



## MANAGEMENT OF BORDER SECURITY USING IOT TECHNOLOGY

**Jayantee N.  
Bhalerao**

**ABSTRACT**

In the modern world the intelligent systems with wireless connectivity are used extensively. These intelligent systems are widely used to connect, discuss, demonstrate, control, operate, etc. The IOT (Internet of Things) is a reliable and secure technique. Moreover it can be remotely monitored and controlled. This technology can be used as an important tool to guard our border areas. Infiltration is a big threat today. This protection mechanism notifies the designated center giving a clear picture of the scenario happening at the borders. Various sensors with active cameras, GPS system and wireless secured internet can be used to monitor any infiltrations. In case of any suspicious activity the weapon systems can be activated remotely to control such infiltrations. This way we can save the valuable life of our brave soldiers. To secure our borders, we can have PIR sensors and GPS enabled wireless intelligent cameras along with automated weapon systems at border areas. These systems can be connected wirelessly to the control stations. The monitoring and analysis of the signals can be done at control stations. The signals received from sensors and cameras can be resolved using GPS with the help of geo-tagging, photo mapping techniques and software. In case of confirmation of infiltration or trespass the automated weapon systems can provide the geographical coordinates. It can further be guided to fire and control the malicious activity. This way machine to machine communication can help to reduce a major threat to our country. This will help in controlling the infiltration without the life threat to our soldiers.

**KEYWORDS :** IOT; PIR Sensor; GPS Enabled Camera; Geo-Tagging; Photo Mapping**INTRODUCTION:**

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors. It takes advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities, which were not previously possible. There are number of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT Revolution". There are concerns about security, privacy, and technical interoperability of such technologies.

Today our major concern is the security of the borders of our Nation. These borders are guarded by our soldiers. These soldiers encounter threat to their lives due to infiltrations (1), Cross Border Terrorism, Drug Peddlers, etc. During the process to secure our Nation from these malicious elements they make supreme sacrifice. Till date we have lost countless brave and decorated soldiers. They were gallant and heroic enough to lay their lives on the battlefields. But the losses to the nation were permanent. If we could have saved half of these lives, we would have an even mettlesome force. This may not have been possible in the past wartimes, but today the scenarios are changing. We are advancing to a technological more dexterous globe. We can now save the valuable lives of our soldiers that guard our borders. They no more have to risk their lives.

Terrains like valleys, rivers, hilly areas, fissures, etc., which are comparatively difficult to guard and where it is more likely for our soldiers to lose their lives and meet martyrdom can now be stopped because of the IOT based technology.

Advanced situational awareness allows today's military personals to make decisions based on real-time analysis. This can be done by integrating information received from watch towers, unmanned sensors, reports from the field, interception of messages and other such sources. These commanders benefit from a wide range of information if it is supplied by sensors and cameras mounted on ground. These devices can survey the mission landscape and feed data to a forward base, some or all of which may be relayed to a command center (2), where it is analyzed and integrated with data from other sources to enable comprehensive battlefield situational awareness. Commanders then can make decisions based on that data, and the task of eliminating the threats on the front lines can be executed by automated weapons. Thus we can save the lives of our most valued soldiers.

**OBJECTIVES:**

- Defending the difficult terrains from infiltration in safe and secure manner.

- Monitoring, Sensing and identifying the human infiltration.
- Analyzing data and images along with the Coordinates of the exact location.
- Utilization of automated weapons to eliminate the threats at borders.
- Facilitation of modern technological infrastructure at Border areas.

**SCOPE OF WORK:**

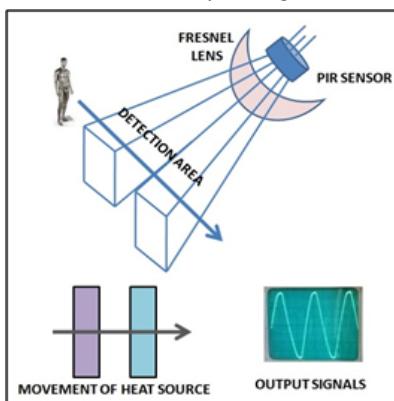
Gorges, Valleys, River beds, muddy areas, fields with high grass, etc., are comparatively difficult to protect. The terrain here is tiresome and risky. Therefore, chances of infiltration through such border areas are very high. Defending these boundaries lead to loss of the lives of our brave soldiers. Thus in such cases it will be very revolutionizing to be able to sit and guard from a safe distance without the threats to the lives of our soldiers.

To achieve this we propose to use Wireless PIR (3) Human Body Detecting Sensors, GPS enabled cameras and automated weapon system (WiFi enabled) and Secured Connectivity (4). At places Microwave detection (5) system can also be used.

**Pyro-electric (Passive) Infra-Red (PIR) Sensors:**

PIR sensors allow sensing thermal radiations emitted by human body, motion, infrared radiations. These pyroelectric sensors detect levels of infrared radiation (6). These are mostly used to detect human crossing the range of the sensor.

They are small, economic, consumes very low-power, easy to use and robust. We are aware that everything emits some low level radiation. The hotter elements like human body emit higher radiations.



**FIG 1.0 PIR Sensor showing Detection Technique**

The sensor detector is actually split in two halves. Firstly it detects the thermal radiations. Whenever, a warm body like a human passes by, it first intercepts one half of the PIR sensor. It causes a positive differential change between the two halves. When the warm body leaves the sensing area, the reverse action takes place. The sensor generates a negative differential change. The mapping relationship between the sensed waveform and multiple influencing factors is established, and a group of mathematical models are deduced which fuse the macro factors and micro factors. The detected changes in the pulses can be analyzed for human infiltration. Whenever such a differential waveform is obtained at the base station, an infiltration can be confirmed.

#### **GPS ENABLED CAMERA:**

These are high resolution cameras having fairly good coverage range. Along with the images (7) we require several other inputs like, the coordinates of the object, Altitude, Distance from the Camera, Direction (Compass heading) of the object. All such information are provided by these cameras.

The 3D (7) compass and Altimeter provides the direction and altitude. The Geo-tagged cameras with the help of GPS inbuilt module in the camera, provides the coordinates of the object. The True Pulse laser range finder provides the distance of the object from the camera. The photo mapping module and geo-tagging helps to generate report templates for quick dissemination.

#### **CONNECTIVITY:**

All these devices, viz., the PIR sensors, GPS enabled cameras and the automated weapons will all have Wi-Fi cards. These will be connected to a tower. The devices will have a secure point to point connectivity with the server. The data will be transmitted in an encrypted manner with highly secured mechanism.

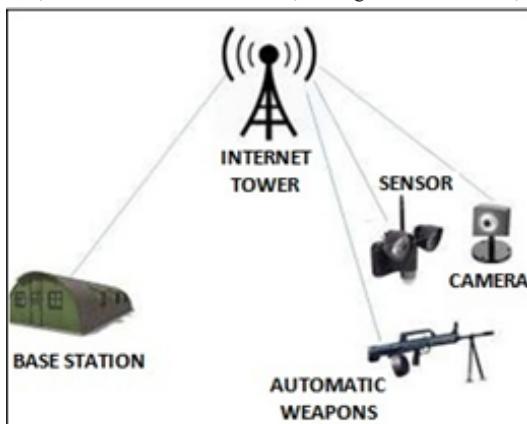
This way, all our devices can be well connected to the base station. We can therefore have an effective surveillance as all the data collected from our various devices can be analyzed at the base stations for further processing. The decision taken based on analyzed data can be transmitted back to the weapon system or troupes for necessary actionable.

#### **METHODOLOGY:**

We need to create infrastructure at the base station to monitor and analyze the system. It includes computers, redundant networking equipments, security systems, software, firmware, etc. Secured Wi-Fi connectivity infrastructure should be in place.

The locations in the difficult terrains will have to be searched and fixed for fixing the cameras and sensors. Then these will be installed at these prefixed locations. There after these cameras and sensors will be configured remotely. The automatic weapon system will also be fixed in respective locations. These weapon systems will be connected wirelessly to the base system remotely. Testing of these items should be done before commencing the operation.

Now a continuous monitoring can be done at the base station. The data transfer will be done securely in encrypted format. We can have alerts for the security threats of the data. For any physical instances at the borders, we can have alerts like alarms, messages to commanders, etc.



**FIG 2.0 Schematic diagram of equipments and connection**

If any malicious instance diagnosed by the camera or sensors or both (3, 8), appropriate analysis can be done at base station. On confirmation of an infiltration or malicious attempt necessary instructions can be issued to weapon systems or the troupes. The weapon systems can be triggered remotely (3, 6) to control the illegal; activity or the troupes can be deployed with proper information of the enemy.

This system will help in providing accurate information about the exact location of malicious activity. The infiltration efforts can be neutralized without compromising the lives of the soldiers.

#### **FUTURISTIC APPROACH**

The technology is also useful in the naxal affected areas. There also we find difficult terrains and challenges like we have at borders. In attacks like Pathankot airbase, where we had to search for the hidden terrorists, we can use hand held versions of such equipments. In attacks like Taj hotel, hand held devices with such technology may help in searching the terrorists in closed rooms. We can make need based advancements in the equipments. The concept presented here with modern equipments will help to make safe and secure Nation. There are possibilities of using some other techniques and models (5, 9) to hunt such threats.

#### **CHALLENGES:**

There are various challenges to deploy such system. As we need to purchase such system from advanced countries, we need to have all information about the equipments. The terrains will place challenges in fixing and maintaining the systems. Security threats to the IT system will have to be addressed properly. Data transmission should be done highly secured manner. In case of any breach, the data should be destroyed. A proper analysis is a must. We should be able to discriminate between friends and foes, before taking any decision.

#### **CONCLUSIONS:**

Security of the Nation is a prime concern. But at the same time, the lives of men safeguarding the borders must be protected. Warfare does not depend upon manpower only. The advancements in technology are quite helpful in providing the security without causing threat to the soldiers. The modern day technology and equipments will have to be deployed in a smart manner.

The concept mentioned above not only secures borders effectively, but also avoids life threats. We need to adopt such techniques and check the loopholes at border areas due to difficult terrains. However, this amalgamation of technologies needs further investigation and refinement for an efficient management of borders.

#### **ACKNOWLEDGEMENTS:**

The author is grateful to Dr. Mahesh D Goudar, HOD (ETX), Mr. S A Khandekar and the teaching staff of MIT Academy of Engineering for their constant encouragement. The author is also thankful for the support from her lab-mates at MIT Academy of Engineering, Alandi, Pune (MS)

#### **REFERENCES:**

1. Aishwarya D, Dr J Arokia Renjith, Enhanced Home Security Using IOT and Raspberry, IRJET, 2017, Volume: 04 Issue: 04, 3155-3158.
2. Chou Wusheng, Wang Tianmiao, You Song, "Sensor-based autonomous Control for telerobotic system", Proceedings of the 4th World Congress on Intelligent Control and Automation, 2002, vol.3, pp. 2430 -2434.
3. Research on the Multiple Factors Influencing Human Identification Based on Pyroelectric Infrared Sensors, Junwei Yan, Ping Lou, Ruiya Li, Jianmin Hu, and Ji Xiong, 2018, 604.
4. Miyama, S.; Imai, M.; Anzai, Y.; "Rescue robot under disaster situation: position acquisition with Omni-directional video footage sensor detection and robot movement Intelligent Robots and Systems, IROS, 2003, vol.3, pp. 3132 -3137.
5. Kun-Muchen, Yong Huang, Jianping Zhang, Narman A. "Microwave Life-Detection System for searching Human subjects under Earthquake Rubble or behind Barrier", IEEE Transaction, Biomedical Engineering, 2000, volume 27, pp 105-114.
6. Saeed Moradi, "Victim detection with Infrared Camera in a Rescue Robot" IEEE International Conference on Artificial Intelligence System, 2002.
7. T. J. Fan, G. Medioni, & R. Nevatia, "Recognizing 3D objects using surface descriptors," IEEE Trans. On PAMI, 1989,L, Vol.41, No. 11,
8. M. Snoka, V. Hlavac, & R. Boyle, "Image processing, analysis and machine vision," Chapman & Hale Computing Great Britain, 1993.
9. Mata et al. "Object learning and detection using evolutionary Deformable models for mobile robot navigation", ROBOTICA, Cambridge University Press, 2008, vol. 26, pp. 99-107.