through the deployment of wireless sensor nodes and autonomous surveillance camera systems. The imagery of human-conceived weapons is collected and experimented on with the YOLOv5 model for object detection and classification using a deep convolutional neural network (DCNN) embedded within the YOLOv5 platform. The average detection accuracy results obtained from the simulation of attacker detection in a spanning tree network-based wireless sensing model are 94.85%, 95.10%, 96.58%, 93.57%, 95.26%, and 97.17%, respectively. Additionally, the detection accuracy for firearm identification is 100%, with a processing time of 0.875 seconds.

Keywords: artificial intelligence, deep convolutional neural network, firearm, surveillance system, wireless sensor network, YOLOv5

1. Introduction

Recently, wireless sensor networks (WSN) emerged as a dynamic way of gathering security information and monitoring terrorist movement patterns in war zones by deploying distributed self-configure resources such as sensor nodes, actuators, robotics, drones, and CCTV cameras for monitoring and surveillance [1, 2]. WSN can be used for environmental data acquisition, communicating information remotely, monitoring danger zones, and suspicious behaviors on the battlefields [3-5]. Some application areas are smart cities, smart homes [6-8], smart agriculture, smart healthcare, and smart factories [9, 10]. Another significant area is the military for tracking opposition, battlefield

surveillance, defensive measures, and field monitoring [11]. Wireless sensor technology plays a significant role in gathering security information about insurgency attacks, surveillance of conflict zones, and monitoring the pattern of terrorist movement remotely [12, 13]. Biochemical explosive detection, emergency rescue assistance, fire explosion, and surveillance trailing are included in the WSN application. This sensor can be arrayed in land, oceans, forests, deserts, or hazardous areas for autonomous and real-time monitoring.

The use of unmanned aerial vehicles (UAV) known as drones has emerged newly which can be engaged to complement the functionality of wireless sensors and beyond in the monitoring, surveillance, and resilience of terrorist attacks in the conflict zone. This UAV is incredibly effective for intelligent information gathering, surveillance, environmental monitoring, and combat of terrorists in the war zone. Other functions of UAVs include aerial photography, infrastructure inspection, wildfire fighting, and tactical reconnaissance operations [14]. For instance, a UAV was used in surveillance which detects normal and abnormal human trespasses on the border. The images captured through the surveillance system are experimented with in MATrix LABoratory (MATLAB) using a quadrotor, Raspberry Pi, and robot operating system (ROS). This method can be used as a front-liner, boundary monitoring, no-man zone areas, and security border surveillance. Although the UAV found its applications in many areas as WSN, it is more sophisticated and dynamic in practical surveillance.

Surveillance refers to the security operation against illegal activity and the detection of potential threats that could be carried out by terrorists, smugglers, and illegal immigrants in a border region [15]. The surveillance system can be purposely deployed to a nation's boundary for adequate protection against the illegal movement of arms, human trafficking, drug pushers, contraband goods, and terrorists [16-18]. This terrorism is one of the most challenging threats to human security, food infrastructures, life and properties, and government organizations at present [19, 20]. It became worried about world economic stability, and national sovereignty, with different radical groups growing across the states and in possession of sophisticated weapons and explosive devices in recent times [21].

The statistical report analysis shows that Asian regions have become the most violent extremist groups of terrorists with over 30,000 foreign radical fighters recruited across over 100 states, and more than 11,098 people died from the terror activities in India [22, 23]. Terrorist acts have also damaged the Indian economy and devastated the impact on the neighboring countries [24]. This impact of terrorism on the Indian economy was discussed using time series data from 1994-2017 for analysis using the auto-regressor distributed lags (ARDL) technique and error correction mechanism [25]. The results breakdown shows that terrorism activities have a high negative effect on economic growth and increase unemployment. Another long-run impact is on foreign direct investment and international trade [26].

However, Nigeria as a nation is facing the global challenge of terrorism, insurgency, kidnappers, and brutal killings of innocent citizens perpetrated by terrorist groups. The terrorist has become a giant with the military and para-military efforts stretched to their limits in combat insurgency. There are currently military engagements across several states in Nigeria with the insurgency in the North-East accounting for a greater demand. The area of military engagement in this zone is so vast that it is practically non-feasible for the whole area to be covered effectively by the combatants at the front lines. Even if that were feasible, the economic variable of maintaining such a large catchment of troops becomes wearing and excruciatingly burdensome. Nigeria has recorded about 22,000 deaths and 8,514 people hostages between 2017-2021 due to terrorist attacks. It has degraded the market value by 2.4% GDP economic cost, with a loss of about 142 bn USD and an 8.3 risk index score on terrorist finance and money laundry [27, 28].

In this work, we proposed a distributed wireless sensing network model for monitoring intrusion patterns in a conflict region and identified human-conceived weapons (Guns). For this purpose, we have implemented a distributed WSN to detect an intruder movement pattern in the conflict zone, and a deep convolutional neural network (DCNN) for human-conceived weapons (gun images) identification. So, this wireless sensor network (WSN) application for surveillance and gathering security information about intrusion patterns in conflict zones renders several advantages. It reduces large personnel fatalities, and loss of lives, minimizing attendant personnel, and maintenance costs. It improves the efficiency of sophisticated machinery and the resilience of humans at the front line through autonomous surveillance. Also, deep convolutional neural network (DCNN) applications have significantly progressed in image processing recognition and object detection modules [5]. Especially, the state-of-the-art real-time object classifier "You Only Look Once" (YOLO) model has been moderately helpful in training, and classifying objects for recognition and detection.

The research gap identified from the literature shows that autonomous combat systems with surveillance, and intrusion detection patterns in the conflict zone have not been considered in the previous works. Also, the detection

accuracy of firearm images or human-conceived guns can be improved. So, this work contributes to the knowledge by:

- i. Develop a distributed wireless sensor network model for the detection of intrusion pattern movement in the conflict zone.
- ii. Develop an intelligent surveillance system for the detection of firearm images in the conflict zone.
- iii. Develop an intelligent deep learning image processing model integrated with YOLOv5 using a deep convolutional neural network (DCNN) for the detection of human-conceived guns in the conflict zone.
- iv. Develop an autonomous combat system architecture for the war zone to repel any action of rebels without the physical appearance of the armed personnel.

Thus, the research sections are prepared as follows. Section 3 presented methods and materials used in the system design, implementation of the multi-wireless sensing module, and the intelligent combat system module. Section 4 presented the experimentation of the distributed wireless sensor network simulated in the spanning tree network and the YOLOv3 model for firearm image detection. Section 5 shows the results and performance evaluation of intrusion detection and image processing. Section 6 presented the conclusion and recommendations for future research.

2. Related works

Recently, terrorist attacks and human intruder trespassing in the region have been a great challenge to the public, religious, ethnic groups, and government organizations. The general way of addressing this terrorist attack is beyond the deployment of military and para-military technocrats only for monitoring and combating the insurgency crisis at the frontline. However, different approaches have been proposed in the literature to tackle terrorism and monitor intruders using surveillance drones, surveillance robots, surveillance cameras, and the deployment of wireless sensor nodes.

A robust symmetry algorithm is developed for early detection of abnormal behavior and terrorist attack prediction at the entrance of public places using a monochromatic stationary video camera that captures the image at the entry and exit and stores it in the database for classification as normal or abnormal [29]. About 20 video clips of different persons were collected for experimentation. The results obtained during the trial are 88.16%, 90.06%, and 89.16% for the detection rate, and the false acceptance rates recorded are 5.30%, 3.65%, and 4.90%.

A multi-phase WSN-based remote monitoring and explosive detection for the earliest warning of terrorist activity in urban areas [30]. The anti-terrorist monitoring system and explosive detection called Wireless sensor network for Remote Monitoring and Detection of Explosives (W-ReMADE) consists of several sensors integrated into a single module for explosive identification and detection. The system utilizes magnetic properties and chemical material for explosive detection. The W-ReMADE system is tested and proven to be efficient, but the accuracy and reliability are challenging.

A wireless sensor network for a military surveillance system is developed, and the block diagram of the system module includes a passive infrared (PIR) motion sensor with a maximum sensitivity of 6 meters and a detection angle of 108 degrees [31]. A Zigbee module was used for the information transmission, and Arduino Mega 2560 was used for the information processing. However, energy-efficient management is a major objective in this study, due to many sensor node deployments for military surveillance. Thus, a randomized sleep assignment technique was implemented for these military surveillance sensor nodes. This randomized technique extends the lifetime of the sensor node coverage by 10.2%.

An intelligent imaging technology to prevent terrorism incidents commonly in the business sector in the 21st century is developed by installing a CCTV camera for environmental surveillance [32]. Computer vision technology and the viola-jones algorithm were used for image capturing and analysis, while the support vector machine (SVM) algorithm was used for image template matching and identification. The proposed techniques achieve a high accuracy of 98% in face recognition and self-identity.

A multi-sensing model for the human intruder and military border surveillance system through WSN technology is experimented with [33]. This system is developed to enhance the military effort in counter-terrorism intruder detection and capturing, compared to the use of patrol systems for the military agent which usually result in line-of-sight restriction and are costly. However, a multi-sensing PANCHENDRIYA system involved a hybrid WSN model using a sensing camera, infrared sensor, geophones, hydrophones, and microphones which are all integrated into a single module for the detection of human intrusion and efficient surveillance with early cautionary capability. Although this

system may be effective for military border surveillance with high accuracy, it has not been implemented for the proof of concept.

A novel real-time processing system model is applied to criminal activity detection for the citizen security control center. The system was used to classify criminal events detected through video surveillance sub-system using region convolutional neural networks (RCNN) and AlexNet [34]. This criminal activity system detection produces an alarm when weapons and short firearms are detected for awareness and strategic decision. The real-time detection of concealed objects hiding in human clothing such as weapons and contraband metal material models is developed using a passive millimeter wave image (PMMWI) classification-based YOLOv3 algorithm [35]. The system can detect hiding contraband materials and weapons detection in real time. A small sample of imagery dataset was used in the experimentation using PMMWI in the YOLOv3 model. The results show better performance with a detection speed of 36 frames per second (FPS) and a mean average precision of 95%. The conflict zone surveillance and gathering of security information in real-time for military awareness is open for future research.

A smart surveillance-based automated system was developed to detect, identify, and recognize human concealed weapons such as handguns and rifles in the YOLOv3 model for training and classification [36]. The results obtained in YOLOv3 prove efficient and have a better detection accuracy of 98.89%, compared to YOLOv2 and the traditional CNN model 95% and 93.1% respectively.

A military surveillance application for intrusion monitoring that may involve humans, vehicles, and other suspicious objects is discussed using a deep learning algorithm with wireless sensor networks [37]. For the surveillance and detection of human movement, events of interest, and vehicles. The convolutional neural network (CNN) was used for the image analysis. This deep learning technique plays a significant role in the feature segmentation of the detected images without human intervention or supervision. The results obtained from the video tracking analysis using CNN have 80.35% efficiency in object tracking and an accuracy of 92% from the test of an image captured. Thus, the summary of the related works based on the methods, and performance evaluation results are presented in Table 1, with our proposed techniques.

An intelligent ammunition system for monitoring, detecting, and classifying people carrying harmful materials, weapons, or ammunition is developed using a convolutional neural network [38]. The system model utilizes CCTV cameras to capture images for analysis using deep CNN in learning and classification. MATLAB was employed to simulate intelligent ammunition detection and classification using CNN. The results show 99.41% detection accuracy, and the loss rate is 0.01. However, the result obtained in this work outperforms the methods in the existing literature, such as Overfeat-1, Overfeat-2, and VGGNet.

The surveillance system-based internet of things (IoT) and artificial intelligence (AI) for fire accidents and intrusion was developed using smart drones for factory intruders monitoring, and fire accidents by alerting about the situation [39]. A passive pyroelectric infrared detector and flame sensor were used to detect human trespassers and to sense the occurrence of flame or smoke. However, the YOLOv8 and Cascade Classifier are trained and implemented in the module to analyze some dangerous objects, fire, and people squatters. The performance shows 92.1% detection accuracy and direction tracking 90%. The system is efficient for automatic tracking and video streaming of some circumstances is transferred to the security agent with relative accuracy.

An unmanned aerial vehicle system is developed for intrusion detection in a military zone using a timed-probabilistic automata (TPA) technique [40]. This surveillance system is targeted for environmental monitoring, rescue missions, and searching in military operations by modeling normal maneuvers of UAVs swarming and observing any deviations that may indicate an intrusion activity. The UAV system swarming is adaptable to the various intrusion patterns detection and efficient in identifying zero-day attacks. The performance of the TPA algorithm on the intrusion detection system was experimented with based on different automata models. The performance detection accuracy with 30 drones is 99.17%, F-measure is 99.10%, and precision is 99.13%.

3. Methodology

3.1 The intrusion detection module

The detection architecture of an impostor pattern movement in the conflict zone is developed and simulated in a

spanning tree network (STN) environment, programmed with Python language, and uses a quasi-unit-disk graph (QUDG) for node communication. Other supportive libraries such as Networkx 2.2, NumPy, Scipy, and Matplot 2.3 were used for the graphical design of the sensor nodes, connectivity of cluster heads, and communication. Approximately 400 sensor nodes were deployed into the network for the intrusion detection investigation in the conflict zone, and configured for non-intrusion node communication at a radius 120 cm apart, intrusion node communication at 60 cm, and the node communication to each other (neighbors' node) is 600 cm with seven cluster head as depicted in Figure 1.

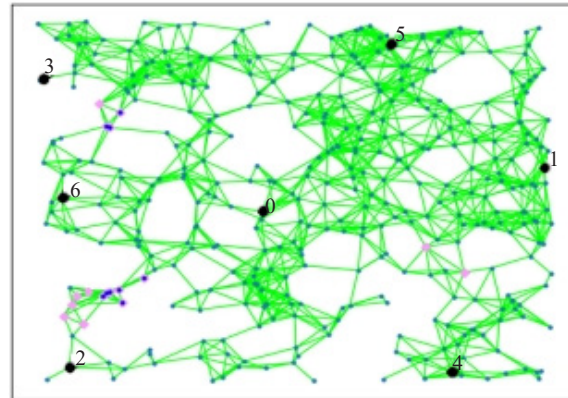


Figure 1. Distributed wireless sensor network architecture

The breadth-first search algorithm (BFS) was used for searching and detecting intrusion patterns through the root nodes, by estimating the neighbor nodes' connectivity distance, and communication radius. The configuration of the network model is given in Table 1.

Table 1. Simulation parameters for the smart city networks

Node deployment category	Configuration
Communication model	Quasi-unit-disk-graph (QUDG)
Number of nodes	400
Normal nodes' communication radius	1.2 m
Anomaly node communication radius	0.6
Node distance	6 m
Number of cluster head	8

This intrusion detection network model was built on the layer 2 network topology using spanning tree protocol. The spanning tree network (STN) is a layer 2 protocol that builds a logical topology loop-free to prevent the broadcast radiation and bridge of loops that may arise from the networks. This STN protocol elects one of the root bridges (cluster head) and selects one root node from the non-clustering head. The designated cluster head (port) is selected from the segmented network to determine the impostor pattern movement. The distributed sensor node architecture for intrusion detection in conflict zones is presented in Figure 2. This architecture consists of several sensor nodes in purple color, cluster heads in green-yellow color, a sink node that provides a wireless transmission link between the sensor field environment and remote monitoring center, and the gateway server. All the security information, and terrorist movement

patterns gathered from the field sensing environment are transmitted through the cluster head to the monitoring center for their attention and notification.

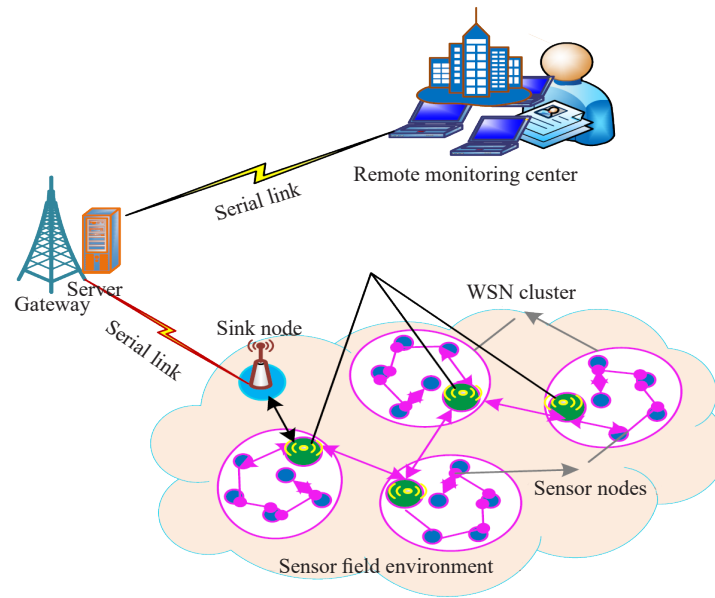


Figure 2. Distributed wireless sensing architecture

3.2 The surveillance sensing module

The proposed surveillance architecture utilized an embedded advanced RISC machine (ARM) Cortex A75 processor, PIR motion sensor, camera sensor, and microelectromechanical system. The Raspberry Pi controller is a small computer single-board (SCSB) using an ARM Cortex A75 processor. The raspberry Pi (RPi) technology uses Python programming for intelligence activities such as machine learning, deep learning, and computer vision for image processing, training, and recognition. The features of RPi include a high-definition multimedia interface (HDMI) port for video connection a graphic processing unit (GPU) for accelerating image processing, and many others. This processor includes random-access memory (RAM), Ethernet port, secure digital (SD) card slot, and general-purpose input and output (GPIO) interfacing with various electronic systems, with a standard wired/wireless keyboard and mouse port. A camera sensor is integrated into the surveillance system module detecting the motion/movement of an impostor and sends information to the arm-cortex processor for the camera-sensor activation. A camera sensor is a hardware component designed with millions of light-sensitive spots called photo sites within the camera, which capture light signals across the objects through the lens and transform them into an image for storage. The quality of the image from the camera sensor can be determined through the image quality and resolution, angle of view, depth of field, low-light performance, and size of the camera and lens. This surveillance system also comprises a global positioning system/global system for mobile (GPS/GSM) module for localization detection and transmission of information remotely to the cloud database in real-time. The block diagram of the surveillance system is presented in Figure 3, and the circuit diagram of the surveillance prototype is shown in Figure 4.

However, the intruder detection unit integrates with a infrared (IR) passive infrared (PIR) based switch light emitting diode (LED) sensor to detect the object passing around the conflict zone. The geophone sensor detects human footstep movement over a distance, the camera sensor works concurrently with the IR-LED switch to take a snapshot image of the human intruder around the conflict region. This information is transmitted to the intelligent controller unit for image processing, analysis, and identification, and immediately forwarded to the central location called the monitoring center for an urgent response.

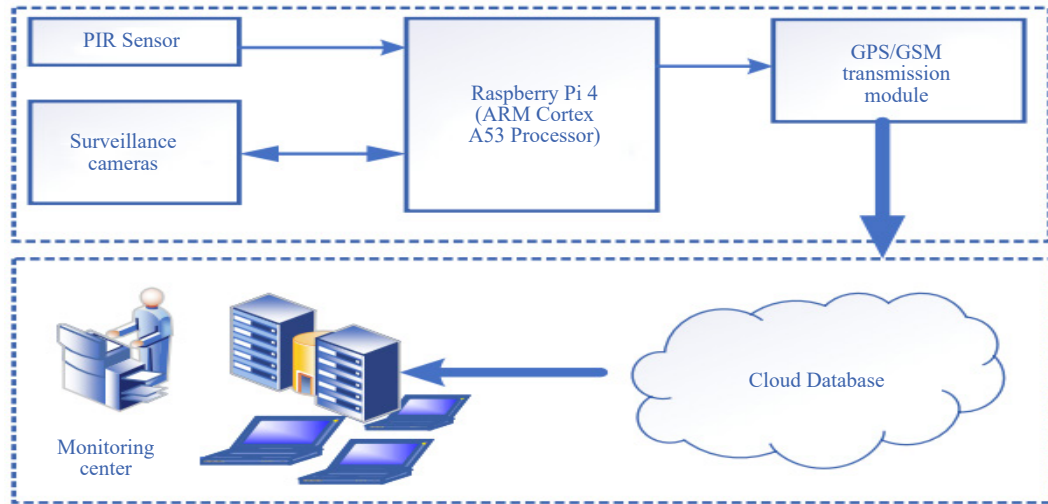


Figure 3. Block diagram of the surveillance system

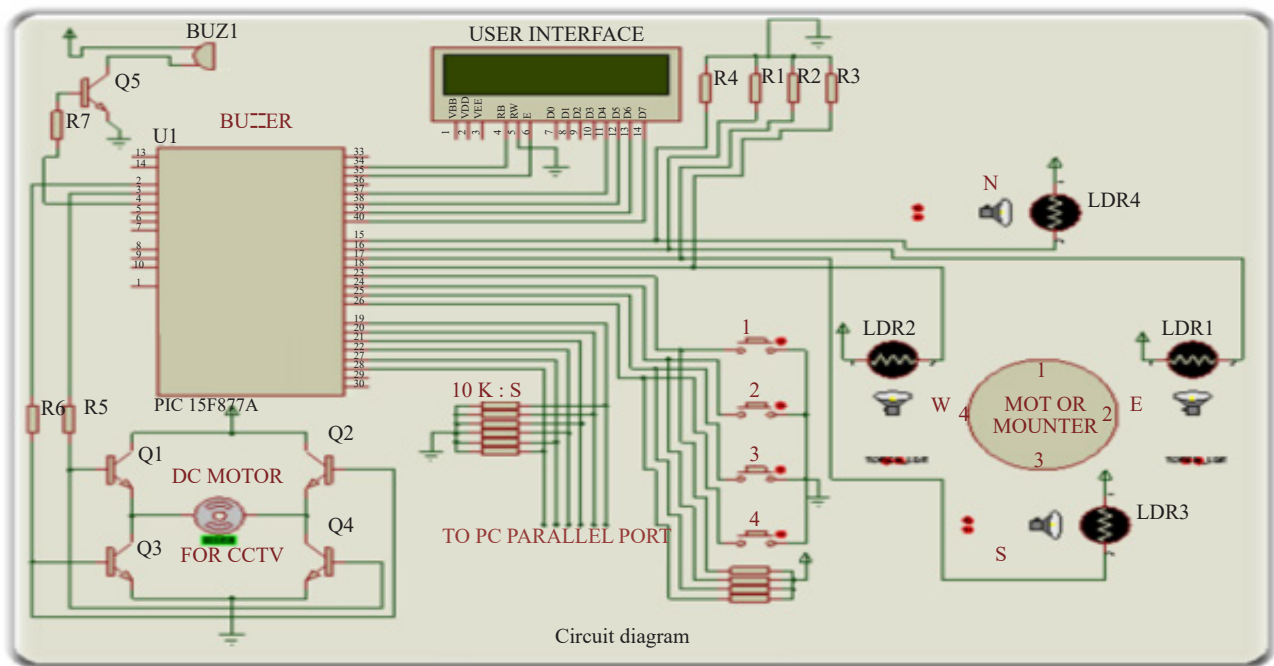


Figure 4. Circuit diagram of the surveillance system overview

3.3 The intelligent surveillance and firearm detection model

The firearm image detection model is developed, simulated, and experimented with in YOLOv5 using multi-scale prediction and deep learning classifier algorithm. The self-taught learning architecture uses an anchor box to transform the object detector and perceive the prediction. The non-maximum suppression threshold (NMST) is applied to avoid multiple times box detection in the model as shown in Figure 5. The process is initialized with firearms image acquisition which is inputted into the YOLOv5 model for the object identification. The firearm image is processed using a deep learning convolutional neural network (DLCNN) for object detection, and image recognition in the multi-layer

visual geometry group (VGG).

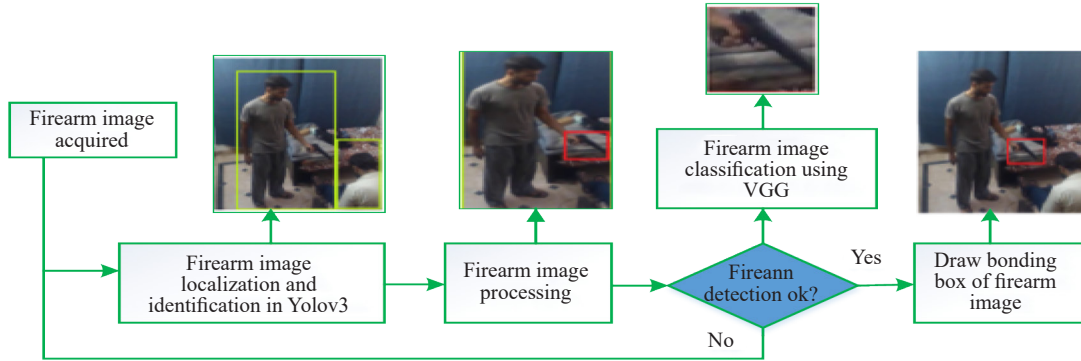


Figure 5. A firearm detection model in Yolov5

The non-maximum suppression threshold (NMST) algorithm for anchor box densities in firearm image detection and object recognition is presented in Algorithm 1. This NMST algorithm ensures that only a significant part of the image edges is reserved to reduce error rate and false edge tracking.

Algorithm 1: Non-maximum suppression threshold algorithm for anchor box densities-based image detection

Input: $\partial_b = \{b_1, b_2, b_3, \dots, b_N\}$, $\partial_s = \{s_1, s_2, s_3, \dots, s_N\}$, $\partial_d = \{d_1, d_2, d_3, \dots, d_N\}$, $\aleph_{th}$
 where, ∂_b is the list or set that contains beginning of detection box or bounding, ∂_s is the list contains detection scores correspondence, ∂_d is the detection densities index, $\aleph_{th}$ is the non-maximum suppression threshold

Begin
 $\zeta \leftarrow \{ \}$
while $\partial_b \neq \text{empty}$ **do**
 $m \leftarrow \text{argmax } S$
 $M \leftarrow b_m$
 $N_M \leftarrow \max (N_t, d_m)$
 $\zeta \leftarrow \zeta \cup M$; $\partial_b = \partial_b - M$
for b_i in ∂_b **do**
if $iou(M, b_i) \geq N_t$ **then**
 $\partial_b \leftarrow \partial_b - b_i$; $\partial_s \leftarrow \partial_s - s_i$;
end
end
end
return ζ, ∂_s
end

Therefore, a binary cross-entropy approach was used for the classification, and estimation loss in each bounding label to achieve confidence in the object class prediction as given in Equation (1).

$$L_{loss} = -\frac{1}{m} \sum_{j=1}^m \left[\left(\gamma_j \cdot \log \hat{\gamma}_j + (1 - \gamma_j) \cdot \log (1 - \hat{\gamma}_j) \right) \right] \quad (1)$$

where, L_{loss} is the binary cross-entropy classification loss function in each bounding label, m is the number of classes, γ_j is the probability of class 1, and $\hat{\gamma}_j$ is the probability of class 0.

This Yolov5 model trains about 100 firearms, and 50 non-firearm sample images. However, the multi-tasks involved in the learning activities are fine-tuning for data learning, pre-trained adapter module, features extraction module, and zero-shot assumption.

i. Data learning fine tuning: The several layers of the features extraction such as problem-specific features called top layers, mid-level and bottom layers are weighted, and fine-tuned for the pre-trained, and training on the new data of transfer learning model. This learning functions described the new data function $\mathcal{F}_T$ that interprets the weighted parameters values $\mathcal{F}_T(W_s) = W_T$ from the weighted source W_s and W_T , and target tasks T_s and T_T through the pre-trained models (PTMs). So, the learning for each layer can be fine-tuning by adding a new set of parameters k to the tasks target for obtaining better performance accuracy as expressed in Equation (2).

$$\mathcal{F}_T(W_T, k) = W_s \cdot k \quad (2)$$

ii. Pre-trained adapter module: This is a fully fine-tuning of pre-trained models which implemented as a lightweight feedforward neural networks between several layers of pre-trained model to provides modular approach for the transfer learning, efficient-parameters, and resourceful computation. This adapter module introduces a different set of k -parameters which less to the weight values W_s (i.e $k \ll W_s$), and can be decomposed into the more compact module function such that $W_s = \{w\}_n$ and $K = \{k\}_n$. The learning function in the adapter module can be expressed as given in Equation (3), when the set of weight k parameters is changed to $k' = \{k'\}_n$, and original set of data weight is unchanged as $W_s = \{w\}_n$.

$$F_T(k \cdot W_s) = k'_1 \cdot w_1 \cdot k'_2 \cdot w_2 \cdot k'_3 \cdot w_3 \cdot \dots k'_n \cdot w_n \quad (3)$$

iii. Features extraction module: This module helps to transform the raw weighted data into a set of numerical features that can be processed to obtain original information. This processing involved learning concepts and representations of different levels of images such as edges E , regions R , and corners C or called interest points as illustrated in Figure 6. But, the collection of interest points in the pre-trained module is unchanged when fine-tuned, and can be expressed as in Equation (4).

$$F_T(W_s \cdot E) = E \times W' \quad (4)$$

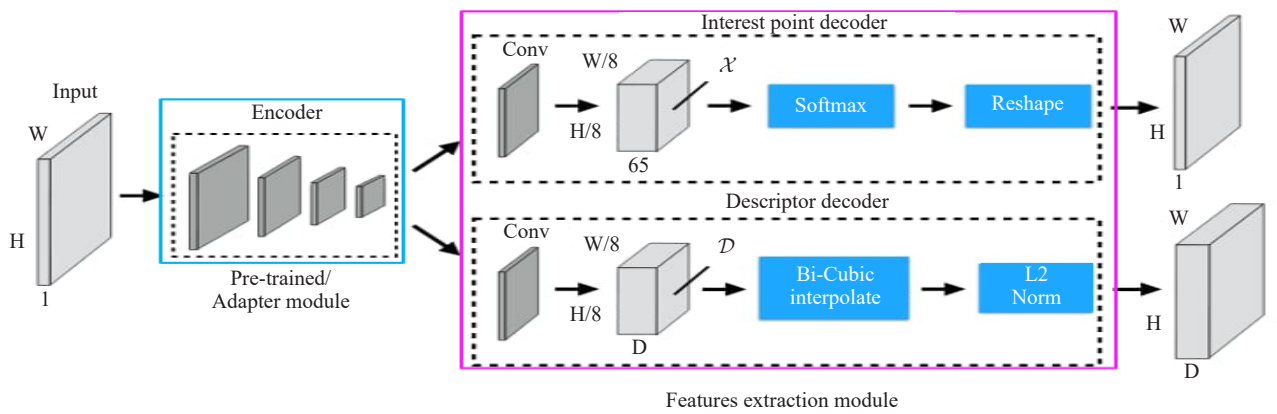


Figure 6. Fine-tuning and features extraction model processes through CNN

iv. Zero-shot: This process helps the pre-trained learning model classify the predicted samples, and observe the classes of samples belonging. The logical process involved in the object detection, and recognition of human-conceived

weapons using a deep convolutional neural network model is given in Figure 7.

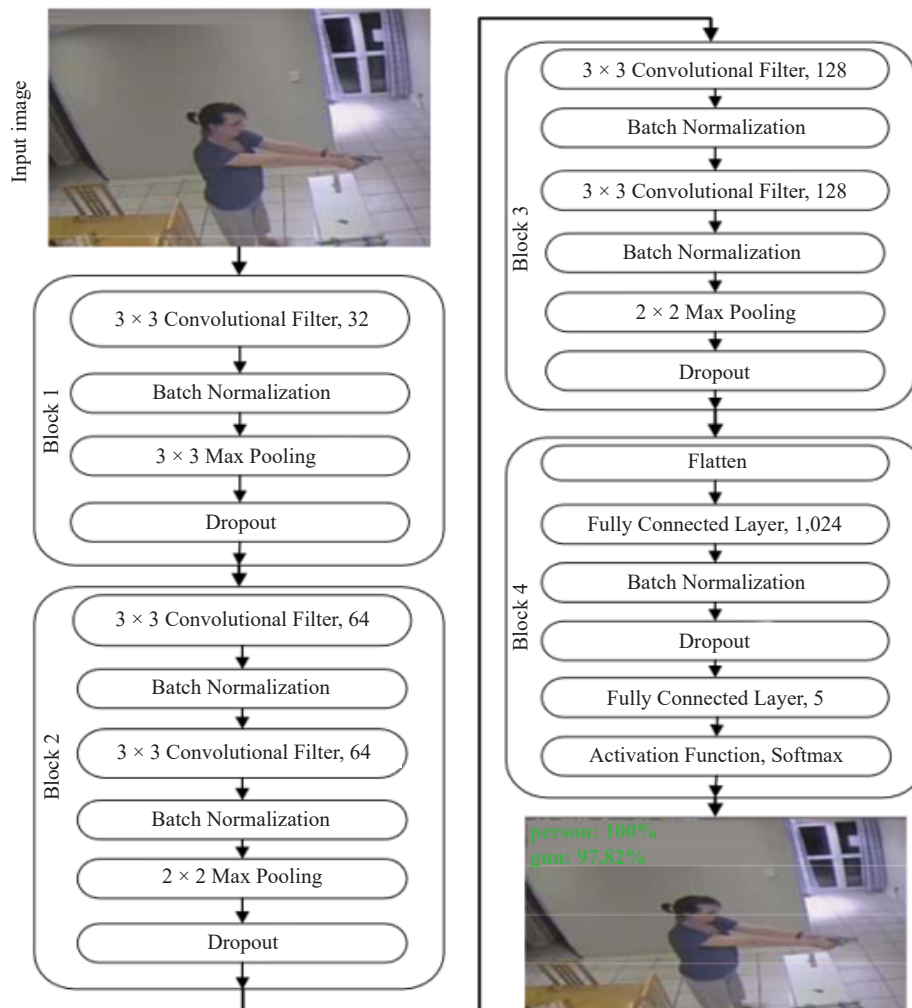


Figure 7. Human-conceived weapon image detection model using CNN

3.4 The autonomous combat and defense system architecture

The intelligent surveillance system module and defense architecture are responsible for processing the human image conceived weapon or video streams captured at the conflict region using the convolutional neural network (CNN) in YOLOv5 for training and classification. This autonomous system architecture includes sensor nodes that capture the frontline picture/video and transmit the security information to the cluster head. Each cluster head is responsible for big data transmission to the monitoring and control center (base station), where the picture/video is viewed for autonomous combat system response. Once the video/picture acquired is processed and analyzed, the surveillance unit activates the combat system to engage the opposition autonomously using drones or artillery weaponry to tackle the firearm adversary in the conflict region. The autonomous combat and defense system architecture is presented in Figure 8.

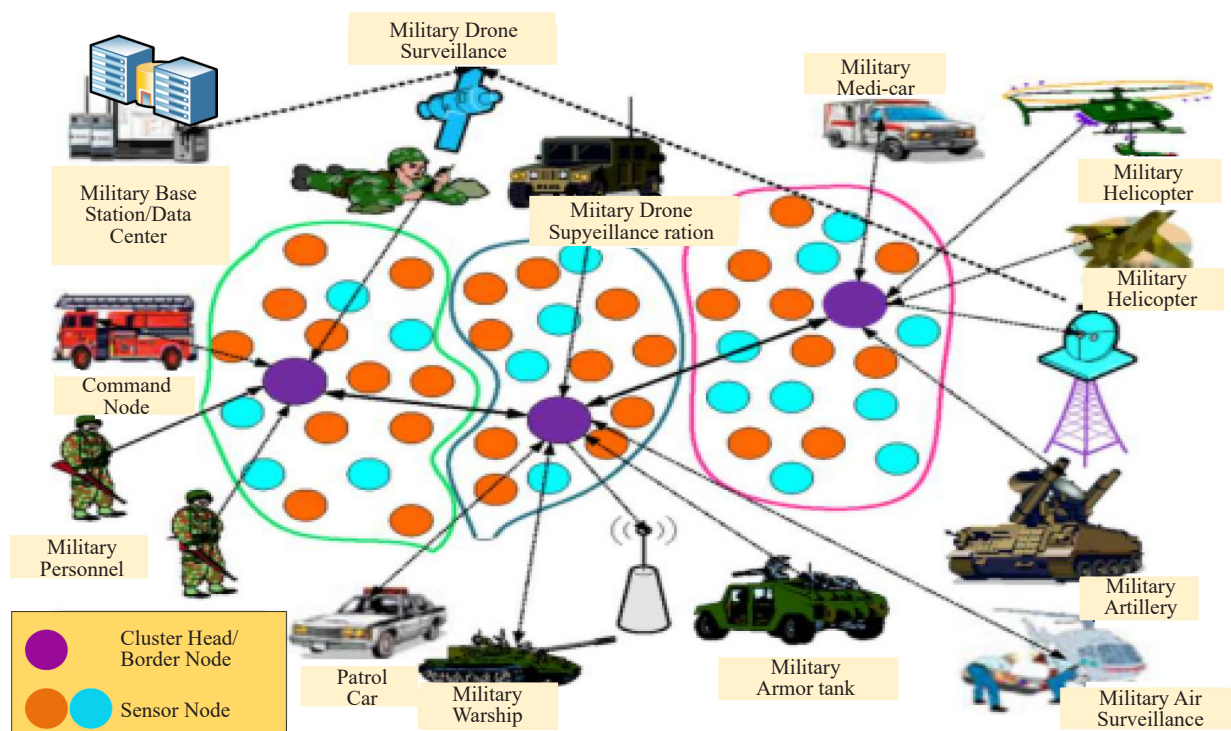


Figure 8. Intelligent surveillance and combat system architecture

4. Experimental results and discussion

4.1 Simulation result of distributed wireless sensor for intrusion detection

A distributed wireless sensing framework for security information gathering and intrusion detection patterns is implemented and simulated in a spanning tree network (STN) using a quasi-unit-disk graph (QUDG) for node communication. Many sensor nodes were deployed into the network area of 10 by 10 meters for surveillance and to detect intrusion in a region. These sensor nodes were grouped into different root nodes called cluster heads with a communication radius of 1.2 m for effective localization and detection. The movement/motion of intrusion over a distance in the region is configured to be 3 meters, and their communication radius is 0.6 m. This distributed wireless sensor testbed model is programmed using Python with other supportive libraries such as Networkx 2.2, NumPy, Scipy, and Matplot 2.3. The distributed wireless sensors for security information gathering were simulated using a breadth-first search algorithm (BFSA). This BFSA algorithm was adopted to search through each root node by estimating the neighbor connectivity distance, and radius. This experimentation was carried out when the deployed sensor nodes were 250, 260, 270, 280, 290, and 300 respectively.

During the investigation, about 250 sensor nodes were deployed in the STN. It is observed that 11 nodes in the region were truly identified as intruders, 11 as false intruders, and 228 nodes in the region were identified as true positive (normal nodes) in the networks. This process is repeated when the number of nodes increases from 250 to 260, 270, 280, 290 and 300. It is observed that the detection accuracy increases when the network size is increasing. This network simulation helps detect the intrusion during security information recovery at the region with the color blue-pink nodes. The predicted region likely to be attacked is identified in color pink nodes, and the unaffected region remains green color nodes as presented in Figure 9.

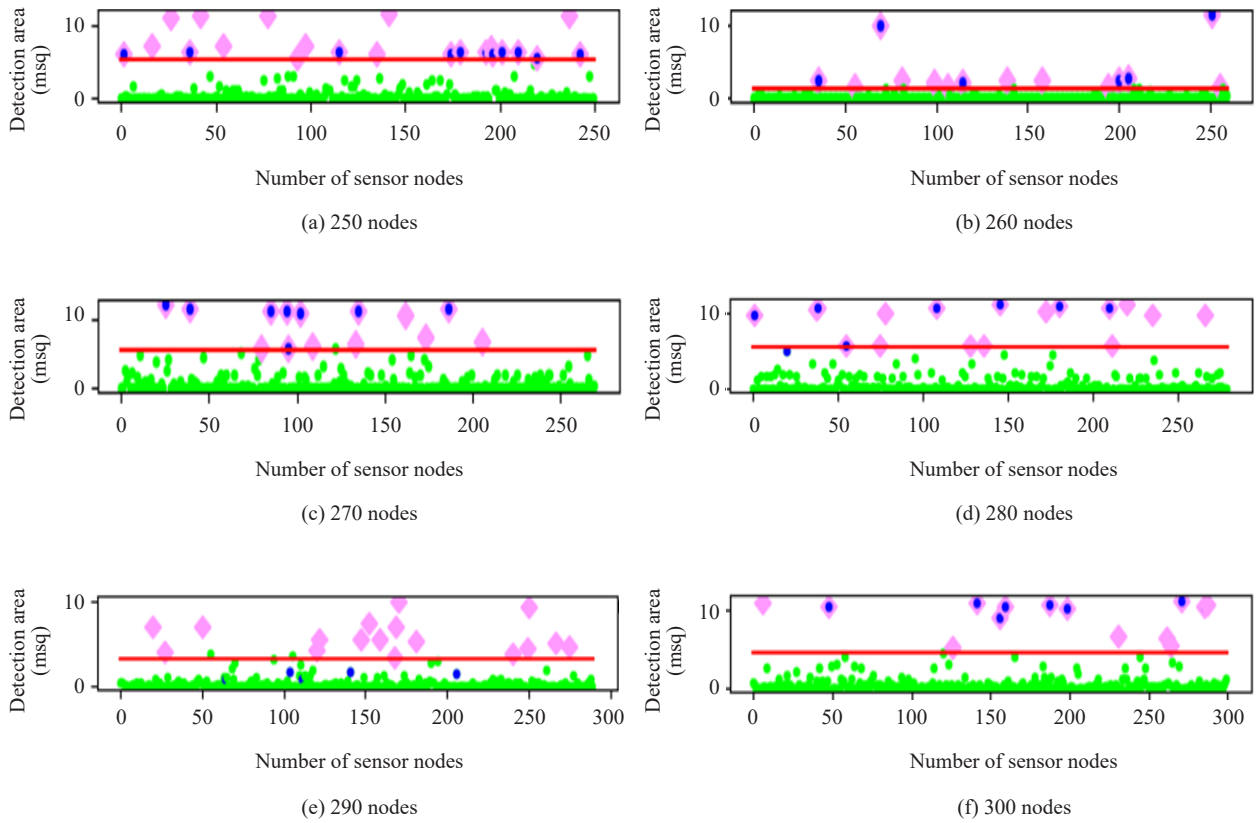


Figure 9. A graphical result of the surveillance detection model implemented in the spanning tree network with various numbers of nodes (250, 260, 270, 280, 290, and 300) respectively

Therefore, the intrusion detection system model implemented in the STN was evaluated using a confusion matrix based on the true positive (TP), true negative (TN), false positive (FP), false negative (FN), accuracy, sensitivity, and precision are discussed. The graphical results of the confusion matrix that illustrate prediction, normal, and abnormal activity are shown in Figure 10. The detection accuracy against the number of deployed sensor nodes in the STN model is presented in Figure 11. Table 2 shows the performance evaluation analysis of the detection model.

i. Detection accuracy: This metric is used to evaluate the performance of anomaly detection in the model by calculating the number of anomalies predicted correctly to the total number of prediction nodes as expressed in Equation (5).

$$D_A = \frac{T_p + T_N}{T_p + T_N + F_p + F_N} \quad (5)$$

ii. Sensitivity/Recall (S/R): This evaluation measure verified the rate through which the positive class anomalous observed are correctly predicted as expressed in Equation (6).

$$S \text{ or } R = \frac{T_p}{T_p + F_N} \quad (6)$$

iii. Precision (ρ): This evaluation metric shows the rate through which the correctness of true positive of anomalies prediction is accurate as expressed in Equation (7).

$$\rho_r = \frac{T_p}{T_p + F_p} \quad (7)$$

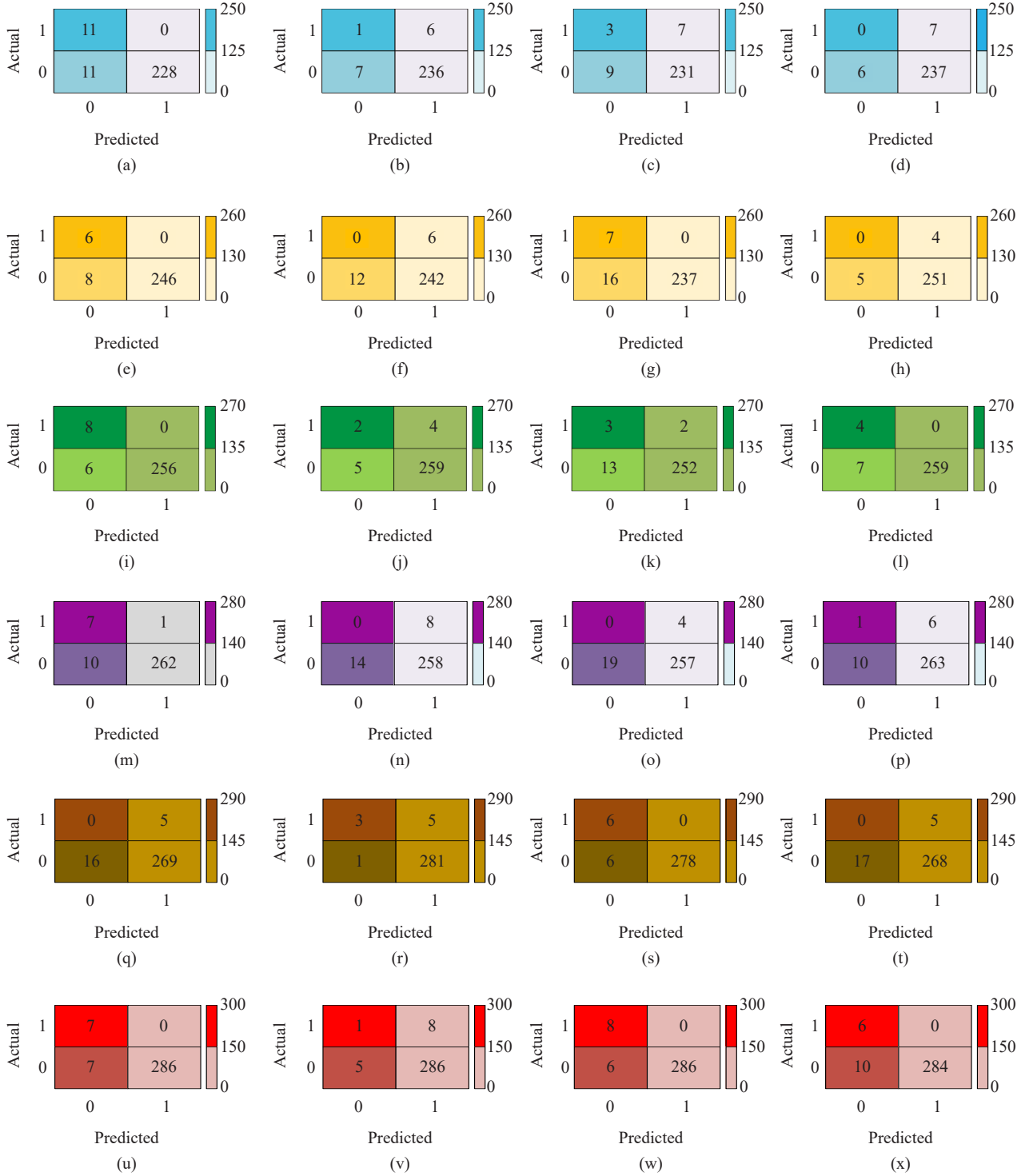


Figure 10. Prediction analysis of the intrusion detection model based on the true positive (TP), true negative (TN), false positive (FP), and false negative (FN) with the deployment of 250, 260, 270, 280, 290, and 300 nodes respectively

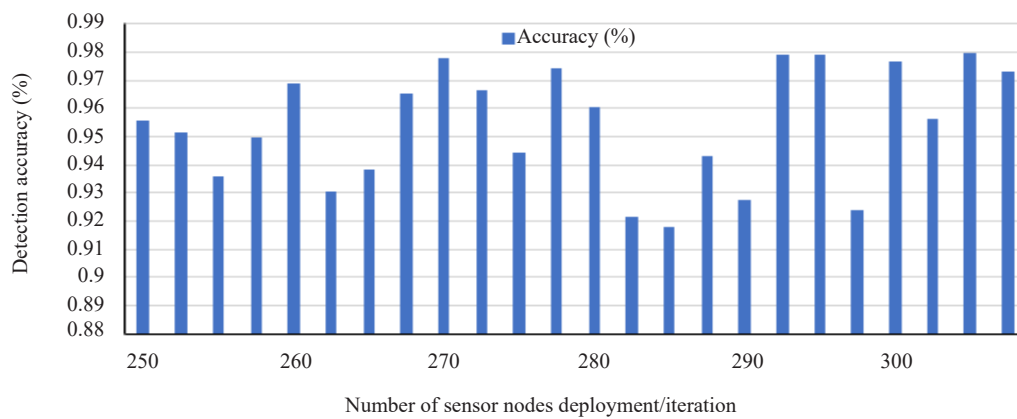


Figure 11. Number of surveillance nodes against the detection accuracy (%)

Table 2. Performance analysis of surveillance system in an STN

Nodes	Accuracy (%)	Sensitivity	Precision	Average detection accuracy rate $\times 100$
250	0.9560	0.0000	0.5000	94.85
	0.9518	0.1429	0.1250	
	0.9360	0.3000	0.2500	
	0.9500	0.0000	0.0000	
260	0.9692	0.0000	0.4286	95.10
	0.9308	0.0000	0.0000	
	0.9385	0.0000	0.3043	
	0.9654	0.0000	0.0000	
270	0.9778	1.0000	0.5714	96.58
	0.9667	0.3333	0.2857	
	0.9444	0.6000	0.1875	
	0.9741	1.0000	0.3636	
280	0.9607	0.0000	0.6363	93.57
	0.9214	0.0000	0.0000	
	0.9179	0.0000	0.0000	
	0.9429	0.1429	0.0909	
290	0.9276	0.0000	0.0000	-
	0.9793	0.3750	0.7500	
	0.9793	1.0000	0.5000	
	0.9241	0.0000	0.0000	
300	0.9767	1.0000	0.5000	97.17
	0.9566	0.1111	0.1667	
	0.9800	1.0000	0.5714	
	0.9733	1.0000	0.3750	

4.2 Simulation result of human-conceived weapons detection in the YOLOv5 model

The video clips/images of firearms captured in the process of surveillance activities are loaded into the YOLOv5 model for the training and identification using deep convolutional neural network (DCNN), and visual geometry group (VGG) that contains 2D-convolution and max pooling layers for images detection and classification. The firearm images dataset is fine-tuned by adding a new set of parameters k to the target tasks for better performance output. This fine-tuning output is pre-trained in the adapter module for efficient computation and adequate feature extraction. The result shows excellent performance with better detection accuracy as presented in Figure 12. The first category of the images clip is classified as human images with possession of a real firearm in (a-c) and, the weapon is identified with performance of 100%, 99.69%, and 88.09% detection accuracy and the processing time taken for each image/video clip are (0.875, 0.875, and 0.844) seconds respectively. The second is the weapon descriptions predicted only presented in (d-j). The detection accuracy results obtained for the image detection accuracy are (100, 97.99, 100, 91.55, 100, 100)%, and the processing time are (0.859, 0.859, 0.828, 0.812, 0.875, and 0.875) seconds respectively. The third category weaponry classification is not a real firearm but has a gun structure as presented in (k-l). The detection accuracy results obtained for the third category that are not weapon images are (100, 100, and 99.71)% with processing times of 0.828, 0.828, and 0.844) seconds respectively.

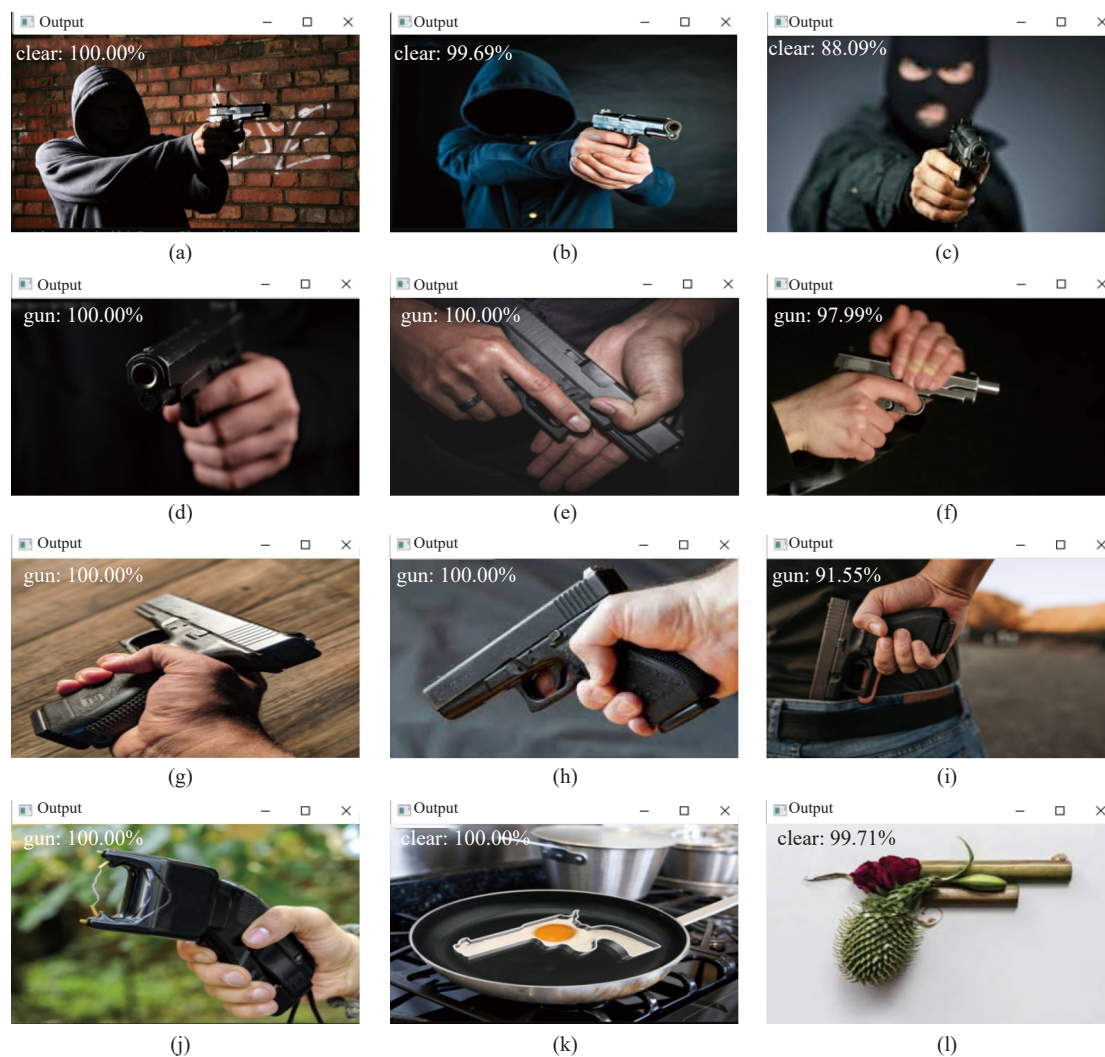


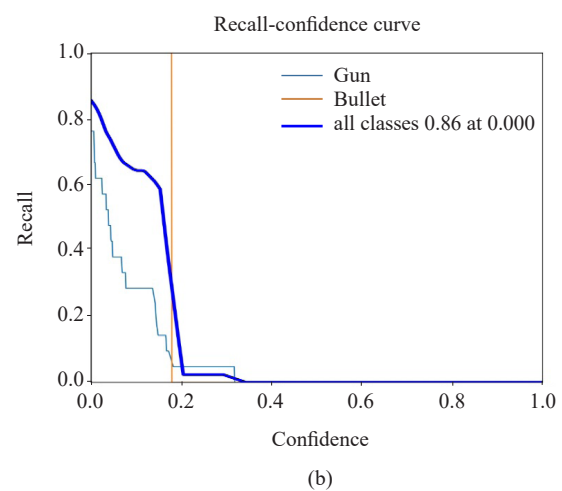
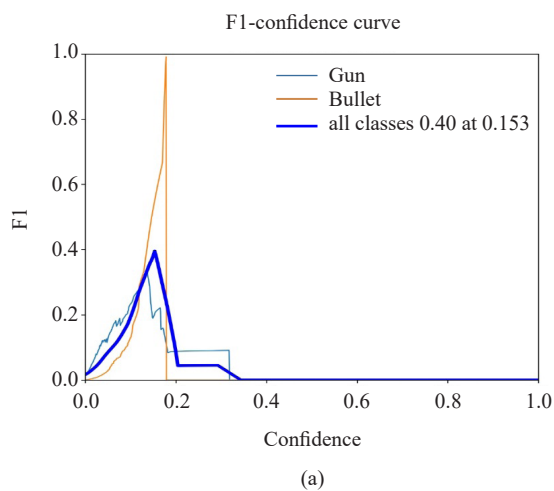
Figure 12. Firearm image detection analysis in YOLOv5 model

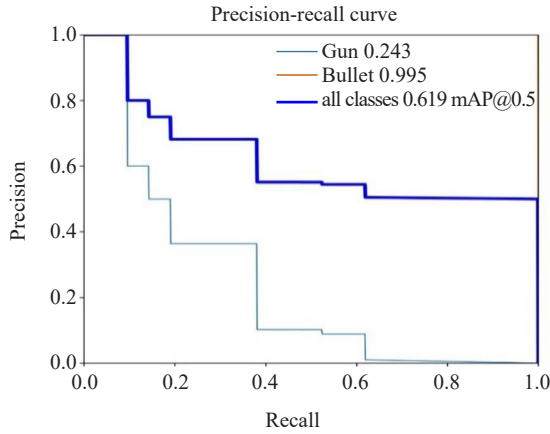
However, other images like bullets and Ak-47 rifles are subjected to the intelligent deep learning image processing and detection module in Yolov5 for identification. The detection accuracy obtained on the bullet and Ak-47 rifles images is presented in Figure 13.



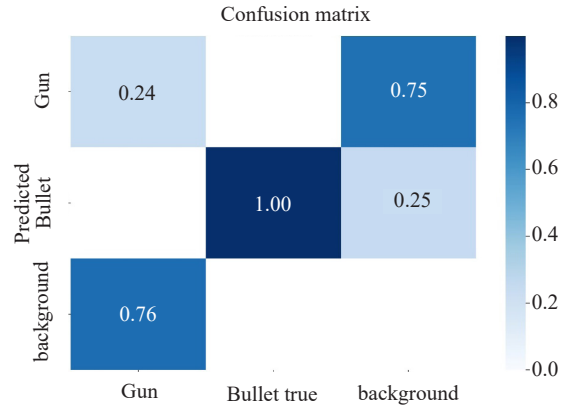
Figure 13. Identification and detection of weapon image simulation

The illustrated graph in Figure 14(a) shows the F1-confidence curve comparison between the bullets, Ak-47 rifles, and all classes of weapons as a good balance object detection of 0.55 threshold at a confidence of 0.31 for precision and sensitivity. This curve signifies that a model can be better detected while minimizing the false positive rate. Therefore, Figure 14(b) shows the recall-confidence curve of 0.86 at 0.00 for all classes of image identifiers, and Figure 14(c) illustrates the precision recall. For gun image detection is 0.243, bullets are 0.995, and mAP_0.5 of 0.619 for all classes of image detection. Figure 14(d) illustrates the confusion matrix to visualize the model performance classification, and provide detailed outcomes results based on true positive counts, true negative, false positive, and false negative of image class through the training processes. The training models in Yolov5 show that the model is losing below 0.15, and, train_loss metric mAP_0.5-0.95, as illustrated in Figure 14(e) for the image detection model.

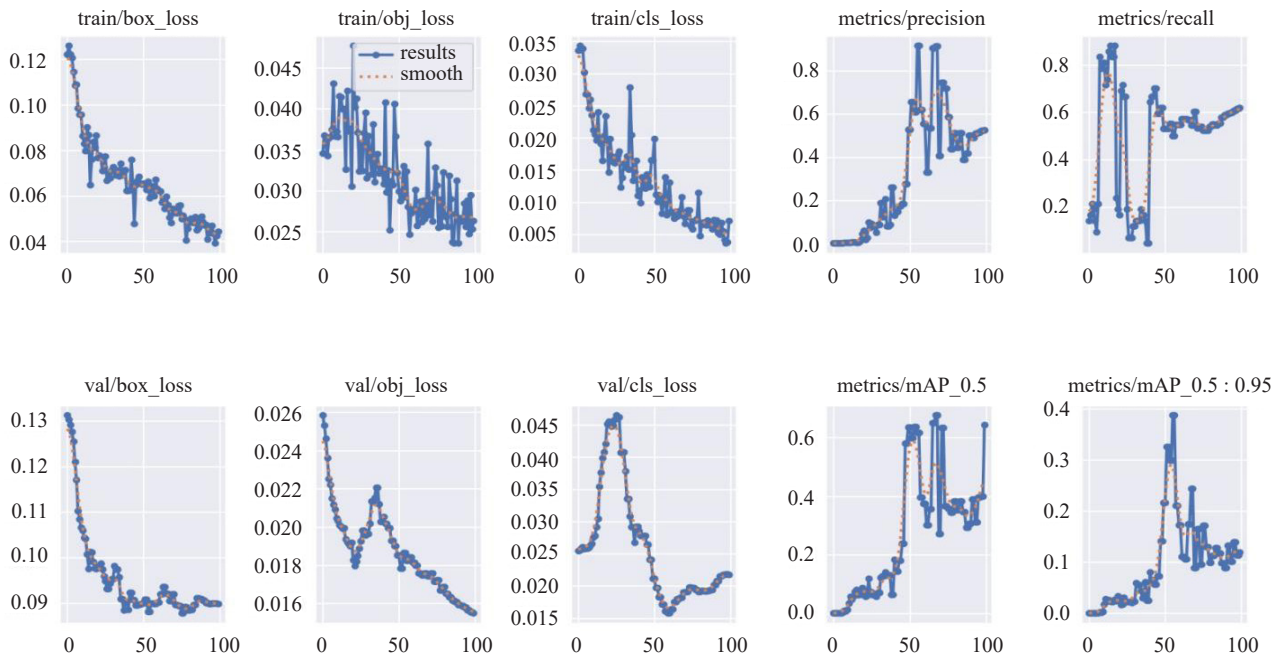




(c)



(d)



(e)

Figure 14. The graphical performance analysis of firearm detection in the yolo model is (a) F1-confidence curve (b) Recall-confidence curve (c) Precision-recall curve (d) Confusion matrix for the weapon image detection accuracy (e) Plot of box loss, object loss, and classification loss

4.3 Performance evaluation analysis

The proposed model is evaluated and compared with the state-of-art based on the methods and the performance of the proposed methods as presented in Table 3.

Table 3. Summary of the related works based on the methods and performance evaluation

Research works	Methods	Performance evaluation
Early detection of abnormal behavior and terrorist attack warning.	Robust symmetry algorithm (ROSY).	Detection accuracy is 88.16%, 90.06%, and 89.16%, and false acceptance rates are 5.30%, 3.65%, and 4.90%.
Multi-phase wireless sensor network design for the detection of explosive devices.	Multiple wireless sensor-based on diverse orthogonal techniques simulated in LabView.	A false alarm is reduced, and improved detection accuracy.
Military surveillance system with sensor nodes batteries management [31].	Using WSNs, and node scheduling for node-efficient energy management.	Not available.
Intelligent imaging technology for the prevention of terrorism [32].	Computer vision & Viola-Jones algorithm with SVM.	Image detection accuracy is 98%.
A multi-sensing framework for human intruder detection and border surveillance [33].	Using WSN such as Hydrophones infrared, and camera sensors.	Not available.
Military surveillance for intrusion monitoring, detection, and tracking [37].	Using WSNs and deep-learning approach.	The detection accuracy of the object detected through the surveillance area is 72.29% and 91.54%.
Real-time concealed object detection [35].	Passive millimeter wave images (PMMWI) embedded with the YOLOv3 Algorithm.	The result shows a detection speed of 36 FPS and a mean average precision of 95%.
Smart surveillance system for weapons detection [36].	YOLOv3.	The result shows a detection accuracy of 98.89%.
Intelligent ammunition detection and classification system [38].	Convolutional neural network (CNN).	The results show 99.41% detection accuracy, and the loss rate is 0.01.
An intrusion detection system for drone swarming [40].	Timed probabilistic automata (TPA) algorithm.	The performance detection accuracy with 30 drones is 99.17%, F-measure is 99.10%, and precision is 99.13%.
Smart drone surveillance system for fire accident detection and intrusion [39].	Passive pyroelectric infrared detector, analog flame sensor, ESP32 microcontroller, and YOLOv8.	Performance shows 92.1% detection accuracy and direction tracking 90%.
Distributed wireless sensor network for surveillance and autonomous combat system (Proposed work).	Using WSNs, computer vision, and SVM. The WSNs are simulated in the STN, and image processing is simulated in the YOLOv5 model.	The intrusion detection accuracy is 97.17%, sensitivity is 1.0000, and precision is 0.3750. Firearm detection accuracy is 100%.

5. Conclusion

The WSN prototype for security information gathering and intrusion detection is implemented in a spanning tree network testbed model for the simulation, and the performance evaluation was based on standard metrics. The average detection accuracy results obtained when deployed 250, 260, 270, 280, 290, and 300 nodes are 94.85%, 95.10%, 96.58%, 93.57%, 95.26%, and 97.17% respectively. A prototypical model of the multi-wireless sensor network for autonomous defense systems and security information gathering is proposed. The model includes a Raspberry Pi ARM Cortex A53 processor, PIR-LED switch, and surveillance cameras for human intruder detection in a conflict region.

The intelligent part of the system for autonomous combat uses a deep convolutional neural network (DCNN) for video stream analysis, and image processing in the Yolov5 model. However, the firearm detection model is implemented in YOLOv5 using deep convolutional neural network (DCNN). The result shows better performance with a detection accuracy of (100, 97.99, 100, 91.55, 100, 100)%, and the processing time of (0.859, 0.859, 0.828, 0.812, 0.875, and 0.875) seconds respectively.

Acknowledgment

This work is supported by the Tertiary Education Trust Fund Federal Republic of Nigeria, through the Local Research Grant (TETF/DR&D/CE/NDA/KADUNA/IBR/2020/VOL.1). The authors acknowledge the support of the Board of Trustees of TETFund, Nigeria.

Conflict of interest

The authors declare no conflicts of interest associated with this publication.

References

- [1] Jimoh OD, Ajao LA, Adeleke OO, Kolo SS. A vehicle tracking system using greedy forwarding algorithms for public transportation in urban arterial. *IEEE Access*. 2020; 8: 191706-191725.
- [2] Layton P. *Fighting Artificial Intelligence Battles Operational Concepts for Future AI-Enabled Wars*. Australia: ADC Publications; 2021.
- [3] Ajao LA, Agajo J, Kolo JG, Maliki D, Adegboye MA. Wireless sensor networks based-Internet of Things for agro-climatic parameters monitoring and real-time data acquisition. *Journal of Asian Scientific Research*. 2017; 7(6): 240-252.
- [4] Ananthi JV, Koresh HJD, Vengatesan S, Glorita YBA. A secure communication over wireless sensor devices using intelligent arrival estimation algorithm. *International Journal of Networking and Virtual Organizations*. 2018; 19(2-4): 385-394.
- [5] Heidari A, Nima JN, Dag H, Unal M. Deepfake detection using deep learning methods: A systematic and comprehensive review. *WIREs Data Mining and Knowledge Discovery*. 2024; 14(2): e1520.
- [6] Zhang X, Yi WJ, Saniie J. Home surveillance system using computer vision and convolutional neural network. In: *2019 IEEE International Conference on Electro Information Technology (EIT)*. Brookings, SD, USA: IEEE; 2019. p.266-270.
- [7] Ajao LA, Adedokun EA, Mua'zu MB, Agajo J. Smart embedded wireless system design: An Internet of Things realization. *International Journal of Automation and Smart Technology*. 2021; 11(1): 2146.
- [8] Heidari A, Nima JN, Unal M, Zhang G. Machine learning applications in Internet-of-Drones: Systematic review, recent deployments, and open issues. *ACM Computing Survey*. 2023; 55(12): 1-45.
- [9] Osamy W, Khedr AM, El-Sawy AA, Salim A, Vijayan D. IPDCA: Intelligent proficient data collection approach for IoT-enabled wireless sensor networks in smart environments. *Electronics*. 2021; 10(9): 997.
- [10] Ngabo D, Wang D, Iwendi C, Anajemba JH, Ajao LA, Biamba C. Blockchain-based security mechanism for the medical data at fog computing architecture of Internet of Things. *Electronics*. 2021; 10(17): 2110.
- [11] Ali A, Jadoon YK, Changazi SA, Qasim M. Military operations: Wireless sensor networks-based applications to reinforce future battlefield command system. In: *2020 IEEE 23rd International Multitopic Conference (INMIC)*. Bahawalpur, Pakistan: IEEE; 2020. p.1-6.
- [12] Xi M, Lingyu N, Jiapeng S. Research on urban anti-terrorism intelligence perception system from the perspective of Internet of things application. *The International Journal of Electrical Engineering & Education*. 2021; 58(2): 248-257.
- [13] Ajao LA, Apeh ST. Secure edge computing vulnerabilities in smart cities sustainability using petri net and genetic algorithm-based reinforcement learning. *Intelligent System with Application*. 2023; 18: 200216.
- [14] Sabol J. Sophisticated drones: New dangerous tools for potential radiological attack on selected soft targets. In:

Soft Target Protection: Theoretical Basis and Practical Measures. Netherlands: Springer; 2020. p.327-336.

- [15] Sadik G, Kaya C. The role of surveillance technologies in the securitization of EU migration policies and border management. *Uluslararası İlişkiler Dergisi*. 2020; 17(68): 145-160.
- [16] Moore L. The boundary problem in a surveillance society: Moving beyond individual ethics and compliance. In: *The Routledge Handbook of Accounting Ethics*. Routledge; 2020. p.386-404.
- [17] Karreddula KS, Deb AK. Detection of normal and abnormal conditions for boundary surveillance using unmanned aerial vehicle. In: *2021 International Symposium of Asian Control Association on Intelligent Robotics and Industrial Automation (IRIA)*. Goa, India: IEEE; 2021. p.50-56.
- [18] Kirwan G, Byrne J. Mechanisms of power in the digital age: Surveillance, privacy and professional boundaries in social work practice. In: *The Routledge International Handbook of Digital Social Work*. Routledge; 2023. p.393-403.
- [19] Tin D, Barten DG, Goniewicz K, Burkle FM, Ciottone GR. An epidemiological analysis of terrorism-related attacks in eastern Europe from 1970 to 2019. *Prehospital and Disaster Medicine*. 2022; 37(4): 468-473.
- [20] Ugwueze MI, Onuoha FC. Hard versus soft measures to security: Explaining the failure of counter-terrorism strategy in Nigeria. *Journal of Applied Security Research*. 2020; 15(4): 547-567.
- [21] Singh R, Singh S. Smart border surveillance system using wireless sensor networks. *International Journal of System Assurance Engineering and Management*. 2022; 13(Suppl 2): 880-894.
- [22] Teichmann FM. Current trends in terrorist financing. *Journal of Financial Regulation and Compliance*. 2022; 30(1): 107-125.
- [23] Gundabathula VT, Vaidhehi V. An efficient modeling of terrorist groups in India using machine learning algorithms. *Indian Journal of Science and Technology*. 2018; 11(15): 1-10.
- [24] Shabbir MS, Kiyani M, Zeb A. Impact of terrorism on the exclusive Indian economy. *Journal of Indian Studies*. 2019; 5(1): 29-45.
- [25] Arjun D, Indukala PK, Menon KU. Border surveillance and intruder detection using wireless sensor networks: A brief survey. In: *2017 International Conference on Communication and Signal Processing (ICCSP)*. Chennai, India: IEEE; 2017. p.1125-1130.
- [26] Malik AA. The modern electronic and other technologies to combat new wave of terrorism and criminal activities. *International Journal for Electronic Crime Investigation*. 2023; 7(3): 5-12.
- [27] Davis J. Understanding the effects and impacts of counter-terrorist financing policy and practice. *Terrorism and Political Violence*. 2024; 36(1): 1-7.
- [28] Leese M, Noori S, Scheel S. Data matters: The politics and practices of digital border and migration management. *Geopolitics*. 2022; 27(1): 5-25.
- [29] Segovia-Vargas MJ. Money laundering and terrorism financing detection using neural networks and an abnormality indicator. *Expert Systems with Applications*. 2021; 169: 114470.
- [30] Kumar PS, Anand C, Vasuki N, Ramesh V, Santhoshkumar SP. Wireless sensor networks: Revolutionizing explosive detection. In: *2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS)*. Bengaluru, India: IEEE; 2024. p.118-121.
- [31] Mahamuni CV. A military surveillance system based on wireless sensor networks with extended coverage life. In: *2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC)*. Jalgaon, India: IEEE; 2016. p.375-381.
- [32] Foster B, Johansyah MD. Implementation of intelligent imaging technology as a prevention of terrorism in the business sector in the 21st century using computer vision & viola jones algorithm with SVM (support vector machine) method. *Jurnal Ilmiah Kursor*. 2019; 10(2): 71-80.
- [33] Arjun D, Indukala PK, Menon KU. PANCHENDRIYA: A multi-sensing framework through wireless sensor networks for advanced border surveillance and human intruder detection. In: *2019 International Conference on Communication and Electronics Systems (ICCES)*. Coimbatore, India: IEEE; 2019. p.295-298.
- [34] Suarez-Paez J, Salcedo-Gonzalez M, Climente A, Esteve M, Gómez JA, Palau CE, et al. A novel low processing time system for criminal activities detection applied to command-and-control citizen security centers. *Information*. 2019; 10(12): 365.
- [35] Pang L, Liu H, Chen Y, Miao J. Real-time concealed object detection from passive millimeter wave images based on the YOLOv3 algorithm. *Sensors*. 2020; 20(6): 1678.
- [36] Narejo S, Pandey B, Esenarro Vargas D, Rodriguez C, Anjum MR. Weapon detection using YOLO V3 for smart surveillance system. *Mathematical Problems in Engineering*. 2021; 2021(1): 9975700.
- [37] Mahamuni CV, Jalaududin ZM. Intrusion monitoring in military surveillance applications using wireless sensor networks (WSNs) with deep learning for multiple object detection and tracking. In: *2021 International Conference*

on Control, Automation, Power and Signal Processing (CAPS). Jabalpur, India: IEEE; 2021. p.1-6.

- [38] Ahmad G, Alanazi S, Alruwaili M, Ahmad F, Khan MA, Abbas S, et al. Intelligent ammunition detection and classification system using convolutional neural network. *Computers, Materials and Continua*. 2021; 67(2): 2585-2600.
- [39] Hoang ML. Smart drone surveillance system based on AI and on IoT communication in case of intrusion and fire accident. *Drones*. 2023; 7(12): 694.
- [40] Subbarayalu V, Vensuslaus MA. An intrusion detection system for drone swarming utilizing timed probabilistic automata. *Drones*. 2023; 7(4): 248.