Intelligent Military Bases (IMB): Proposed Framework and Implementation

1st Prawit Chumchu
Faculty of Engineering at Sriracha
Kasetsart University
Thailand
prawit@eng.src.ku.ac.th

2nd Kailas Patil
Department of Computer Engineering
Vishwakarma University
India
kailas.patil@vupune.ac.in

***Abstract*—This paper presents an Intelligence Military Base (IMB) prototype which utilizes multi-sensors for detecting abnormalities. This proposed prototype is based on COTS (Commercial off-the-shelf) IoT (Internet of Things) technology which is applied for military. It is defined as IoBT(Internet of Battlefield Things). This proposed prototype provides an assistance and surveillance in military bases. The proposed system consists of a server and IoT-based sensors. The sensors are classified in two categories: long-range sensors and short-range sensors. LoRaWAN is used for communicating between the server and long-range sensors while WiFi is used for communicating between the sever and short-range sensors. Simple data fusion algorithms are used to fuse data from multi sensors and machine learning events. To monitor the system, an android application and a web-based application were developed. Three prototypes of the proposed frameworks were delivered to use for the South Thailand insurgency**

Keywords—IoT, IoBT, Military base, Surveillance, Security, Home Security

Fig. 1. A Village security base was invaded.

I. INTRODUCTION

South Thailand insurgency has occurred for a long time [1]. It is hard to be stopped. Many innovation solutions have been developed and managed to help military and communities. As in news, soldiers and volunteers in village security team are killed and village security base was attacked as shown in Fig 1. In this event, 15 volunteers and villages were killed 15 volunteers and villages were killed. Affordable intelligent military bases or intelligent village security bases are innovation needed for monitoring and real-time alerting if there are any misbehavior events.

Currently related existing proposals and commercial solutions do not firmly fit with the South Thailand insurgency in terms of cost and environment. In addition, commercial solutions are very expensive. Normally commercial solutions are based on CCTV (Closed-circuit television) [2], [3]. Researches in [4], [5] were proposed surveillance systems using heterogenous sensors.

This paper will present an intelligence military base prototype: IMB. The IMB has face detection and recognition, intrusion person detection, anomaly detection and log management. The rapid advancement of IoT technologies has led to its flexible adoption in battle field networks, known as Internet of Battlefield Things (IoBT) networks [6] - [11]. The proposed framework is IoBT-based. In addition, because continued advances in IoT technology have prompted new investigation into usage of Commercial-off-the-Shelf (COTS) technologies for military operations, the implementation of proposed framework is based on COTS devices. This leads to easily expand to commercial products or mass products.

The organization of paper is as follows. Section II presents background of military base or village security base and related tools. Section III presents design and implementation. Section IV presents data analysis and abnormal detection. Section V presents performance results. Section VI presents innovation and technology management. Section VII presents conclusion and future works.

II. BACKGROUND

In this section, some valuable background knowledge will be discussed.

A. *Overviview of the South Thailand insurgency*

There is an ongoing conflict centered in south Thailand. It originated in 1948 as an ethnic and religious separatist insurgency in the historical Malay Patani Region. It covers the three southernmost provinces: Pattani, Yala and Narathiwat and parts of a fourth province: Songkhla.

B. *Multi-Sensors and Data Fusion*

In military security application, one type of sensors could not fit. Therefore, multi-sensors are selected in this paper. To get final decision for alerting, data fusion needs to be employed.

Visual sensors are based on video cameras or thermal cameras. Video cameras could capture videos and images on daytime. Thermal cameras could capture on day and nighttime. They are suitable for nighttime capture. However, currently, the price is very high. The captured data could be processed by many techniques such as AI, Machine learning. However, limitation of video cameras needs to be line of sight.

Audio sensors or microphones are used to capture the sound in interesting areas. Sound could be analyzed by speech recognition, peak detection, language classification.

PIR (passive infrared) sensors measure infrared (IR) light radiating from moving objects that emit heat such as human, animals. Because PIR sensors do not emit any energy, they are classified as passive sensors. They detect the emission of infrared radiation and not heat.

A radar system is classified as active sensors. It has a transmitter that emits radio waves known as radar signals in predetermined directions. The receiver receives these signals which contact an object and are usually reflected or scattered in many directions

Wifi Sniffer is a tool to sniff WiFi MAC (Medium Access Control) addresses. A MAC address is the hardware address of a WiFi interface of a mobile phone. However, current, new operating systems let users use random MAC addresses.

Like WiFi sniffer, mobile phone sniffer is an equipment to sniff IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity) of a mobile phone.

Only one sensor could not perform well in military areas. To improve induction detection, multi-sensors should be used. In addition, suitable data fusion algorithm needs to be carefully selected.

In this paper, CCTV cameras, raspberry pi cameras, PIR, microphone and wifi sniffer are selected as shown in Fig. 3. The reason for using multi-sensors is that a sensor does not fit all environments.

For short-ragnge, CCTV cameras are slected. This is beause they can monitor and record real-time video aound military base. In addition, the CCTV cameras could be use for authenting staffs and detect a wanted person.

For long-range, rapsberry pi cameras, PIR, Microphone and wifi sniffer are slected. Usb camaras are used to detect inrtrusion person. However the person is not visble by camera, it can not detect. Like raspberry pi cameras, PIR sensors could be used to detect intrusion person based on movement. Microphone is used to detect an intrusion person using speech or sound. However, if he does not speak or is quiet, it can not detect. Wifi sniffer is used to sniff WiFi mac addresses of intrusion person mobile phones, if they enable wifi interfaces.

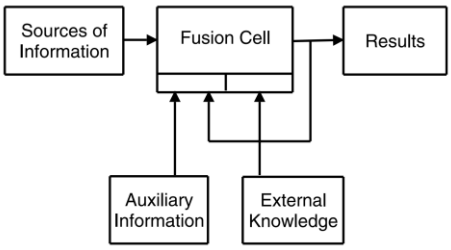

Fig. 2. Data Fusion

To process data from multi-sensors, there are varieties of data fusion algorithms. The good introduction of data fusion could be found in [14]. Fig. 2 shows the basic of data fusion. The inputs are from sources such as motion detection, PIR detection. The fusion cell is the algorithm to process the inputs which also get information from auxiliary information and external knowledge. The results are outputs of the data fusion which could be several formats such as binary format: event or no-event, binary format with confidentiality. The example of using data fusion for binary format could be read in [5]. Wang D. in [15] proposed data fusion from visual and audio for human intrusion detection.

C. *IoBT Technologies for military*

To send sensor data and command control, there are many commination technologies. In this sub-section, communication technologies will be presented.

1) LPWAN Technologies for IoT

Mekki K. et.al in [12] give overviews of LPWAN technology such as Sigfox, LoRaWAN, and NB-IoT. It could be briefed as follows.

LoRaWAN is a low power wide area network. The commination range is up to 15 kilometers. In Thailand, LoRaWAN is serviced by NT (National Telecom Public Company limited). However, currently, service does not cover whole Thailand.

Like LoRaWAN, Sigfox is a low power wide area network. It is used to connect low-power objects such as electricity meters and smartwatches. In Thailand, it is served by Thing on Net company limited.

NB-IoT is a low-power wide-area network (LPWAN) radio technology standard developed by 3GPP for cellular devices and services. NB-IoT normally provides service by mobile phone operators. Expense for accessing is not high such 350 bath per year. However, currently, the coverage area in Thailand is much. In South Thailand insurgency area, the coverage area is not good especially in the forest.

In the proposed framework, LoRaWAN is selected. This is because it gets free of accessing costs in Thailand using own private networks. In addition, it is free for operating in ISM bands while NB-IoT is not free for accessing. In addition, WiFi is selected for communicating in short-range and high bandwidth requirements such as real-time video streaming.

2) Application Layer Protocols in IoT(Internet of Thing)

There are many application layer protocols used in IoT such as CoAP (Constrained Application Protocol), MQTT (Message Queuing Telemetry Transport.), XMPP (Extensible Messaging and Presence Protocol), AMQP (Advanced Message Queuing Protocol) and REST (Representational state transfer). For details of application layer protocols in IoT could be found in [13].

In the proposed framework, REST and MQTT are selected. This is because REST is implemented in web service which is widely used for web-based application. MQTT is light weight and well used in many applications. In addition, LoRaWAN gateways used in our implementation provide MQTT communication.

III. DESIGN AND IMPLEMENTATION

A. *Overviw of proposed framework*

The design and implementation of the proposed framework is shown in Fig. 3. It consists of a dedicated server, 4 CCTV cameras, one access point, an ethernet switch, a LoRaWAN gateway and 4 long-range sensors. The number of sensors is not high. This is because the proposed prototype focuses on small military bases or village security bases. However, the developed software is capable for the large number of sensors.

B. *Long range sensors*

For each long-range sensor, there are one LoRaWAN end node, one raspberry pi zero or Raspberry Pi 4, one WiFi usb adaptor, one PIR sensor, one raspberry pi camera, one microphone and power bank with solar cell charger.

Each sensor detects abnormal events. For example, the WiFi usb adaptor detects the abnormal event from sniffing MAC addresses and comparing them with pre-defined MAC addresses in databases. If the sniffed MAC address is in database and whitelist, the detection is a normal event. If the sniffed MAC address is backlist in database, the detection is an abnormal event.

The PIR measures infrared (IR) light radiating from human movements. If the amount of infrared radiation is higher than manually pre-setting threshold, the detection is an abnormal event.

The raspberry pi camera and corresponding program detects motion detection in the coverage area. If change percentage of current image with a reference image is higher than pre-defined threshold, the result is an abnormal event.

The microphone is used to record sound around the monitoring area, if the average of sound energy is higher than pre-defined threshold, the detection is an abnormal event. The threshold could be changed by using web interfaces.

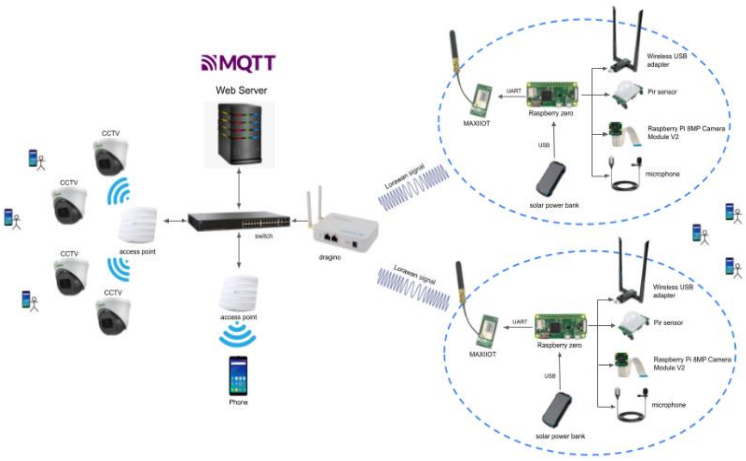

Fig. 3. The proposed framework

Fig. 4 shows the prototype implementation. From outside, it could be seen that the case is metal. The case is designed to be a curve which can be attached with a tree in forest or a pole. There are 3 antennas: one for the LoRaWAN end node and 2 antennas for a usb WiFi adaptor. An example of web page of long-range sensors is shown in Fig. 5. It displays using a corresponding sign and red color for finding an abnormal event. For WiFi sniffer, it will display found MAC addresses.

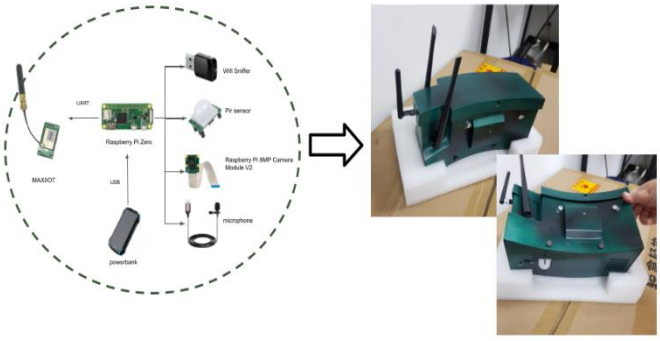

Fig. 4. Long range Sensor

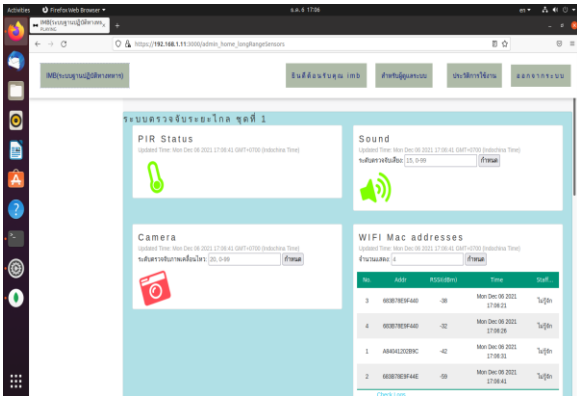

Fig. 5. an example of web page

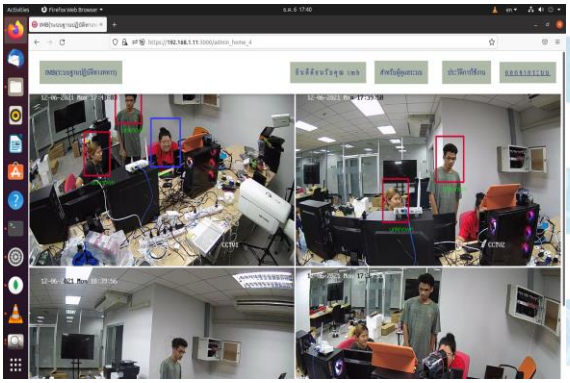

Fig. 7. A web page example of face recognition displaying 4 cameras

C. *Short-range sensors*

Each short-range sensor shown in Fig. 9 consists of a solar cell charger including a 40W-12V battery, a small POE (Power over Ethernet) switch, a CCTV camera and an 23 dBi outdoor access point. The AP is used to communicate to the sever via a receiving access point. The 23 dBi AP is used to extend the communication range to more than 300 meters. The solar cell charger is used to charge the battery to power the short-range sensor for 24 hours per day if there is sunlight at least 6 hours per day. The 5M CCTV camera is used to capture video on daytime and nighttime with 50 meters IR(Infrared). This captured video is streamed to the server for face recognition and person authentication. Current version, face recognition can perform only daytime without mark or balaclava. Example of face recognition web pages are shown in Fig. 6 and Fig. 7.

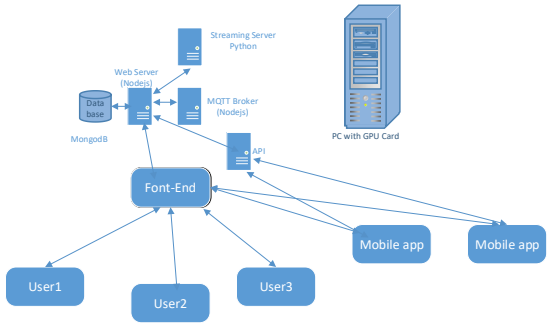

Fig. 8. the server architecture

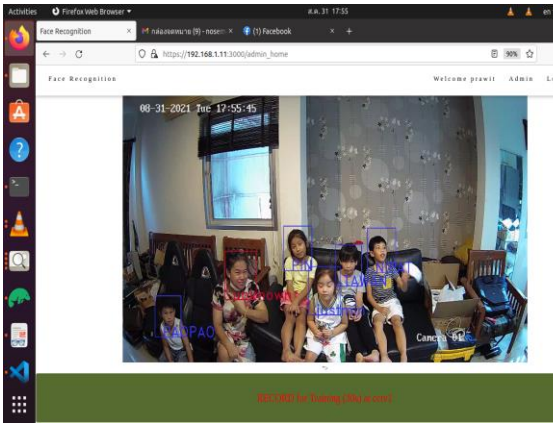

Fig. 6. A web page example of face recognition

D. *The Server*

The server provides a web server, API (Application Programing Interface) and a MQTT Broker. The server architecture is shown in Fig. 8. The web server is provided for web page browsing and video steaming. The API is used for communicating with mobile application. The MQTT Broker is central for publishers and subscribers from LoRaWAN Gateway.

IV. Data Analysis and Abnomal Detection

A. *Data analysis for short-range sensors*

For short-range sensors, CCTV cameras are used. They capture videos and send to the server. The server processes face recognition based on local pre-training faces. The face recognition processes in real-time as shown Fig. 6. The results of face recognition activate sound to a speaker which generate pre-configured sounds: white person, gray person and backlist person.

B. *Data Fusion for long range detection*

For long range sensors, simple algorithm data fusion employed from [5] has been used. each sensor sends a local decision (an abnormal event or a normal event) derived by independent processing of its measurement as described in section III. The data fusion will produce the final output whether it will be alerted or not.

V. Performace Results and Evaluation

Percentage of correction sound detection is more than 95 percent. However, current version, it could not differentiate human sound or not. This feature will be added by using machine learning. In addition, speech recognition and language recognition will be developed.

WiFi sniffer could perform 100 percent if the target device is in radius of 100 meters. However, WiFi sniffer will not apply with new version of mobile phones. This is because they allow mobile phone users select to use randomized MAC address.

Face recognition performs more than 90 percent in range of 5 meters from cameras. However, the pre-training model needs high quality images or videos. For using in southern Thailand, it is quite hard to get high quality of images or video from backlist person. Therefor, pre-training model needs to be further developed.

The correction percentage of PIR depends pre-defined manually setting. In addition, it could not classify between human and other living things such as tigers, bears or boars.

Correction Percentage of motion detection from raspberry pi cameras could be adjusted to 100 percent correction by using web interface to adjust reference images.

Fig. 9 Short range Sensors

Fig. 6 and Fig. 7 show the real-time result from face recognition. Fig. *10* shows the demonstration in the delivery day for using in South Thailand insurgency. The delivery event organized at Sena Narong Camp Military Battalion 42 Station during 21-24 February 2022.

Fig. 10. Presentation for delivering to deploy in the south Thailand insurgency

VI. Technolgy and Innovation Management

In this section, technology and innovation management will be described. After, we finished the first prototypes. The prototypes have been delivered to use in South Thailand insurgency area. The results of the prototypes will be collected and sent to us for developing new versions. While waiting the results from the military, the new version of software has been parallelly developed in a house with 864 square meters land. To get the system is more clever, more real information from field deployment is needed.

The prototype is implemented based on COTS. This leads to easy to implement for commercial products. In addition, the cost of product is low. Therefore, it could be applied for home use as well.

To detect mobile phone identities, mobile phone detection proposal is under review of funding. The main problem of innovation and technology management in Thailand is how to get continuous funds until commercial products are achieved.

VII. Conclusion and Future Works

The intelligent military base (IMB) framework has been designed and implemented. The IMB has features: face detection, abnormal sound detection, motion detection and WiFi mac address sniffer. In addition, for analyzing and logging, the server records real time video, images with names of the detection person and abnormal events. Furthermore, it provides real-time notification by corresponding sounds and web page alerting if there are any abnormal events. The proposed system has been delivered to use in the South Thailand insurgency. Hopefully, they honorably help soldiers to monitor the 3 military bases.

Future works, it could be extended to provide AI-based of intrusion person detection using multi-sensor data fusion. In addition, speech recognition, and low complexity face recognition will be developed for long range sensors. In addition, mobile dispatcher will be used for detecting IMSI and IMEI of person in the interesting area.

REFERENCES

[1] Wikipedia,“ South Thailand insurgency,” wikipedia.org. https://en.wikipedia.org/wiki/South_Thailand_insurgency (accessed Jan. 5, 2022).

[2] T. Bhupathi, A. Chittala, and V. V. Mani, “A Video Surveillance based Security Model for Military Bases,” in *2021 Int. Conf. on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, 2021, pp. 517-522, doi: 10.1109/RTEICT52294.2021.9573572.

[3] S. Chandana, “Real time video surveillance system using motion detection,” in *2011 Ann. IEEE India Conf.*, 2011, pp. 1-6, doi: 10.1109 /INDCON.2011.6139506.

[4] A. Benaskeur, A. Khamis, and H. Irandoust, “Multisensor cooperation in military surveillance systems,” in *2009 3rd Int. Conf. on Signals, Circuits and Systems (SCS)*, 2009, pp. 1-6, doi: 10.1109/ICSCS.2009.5412286.

[5] E. I. Gokce, A. K. Shrivastava, J. J. Cho, and Y. Ding, “Decision Fusion from Heterogeneous Sensors in Surveillance Sensor Systems,” in *IEEE Transactions on Automation Science and Engineering*, vol. 8, no. 1, pp. 228-233, Jan. 2011, doi: 10.1109/TASE.2010.2064305.

[6] Abdelzaher, “Iobt reign cra,” abdelzaher.cs.illinois.edu. http://abdelzaher.cs.illinois.edu/IoBT/index.html (accessed Jan. 16, 2022).

[7] J. Michaelis, A. Morelli, A. Raglin, D. James, and N. Suri, “Leveraging LoRaWAN to Support IoBT in Urban Environments,” in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 207-212, doi: 10.1109/WF-IoT.2019.8767294.

[8] A. Cismas, I. Matei, and D. Popescu, “Condensed Survey On Wearable IoBT Devices,” in *2021 International Conference on e-Health and Bioengineering (EHB)*, 2021, pp. 1-4, doi: 10.1109/EHB52898.2021.9657599.

[9] S. Russell and T. Abdelzaher, “The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making,” in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 2018, pp. 737-742, doi: 10.1109/MILCOM.2018.8599853.

[10] T. Sondrol, B. Jalaian, and N. Suri, “Investigating LoRa for the Internet of Battlefield Things: A Cyber Perspective,” in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 2018, pp. 749-756, doi: 10.1109/MILCOM.2018.8599805.

[11] R. Gupta, K. Nahrstedt, N. Suri, and J. Smith, “SVAD: End-to-End Sensory Data Analysis for IoBT-Driven Platforms,” in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 2021, pp. 903-908, doi: 10.1109/WF-IoT51360.2021.9594944.

[12] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, “Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT,” in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2018, pp. 197-202, doi: 10.1109/PERCOMW.2018.8480255.

[13] P. Gupta and I. O. P. M, “A Survey of Application Layer Protocols for Internet of Things,” in *2021 International Conference on Communication information and Computing Technology (ICCICT)*, 2021, pp. 1-6, doi: 10.1109/ICCICT50803.2021.9510140.

[14] D. L. Hall and J. Llinas, “An introduction to multisensor data fusion,” in *Proc. of the IEEE*, vol. 85, no. 1, pp. 6-23, Jan. 1997, doi: 10.1109 /5.554205.

[15] Wang, Defu, Shibao Zheng, and Chongyang Zhang. “Real-Time Human Intrusion Detection Using Audio-Visual Fusion.” in *Advances on Digital Television and Wireless Multimedia Communications*. Springer, Berlin, Heidelberg, 2012, pp. 82-89.

[16] R. Gupta, K. Nahrstedt, N. Suri, and J. Smith, “SVAD: End-to-End Sensory Data Analysis for IoBT-Driven Platforms,” in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 2021, pp. 903-908, doi: 10.1109/WF-IoT51360.2021.9594944.