Research Article

Wireless Intruder Detection System for Remote Locations

[1]Mrunal Khedkar, [1]GajendraAsutkar, [2]R.Hariprakash

[1]Priyadarshini Institute of Engineering and Technology, Nagpur, 440019, Maharashtra, India
[2]Bharat Institute of Higher Education and Research Chennai, 600073, India
Email: mrunalkhedkar@scholarpiet.com, rhp_27@ieee.org

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract—
At remote locations where mobile networks are not present and remote sensing cannot provide enough information, an ad-hoc network with rechargeable nodes can be implemented. This paper discusses an ad-hoc network of camera based wireless intrusion detection system. In the proposed system each node has been implemented using a motion sensor, digital camera, transmission module, and solar-powered battery. Function of every node is to continuously monitor the occurrence of any intrusion in its range by using a motion detection sensor. The motion sensor triggers the digital camera only when the intrusion occurs. After triggering, camera gets switched on instantaneously and starts capturing the visual data. This recorded visual data is transmitted serially to the base station using Zigbee or Bluetooth transmission module. At the base station, the received information is decoded to obtain visual data. For keeping track of all nodes present in a network, the battery voltage level is also transmitted from each node to the base station at fixed time intervals. Various image parameters are calculated and the energy efficiency of the system is also evaluated at the base station. It is found that the wireless intrusion detection system presented in this paper is reliable and energy efficient.

Keywords: Bluetooth, Zigbee, Motion sensor, Open MV Cam, Wireless sensor network

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a type of ad hoc network consisting of sensor nodes connected to base station. Each node contains a sensor, processor, trans-receiver and battery. These nodes sense the surrounding environment and transmit the report to the base station. The life-time of WSN depends upon the average life-time of its nodes. WSN nodes mostly monitor the scalar data like temperature, pressure, humidity etc. The base station receives data from each node in the network connected to it. Distinct wireless technologies can be used to transmit the data depending upon the distance between nodes and base stations. Base stations can transmit data further to other networks or over the internet.

Now-a-days, security has become a prime issue in all spheres of life. Different security application systems are developed to provide security for homes, hospitals, market places, etc. Presently continuous monitoring camera systems are deployed everywhere to monitor the area continuously. The biggest disadvantage of continuous monitoring is that it captures the data continuously and hence lot of redundant data is generated. It is very difficult to store such huge data and to process it further for extracting the required necessary information. Thus event-based capturing of visual data provides a solution for the above problem.

Previously carried out research work on camera-based intrusion detection system generally uses different image processing techniques like frame differencing [1], background subtraction, etc. Some intrusion detection systems which do not have a camera can detect intrusion using either Wi-Fi signals [2] or Passive InfraRed (PIR) sensors [3]. The proposed method in this paper is event-driven that captures and transmits visual data. This visual data consist of photo or video. Different wireless transmission technologies can be used in this system depending upon the distance between node and base station. For nodes placed near to base station, Bluetooth can be applied and when nodes are away, Zigbee is used. As solar energy is abundantly available in India for most of the time in a year, the solar panel with a rechargeable battery is the best alternative to any conventional power source. The solar powered node based system discussed in this paper is more appropriate for remote locations as it has a long life-time and power dissipation is low.

This paper contains the following sections: Section II discusses the related work performed in an area on intrusion detection. Section III explains the intruder detection system. In Section IV, image

parameters are evaluated. Section V evaluates the energy efficiency of a system, followed by conclusions in Section VI.

2. RELATED WORK

A. Mishra *et al.* [4] propose artificial neural network (ANN) based border intrusion detection by using WSN. Light and sound data sensors are deployed and ANN is trained using this data. Y. Jin, *et al.* [5] provides a home-level intrusion detection system. This system uses the Received Signal Strength Indicator i.e. RSSI of Wi-Fi signal to detect the intrusion. S. K. Roy, *et al.* [6] proposes a Zigbee-based agriculture intrusion detection system. WSN consisting of Passive Infra-Red (PIR) and ultrasonic sensors are used to detect the motion and position of the intruder in the field. Y. Gu, *et al.* [7] present an RF-based device-free motion detection system named Mo-Sense that works on commodity Wi-Fi devices. Motion is detected when Wi-Fi signals present everywhere are attenuated. Thus it's a transparent and real-time system. T. Choubisa *et al*. [8] paper describes the challenges faced during the deployment of PIR sensors-based nodes of WSN in any outdoor environment.

K. C. Sahoo and U. C. Pati [9] developed PIR sensor-based intruder detection system using the Zigbee module. At the base station, the microcontroller interprets the signal and sends a text message to the concerned person by using a GSM module. D. ALshukri *et al*. [10] propose an intelligent border area intrusion detection system that uses a thermal imaging camera (FLIR) to detect the intrusion of objects or persons. Spotlight with infrared and laser gun is also present to illuminate the area under different conditions. C. Pham [11] proposed multi camera-based wireless intrusion detection system based on a criticality-based scheduling approach used to integrate all the camera sensor nodes. Each camera uses pixel-based image differencing to detect the intrusion. R. Singh and Gajendra Asutkar [12] presented a survey paper that discusses the various methods for monitoring and tracking wild animals in the forest using wireless sensor networks and GPS systems.

S.K. Mohapatra *et al*. [13] proposed a big data analytic architecture to analyze the vast data generated from camera sensor nodes. These nodes can move and rotate individually and form a barrier to detect the occurrence of an intruder in the monitored area. J. L. Raheja *et al*. [14] present across border intruder detection systems using kinetic sensors. These sensors extract only the skeleton from full-frame and this feature is explored and further classified using a neural network. Seung Hyun Kim *et al*. [15] designed an intrusion detection system to protect the nuclear power plant. A virtual fence is set up using these nodes and neural network-based classification is used. Lee *et al.* [16] paper illustrate an outline of video wireless sensor networks in which Quality of Service (QoS) is evaluated based on parameters such as allocated energy, capture rate, and transmitted power. These parameters are optimized to improve QoS and the network is said to be energy efficient.

From the previous work done in this area, it is observed that PIR sensors are widely used for motion detection as they are cheap, robust, and reliable. PIR is a low-power device that can detect intrusion even in the dark. Most of the intruder detection systems use only PIR sensors. Though this motion detection technique does not require any processing at the node, it also does not provide any idea about the type of intruder. Few researchers have used only cameras for intrusion detection by using image processing techniques like frame differencing, background subtraction, edge detection, etc. Video camera-based motion detection techniques [17] [18] require more power, continuous processing, and proper illumination conditions. From most of the research carried out in this area, it can be observed that a low-power camera-based intrusion detection system has not been implemented.

The proposed system in this paper overcomes the previous research work drawbacks by providing a complete solution for energy-efficient intrusion detection at remote locations.

3. INTRUDER DETECTION SYSTEM

3.1 System Architecture

The wireless network is made up of base stations and nodes spread over in the surveillance area. All the nodes are connected simultaneously to a base station in a star topology. Each of the nodes acts as a solar-powered standalone system. These nodes can be placed at various key locations in a monitored area [19]. If any one of the nodes senses motion, it captures the video / photo and transmits this video data serially [20] over the wireless network to the base station. When there is no motion, the digital

camera remains non-functional. At the base station, the serial data is received using a serial terminal and decoded back to obtain the video / photo. The visual data further helps to predict the activity and behaviour of the intruder in detail.

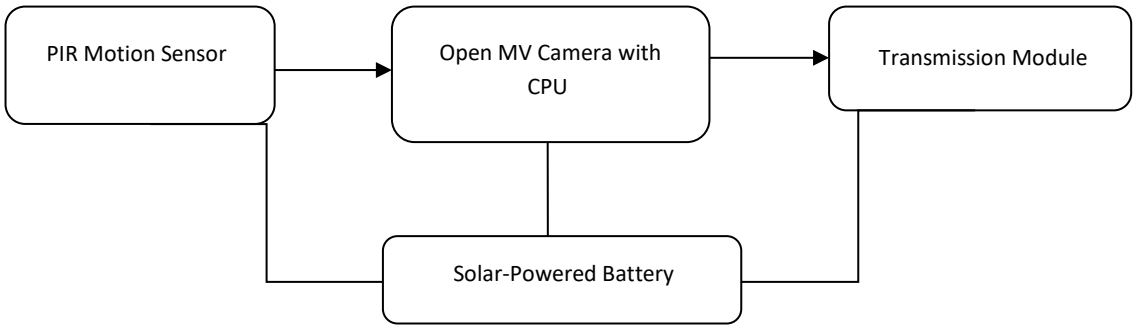


Fig 1 Node architecture

Fig 1 shows the node architecture, which consists of the PIR sensor, Open MV M7 Cam module with an embedded processor, transmission module, and solar-powered battery. PIR sensor is used for motion detection, whose output is connected to the input of the Open MV M7 Cam module. The output of Open MV Cam is connected to the input of the transmission module, which connects the node to the base station wirelessly. These three modules are powered using rechargeable batteries connected to solar panels. All the nodes connected in the WSN have a similar architecture, while the type of transmission module can be different.

3.2 Node Implementation

Fig 2(a) shows the outer view of a hardware implementation of a WSN node that can be mounted at any required location. Fig 2(b) shows the internal node circuit, which is made up of Open MV M7 Cam with inserted SD card, PIR sensor, Hc-05 Bluetooth transmission module, battery, and solar panel. These nodes can be used to monitor areas within the range of 10 meters from the base station. Fig 2(c) displays the internal circuit that comprises Open MV Cam with inserted SD card, PIR sensor, Zigbee S2C transmission module, and solar-powered battery. These nodes can be used to monitor the area in the range of 10 to 100 meters from the base station.

Open MV Cam module is a python based, low-power machine vision module. This module has a camera integrated on a small board that runs on the Micro Python operating system. It has an inbuilt OV7725 image sensor, ARM Cortex M7 processor, which runs at 216 MHz and has 512KB of RAM with 2 MB flash memory. It needs to be programmed using the Open MV integrated development environment. A micro SD card that is placed in its socket capable of 100Mbs reads/writes due to which Open MV Cam can record video. It is expandable by attaching shields to create a customized circuit. A major advantage of this module is that it turns on instantaneously when the signal is received.

PIR sensors are used for motion detection [21]. These sensors are low-cost, low power, small-sized, and thus suitable for WSN. All objects emit infrared (IR) radiations, and the PIR sensor can measure them for objects in their field of view. The term passive indicates that PIR devices neither produce nor radiate any kind of energy for sensing the environment. PIR can sense the changes in the amount of infrared radiation, which differs based on temperature, surface characteristics of the objects as well as the distance between object and sensor. If any object passes in front of the stationary background, temperature change occurs at that point. PIR sensor detects this variation as a change in radiations and gives an output that signifies motion detection.

Fig 2(a) Wireless node

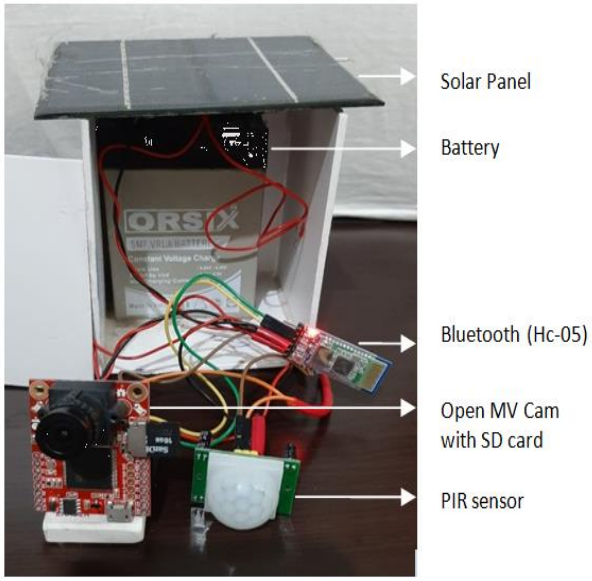


Fig2(b) Wireless node internal circuit using Hc-05

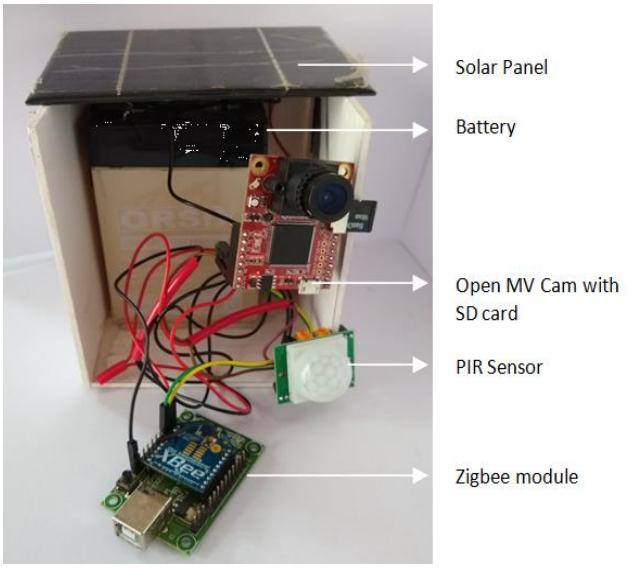


Fig 2(c) Internal circuit of WSN node using Zigbee S2C

Bluetooth wireless technology operates on IEEE 802.15.1 protocol. Here Hc-05 Bluetooth module is used, which has a short-range of up to 10 meters and wireless transmission depends upon the atmospheric and geographical conditions. Hc-05 is a serial communication device that serially transmits the data to the base station. Zigbee modules are used for long-range as compared to Bluetooth modules. Zigbee is a secure, reliable, cheap, low data rate and low power network protocol based on IEEE 802.11.04 standard. It can cover a range of up to 100 meters for a direct line of sight. Zigbee is suitable for infrequent, low-power serial data transmission.

A simple 6V, 4.5Ah lead acid battery connected solar panel is used to power up the circuit. This battery is used because of its easy availability, has higher cell voltage, and lower cost. This battery is connected to the node circuit via voltage regulator IC7805 for getting the constant output voltage. The battery is recharged by using a solar panel mounted at the top of the node. Solar-powered battery thus helps to increase the life-time of the node, which in turn extends the life of the entire network.

4. SYSTEM FUNCTIONING

Fig 3(a) shows the flowchart for the WSN node. When the node is turned on, the PIR sensor immediately starts to monitor the area in its range continuously to detect an event. Event is defined as the occurrence of motion of any object in the given area. PIR sensor generates a signal whenever a motion is detected in its range. This signal turns on Open MV Cam instantaneously and it starts capturing the video / photo with the help of a Micro SD card mounted on the Open MV Cam module. Captured visual data is first saved in the SD card and then converted to serial format. This data is further transmitted serially to the base station through the transmission module. When the motion does not occur, live value of battery voltage is transmitted. As the visual data is saved before transmission at node end, the data can be recovered from the node, if any frame loss occurs during transmission. All the nodes consume low power as the redundant data is not captured due to event detection. Open MV Cam present in the system uses VGA (Video Graphics Array) digital image frame format for capturing gray scale video or gray scale snapshot. The frame size can be varied, if required. If the frame size is increased, the number of bytes transmitted will increase, which will enhance frame quality, but more time and energy will be required for transmission. Thus the tradeoff between frame quality and transmission time needs to be decided depending upon the specific application of intrusion detection system. Open MV Cam is programmed such that it reads the pin input obtained from the PIR sensor.

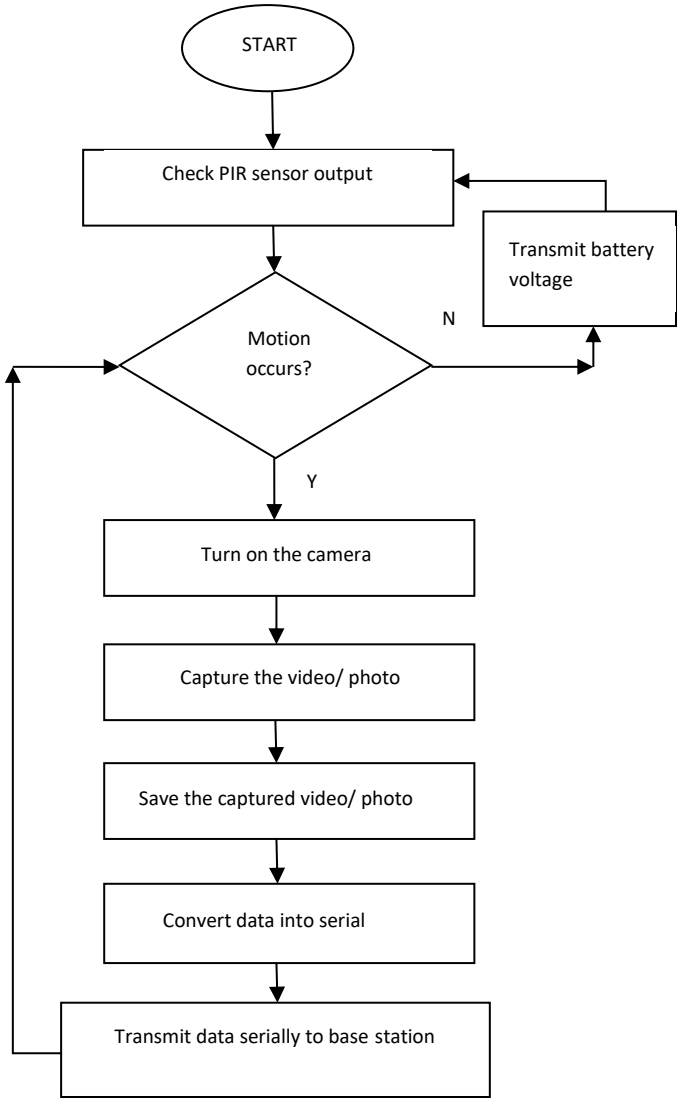


Fig 3(a) Flow chart for WSN node

When the Open MV pin connected to PIR reads 1, Open MV will capture and transmit the video / photo. If it reads 0, Open MV measures the battery voltage and transmits it. UART transmitter terminal of Open MV is connected to the receiver terminal of the transmission module. UART receiver terminal of Open MV is connected to transmit terminal of the transmission module. These pin connections are similar for both the transmission modules (Zigbee or Bluetooth) for serial data exchange. The Baud rate for the Bluetooth module is fixed at 9600 bps and for the Zigbee, transmission module is set at 19200 bps.

For Zigbee S2C module, three different baud rates: 9600bps, 19200bps and 38400bps are compared. At each baud rate, frame delay and frame loss are calculated by transmitting similar video 10 times from node to base station. It was observed that as the baud rate is increased from 9600bps to 38400bps the frame delay is reduced but the frame loss occurs at 38400bps. Frame loss does not occur at 9600bps and 19200bps. Thus 19200bps is a reliable baud rate as frame delay is less as compared to 9600bps and frame loss is prevented.

Table 1: System parameter specification

Parameters	**Specification**
Frame size	160X120 (QQVGA)
Video format	Greyscale
Baud rate	9600 bps (Hc-05), 19200 bps(Zigbee)
Transmission range	10 m (Hc-05) 100 m (Zigbee)
PIR range	10m

Table 1 shows the system parameters and their specifications. These specifications include digital image frame size, format for video, baud rate for serial transmission. Fig 3(b) shows the flowchart for the base station where received data is processed. Zigbee module or Bluetooth module connected at the base station receives data from the serial input terminal. Received data is converted back into frames and displayed. If the received length of bytes is less than 52900, it means frames are not present. During this time battery voltage is displayed. Finally, different image parameters are evaluated to find out and improve the quality of received image frames.

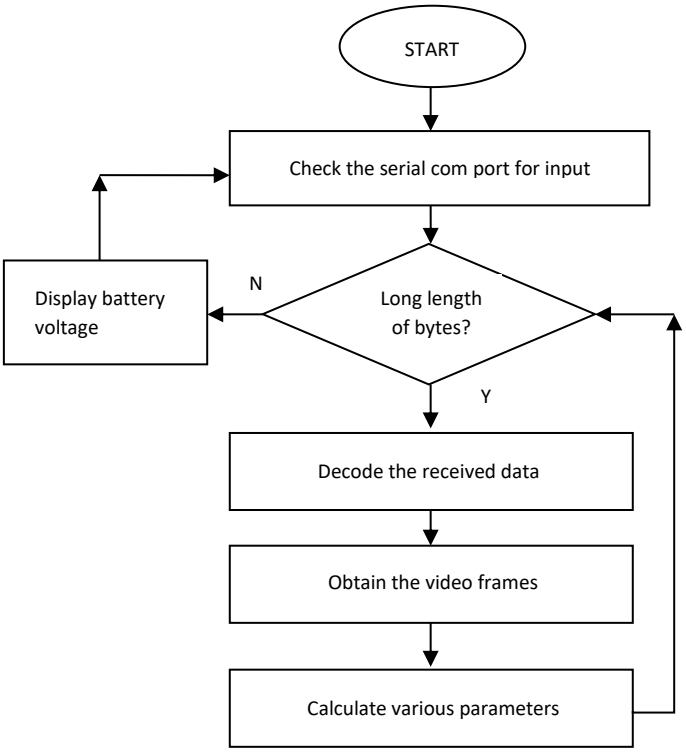


Fig 3(b) Flowchart for base station

To display received serial data, here X-CTU is used as shown in fig 4. For displaying the data received, a separate X-CTU terminal needs to be opened for each node as every node is connected via a different com port. The baud rate of the respective node also needs to be specified.This X-CTU terminal is also used to configure the Zigbee modules as transmitters or receivers. The baud rate for the Zigbee receiver module is set at 19200 bps. Hc-05 Bluetooth transmission module is by default configured in data mode, which enables data exchange. The baud rate for the Bluetooth receiver module is set at 9600 bps. The Hc-05 module is used as the node end as a transmitter and the in-built Bluetooth of the computer is used at the receiver end in this system. If in-built Bluetooth is not present at the base station, then the Hc-05 module is connected to the base station and configured as a receiver.

Serial data received at the base station is displayed in the HEX form, as shown in fig. 4. Transmitted image frames from the node end are shown in fig 5 (a, b). Corresponding decoded frames at the receiver end are shown in fig 6 (a, b). These frames are converted into a video, which can be further analyzed or transmitted, as per the requirement. To keep track of all nodes in the network, the measurement of the battery voltage of each node is sent to base station at regular intervals from the node end. This helps to check the live battery status of all the nodes. If any battery related issue occurs, then it can be easily figured out.

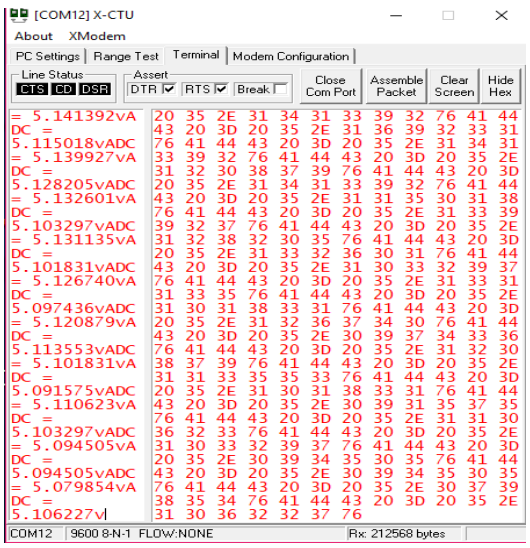
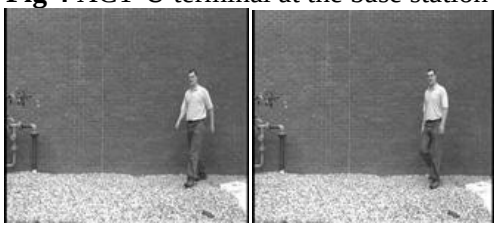
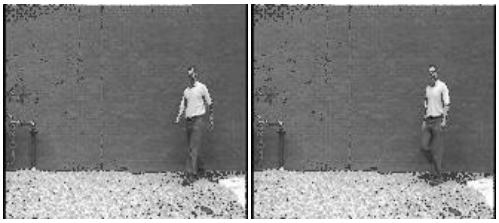


Fig 4 XCT-U terminal at the base station



(a) (b)

Fig. 5 Transmitted frames



(a) (b)

Fig. 6 Received frames

5. IMAGE PARAMETERS

Image parameters are used to find out the quality of the received image as compared to its corresponding transmitted image. For the above system, different image parameters [22][23] are calculated such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index (SI). These parameters for eight different frames are listed in Table 2. These parameters also show the level of distortion in the received image [24]. These parameters are defined as:

5.1.Mean Square Error (MSE)

It is the progressive square of the error between the transmitted image and the received image.

$$MSE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\{T(i,j) - R(i,j)\}^2 \qquad (1)$$

Where *T(i,j)* is the transmitted image, *R(i,j)* is the received image, and the dimension of the image is *M X N*

5.2. PEAK SIGNAL TO NOISE RATIO (PSNR)

In this system, the transmitted image represents a signal, and transmission losses represent noise. This ratio of signal to noise displays the quality of the received image.

$$PSNR = 10\log_{10}\frac{Max_0^2}{MSE} \qquad (2)$$

Here, Max_O *i*s the maximum value of pixels in the given image, every pixel constitutes 8 bits, therefore $Max_O = 2^n - 1 = 255$, n is bits per pixel.

5.3. STRUCTURAL SIMILARITY INDEX (SI)

Total error among images and received images is given by MSE and PSNR. But SI measures the deterioration in structural information for a received image concerning the transmitted image. Thus SI gives the similarity among these two images. The value of SI varies from 0 and 1. For two perfectly similar images, the value of SI is 1. The value of SI lowers when dissimilarity increases and becomes zero when two compared images are dissimilar.

$$SI(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \qquad (3)$$

Here *x* is the transmitted image of size *NXN* and y is the received image of size *NXN*. μ_x and μ_y is the average value of x and y, respectively. σ_x^2,σ_y^2 is the variance and σ_{xy} is the covariance of x and y, respectively.

All the above image parameters are calculated and listed in Table 2. These image parameters are evaluated based on the transmitted video frames by Open MV Cam, as shown in fig 5, to the received video frames at the base station as shown in fig 6. The average value of MSE is found out to be 17.6295, an average value of PSNR is 23.2642 and the average value of SI is 0.6701, which is largely acceptable.

Table 2: Image parameters

Frame No.	**MSE**	**PSNR**	**SI**
Frame 1	17.410933	23.314363	0.667947
Frame 2	17.216250	23.412032	0.671006
Frame 3	13.180174	25.732381	0.827747
Frame 4	19.022785	22.545322	0.631642
Frame 5	19.084111	22.517365	0.628116
Frame 6	16.749896	23.650561	0.681712

Frame 7	19.146226	22.489140	0.628358
Frame 8	19.225787	22.453121	0.624357

6. ENERGY-EFFICIENT SYSTEM

When the image / video is not being transmitted, the voltage level of battery from each node is transmitted to the base station continuously at fixed time interval. This helps in energy monitoring of the system and identifying the dead nodes present, if any. A single node is considered for energy monitoring. Each component of the node circuit is powered by using 6V, 4.5 Ah batteries. For evaluating the energy efficiency of the system, a fully charged battery is connected to the circuit without solar cells, and energy is monitored for one life cycle of the battery. The circuit is switched on and monitored constantly. Fig 7 shows the battery voltage that drops continuously along with time. Fig 8 shows the power dissipation of the node circuit that remains almost constant with time. Fig 9 displays the energy consumed by the node circuit that increases with time. It is observed that the circuit can run for nearly 35 hours before the battery dies out and power dissipated is nearly 552mW (milliWatts) and energy consumed is about 20Wh (Watt-hours). Battery voltage is measured in volts and circuit current in milliamperes. These values demonstrate that it is low power and energy-efficient circuit. This circuit is more suitable for remote locations, as it can work for more than a day even if the weather is cloudy and sufficient sunlight is not available to recharge the battery. To prolong the life of this circuit for few more days under such cloudy weather conditions, a more powerful or higher rating battery has to be applied.

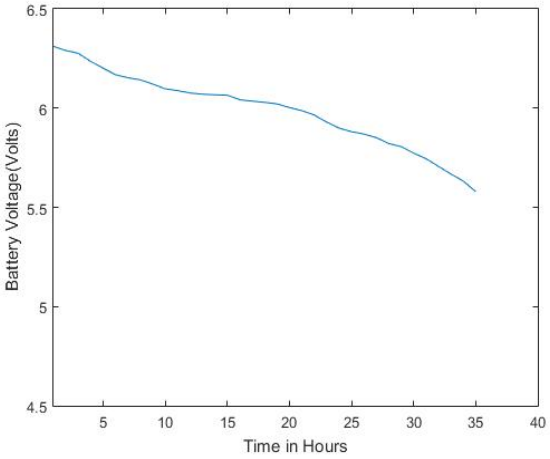


Fig.7 Battery Voltage

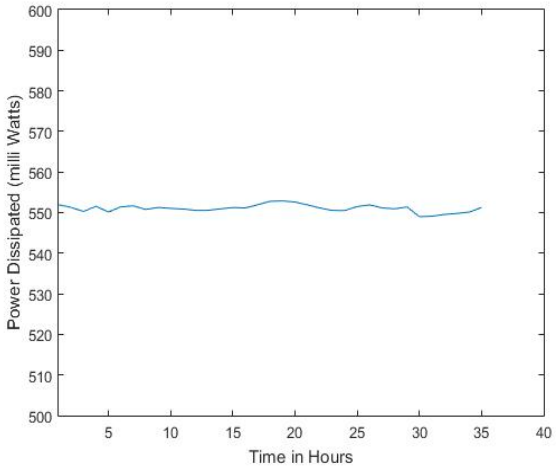


Fig.8 Power Dissipation

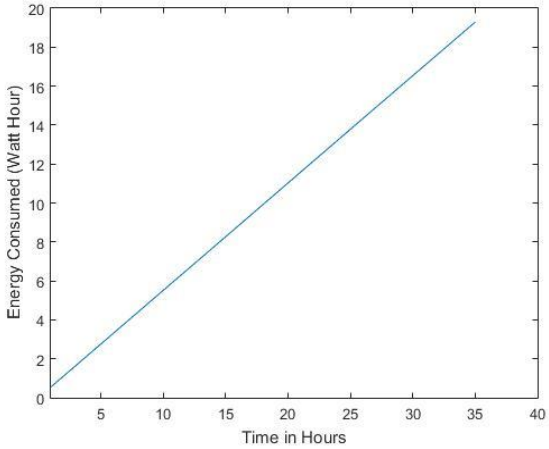


Fig. 9 Energy Consumed

7. CONCLUSION

The wireless intruder detection system presented in this paper is an embedded system consisting of low power standalone nodes connected to the base station. As nodes being solar-powered, this system is suitable for remote locations. The uniqueness of this system lies in avoiding redundant data and identifying dead nodes, if any. This energy-efficient system is combination of Open MV cam with PIR sensor and transmission module. Each node performs motion detection by using a PIR sensor and captures the video/photo by Open MV cam only when the motion occurs. This video/photo of an intruder is transmitted from node to base station serially by using a transmission module (Bluetooth / Zigbee). For nodes in short range of up to 10m, Bluetooth hc-05 module at baud rate of 9600bps is used. From 10m to 100m range Zigbee S2C module is applied inside the nodes at 19200bps, as this baud rate provides reliable transmission without frame loss. At the base station data from all the nodes is received, decoded and evaluation of image parameters is carried out to check the quality of received visual data. It is done by comparing transmitted image frames from nodes with received image frames at the base station. The average value of PSNR is found to be 22.264 and the average value of SI is obtained as 0.670. These values confirm that resultant quality of visual data obtained at the base station is up to the mark for serial data transfer. From an energy monitoring point of view, the circuit is found out to be energy efficient as the average power dissipation is 551.23 m-Watts and the total energy consumed by the circuit is 19.286 Watt hrs. This wireless intruder detection system is reliable and optimizes the power required for transmission.

REFERENCES

1. R. Hariprakash, S. Ananthi, and K. Padmanabhan, "An economical wireless network monitored scheme for camera-based intrusion detection at unattended sites," 2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE), Penang, 2011, pp: 150-155. https://doi.org/10.1109/ICCAIE.2011.6162122
2. J. Lv, D. Man, W. Yang, X. Du, and M. Yu, "Robust WLAN-Based Indoor Intrusion Detection Using PHY Layer Information," 2018 *IEEE Access*, Vol. 6, pp: 30117-30127,.https://doi.org/10.1109/ACCESS.2017.2785444
3. S. Bhagat, C. P. Kothari, V. Bapat, and V. Kulkarni, "Classification and determination of physical intrusion using Wireless Sensor Networks," 2015 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Denton, TX, 2015, pp: 1-5. https://doi.org/10.1109/ICCCNT.2015.7395165
4. A. Mishra, K. Sudan and H. Soliman, "Detecting border intrusion using wireless sensor network and artificial neural network," 2010 6th IEEE International Conference on Distributed Computing in Sensor Systems Workshops (DCOSSW), Santa Barbara, CA, 2010, pp: 1-6. https://doi.org/10.1109/DCOSSW.2010.5593287

5. Y. Jin, Z. Tian, M. Zhou, Z. Li and Z. Zhang, "A Whole-Home Level Intrusion Detection System using Wi-Fi-enabled IoT," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, 2018, pp: 494-499. https://doi.org/10.1109/IWCMC.2018.8450442
6. S. K. Roy, A. Roy, S. Misra, N. S. Raghuwanshi and M. S. Obaidat, "AID: A prototype for Agricultural Intrusion Detection using Wireless Sensor Network," 2015 IEEE International Conference on Communications (ICC), London, 2015, pp: 7059-7064. https://doi.org/10.1109/ICC.2015.7249452
7. Y. Gu, J. Zhan, Y. Ji, J. Li, F. Ren, and S. Gao, "MoSense: An RF-Based Motion Detection System via Off-the-Shelf Wi-Fi Devices," 2017 IEEE *Internet of Things Journal*, Vol. 4, no. 6, pp: 2326-2341,. https://doi.org/10.1109/JIOT.2017.2754578
8. T. Choubisa et al., "Challenges in Developing and Deploying a PIR Sensor-Based Intrusion Classification System for an Outdoor Environment," 2016 IEEE 41st Conference on Local Computer Networks Workshops (LCN Workshops), Dubai, 2016, pp. 148-155. https://doi.org/10.1109/LCN.2016.041
9. K. C. Sahoo and U. C. Pati, "IoT based intrusion detection system using PIR sensor," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp: 1641-1645. https://doi.org/10.1109/RTEICT.2017.8256877
10. D. ALshukri, V. L. R, S. E. P, and P. Krishnan, "Intelligent Border Security Intrusion Detection using IoT and Embedded systems," 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 2019, pp: 1-3. https://doi.org/10.1109/ICBDSC.2019.8645587
11. C.Pham, "Large-scale intrusion detection with low-cost multi-camera wireless image sensors," 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, 2015, pp: 484-491. https://doi.org/10.1109/WiMOB.2015.7348001
12. R. Singh and G. M. Asutkar, "Survey on various wireless sensor network techniques for monitoring activities of wild animals," 2015 IEEE International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore,pp: 1-5. https://doi.org/10.1109/ICIIECS.2015.7192979
13. Suvendu Kumar Mohapatra; Prasan Kumar Sahoo; Shih-Lin Wu, "Big data analytic architecture for intruder detection in heterogeneous wireless sensor networks", 2016Elsevier,*Journal of Network and Computer Applications*, Vol: 66, pp: 236-249.https://doi.org/10.1016/j.jnca.2016.03.004
14. JagdishLalRaheja; Swati Deora; Ankit Chaudhary, "Cross border intruder detection in hilly terrain in a dark environment",2016Elsevier,*Optik Journal*, Vol: 127, Issue: 2,pp: 535-538. https://doi.org/10.1016/j.ijleo.2015.08.234
15. Seung Hyun Kim, Su Chang Lim, Do Yeon Kim, "Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition",2017 Elsevier,*Annals Nuclear Energy*, Vol 112, pp: 845-855.https://doi.org/10.1016/j.anucene.2017.11.026
16. Sungjin Lee, Inwoong Lee, Seonghyun Kim, Sanghoon Lee, and Alan Conrad Bovik, "A Pervasive Network Control Algorithm for Multicamera Networks", 2014 IEEE *Sensors Journal*, Vol. 14, No. 4, pp: 1280-1294.https://doi.org/10.1109/JSEN.2013.2294743
17. R. Unni and U. C. Pati, "PC Based Ultrasonic Intrusion Detection System," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, pp: 942-947. https://doi.org/10.1109/ICCSP.2018.8524262
18. B. C. Norman, "Assessment of video analytics for exterior intrusion detection applications," 2012 IEEE International Carnahan Conference on Security Technology (ICCST), Boston, pp: 359-362. https://doi.org/10.1109/CCST.2012.6393585
19. SubirHalder, Amrita Ghosal, Mauro Conti, "Efficient Physical Intrusion Detection in Internet of Things: A Node Deployment Approach",2019Elsevier, *Computer Networks* Vol. 154,pp: 28-46https://doi.org/10.1016/j.comnet.2019.02.019

20. A. Jasim and C. Çeken, "Video streaming over wireless sensor networks," 2015 IEEE Conference on Wireless Sensors (ICWiSe), Melaka, 2015, pp: 63-66 https://doi.org/10.1109/ICWISE.2015.7380355
21. Wang, T.; Yang, D.; Zhang, S.; Wu, Y.; Xu, S. "Wi-Alarm: Low-Cost Passive Intrusion Detection Using Wi-Fi", 2019 MDPI *Sensors Journal*, Vol. 19, Issue 10, pp: 2335.https://doi.org/10.3390/s19102335
22. Conduct Pham et.al, "Performances of Multi-Hops Image Transmissions on IEEE 802.15.4 Wireless Sensor Networks for Surveillance Applications" 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) 2013 IEEE pp: 477-484. https://doi.org/10.1109/WiMOB.2013.6673402
23. Mrunal Khedkar, G. M. Asutkar. "Energy Optimization in Wireless Sensor Network for Video Data Transmission", 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp: 20-24. https://doi.org/10.1109/GCWCN.2018.8668652
24. Mrunal Khedkar, G.M. Asutkar, R.Hariprakash, "Evaluation of Data Compression Techniques for Video Transmission over Wireless Sensor Networks" 2019, Elsevier, *International Journal of Engineering and Advanced Technology (IJEAT)*', Vol-8, Issue-6, pp: 5328–5335. https://doi.org/10.35940/ijeat.F7923.088619
25. K. Yang, J. Ren, Y. Zhu, and W. Zhang, "Active Learning for Wireless IoT Intrusion Detection,"2018 IEEE *Wireless Communications*, Vol. 25, No. 6, pp. 19-25.https://doi.org/10.1109/MWC.2017.1800079
26. Wang, Y.; Zhu, L.; Yu, Z.; Guo, B. "An Adaptive Track Segmentation Algorithm for a Railway Intrusion Detection System" 2019 MDPI *Sensors Journal*, Vol. 19, Issue 11,pp:2594. https://doi.org/10.3390/s19112594
27. Mrunal M. Khedkar, G.M. Asutkar, "Intruder detection System" Indian Patent 201921024557 A, published July 19, 2019.