IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-10, Oct 2019 E-ISSN: 2347-2693

A Survey of Different Methods in Border Security and Surveillance

Palak Sood[1*], Himani Sharma[2], Sumeet Kaur Sehra[3]

[1,2,3]Guru Nanak Dev Engineering College, Ludhiana, India

Corresponding Author:Palak.sood001@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i10.217228 | Available online at: www.ijcseonline.org

Accepted: 10/Oct/2019, Published: 31/Oct/2019

Abstract— This paper presents a review of the existing border security and surveillance techniques proposed, keeping in view the energy optimization and economic integration at the same time. As the task of border monitoring becomes more and more difficult, searching for solutions beyond physical barriers may be one way to improve security. This paper aims to compare different researches in border security with respect to technique, technology, merits and demerits, time complexity, efficiency and unique features. This paper also highlights their fundamental working principles. The solely aim of this paper is to present a direct comparison of various major researches done in this field so as to facilitate the best optimized method to be deployed according to the current scenario.

Keywords—Wireless Sensor Networks (WSNs), ZigBee, OPNET Simulator, Barrier Coverage, Wireless Integrated Network Sensors (WINS), Raspberry Pi, IoT, Radio Frequency Identification (RFID) tags.

I. INTRODUCTION

Border security and surveillance in the age of globalization: How can we protect ourselves without losing the benefits of openness? [1] This question has remained unanswered for decades. Traditional methods like fencing and manual monitoring across the borders never came up with a complete assurance to the authorities. Productive border security and surveillance play a vital role in curbing the terrorist and illegal activities that take place in the border areas [2]. Border governing is itself a heterogeneous term and may contain, but is not constrained to, the supervision of illegal and legal immigration, ensuring secure movement of authorized individuals and goods, restriction of smuggling, infiltration and human trafficking.

The toughest borders of the world like India-Pakistan Border, US-Mexico Border, and Sudan-South Sudan Border [3] cannot rely on traditional methods for assuring the security of border areas. They need to switch to more trustworthy methods with 24*7 surveillance. The level of security as demanded by current border scenarios can only be achieved when technology is adopted at the root level to ensure better security and human independency.

This paper aims to compare the different mechanisms which have been proposed by various researchers concerning border security and surveillance. The comparison is based on different parameters like technology used, techniques implemented, functionality, efficiency, outcome measures, merits, demerits and future scope.

This paper is organized as follows: Section II discusses the background of border security and the need to do this research with some real-time examples; Section III provides details about major technologies used in different proposed works which are compared in this survey paper ; Section IV presents the implementation of the details of the literature reviews;

Section V presents a tabular comparison of the various research works based on certain parameters; and finally, Section VI concludes the paper with summary and limitations of this research.

II. BACKGROUND

Border Security is the alarming need of all the nations of the world, not only border security but “Smart Border Security”. Here we see some real time scenarios where smart border implementation is taking place in the world. The United Nations also addresses border security under UNCCT Border Security Initiative (BSI) that aims to assist Member States in implementing the United Nations Global Counter-Terrorism Strategy and relevant Security Council resolutions in addressing the overall difficulties in the area of integrated/cooperative border management, cross-border cooperation and border surveillance issues, including the prevention of travel of the foreign terrorist fighters (FTFs) [4].

Indian government, in 2018, has launched a project of Smart Fencing at India Pakistan [5] Borders and India-Bangladesh Borders [6] to make the borders of the nation more secure using Laser Fencing technique. According to the government, technological solutions to security will prove to be an effective way in assuring the minimized number of casualties of our military officers at the border. Digital Smart Fencing would make it virtually impossible for the intruders to do security breach and infiltrate the borders. So far the stretch of 71 Kms has been achieved in Stage 1. They aim to move on to Stage 2 and Stage 3 covering almost 1955 Kms and then to total of 2026 Km of area which is vulnerable.

Kunio Mikuriya, the Secretary General of the World Customs Organization (WCO), made an announcement in 2019 will be dedicated to the fast and smooth cross-border movement of people, goods, and means of transport, with the phrase "SMART borders for seamless Trade, Travel and Transport."

The Custom need to ensure the following guiding: Secure, Measurable, Automated, Risk Management-based and Technology-driven borders [7].

There are number of methods proposed by various researchers in the field of border security and surveillance and therefore we find it important and the need of the hour to compare the major work done in this field so as to come up with the best strategy as per the situation in hand.

III. TECHNOLOGIES FOLLOWED

A. Wireless Sensor Network (WSN)

Wireless sensor networks have become more and more popular these days. It can be defined as a self- configures infrastructure-less wireless network and have less power requirement, low cost but high performance at the same time. WSNs play a significant role in monitoring physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and pass their data on the network to a base location where the data can be worked upon. A base station also called acts as an interface between users and the network channel. One can fetch desired information from the network by shooting queries and collecting results from the sink [8]. WSNs include hundreds of thousands of sensor nodes. Further the sensor nodes can communicate with each other by using radio signals. A wireless sensor node is furnished with sensing and computing devices, radio transceivers and power components. The individual nodes in a wireless sensor network (WSN) are basically resource constrained which means they have limited or lack of resources with limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are visualized, they held responsible for self-organizing an appropriate network infrastructure usually with multi-hop communication between them. The working mode of the sensor nodes may be either continuous or event driven. Wireless sensor devices are equipped with actuators/initiators to "act" upon certain conditions [8]. In which there are different type of sensors like seismic sensors, acoustic, infrared, thermal and visual sensors etc. which can monitor variety of commercial conditions that include Vehicle monitoring, light conditions and temperature etc.

WSN is an essential part of military (C4ISRT) command, communication, computing, control, intelligence, surveillance, reconnaissance and targeting. The destruction of any of the dense deployment of sensor nodes does not affect the military operations as much as the destruction of traditional sensors. Some of the applications of WSN in military applications [9] are surveillance of friendly forces, impedimenta and cartridges, scrutiny of opposing forces, battlefield monitoring, (NBC) nuclear biological chemical attack detection. One of the major applications of WSNs in border surveillance is Battlefield monitoring. In order to prepare new operational plans new sensor networks can be deployed anytime in the battle field. Critical areas, easily approachable routes, paths and channels can be efficiently covered with sensor networks.

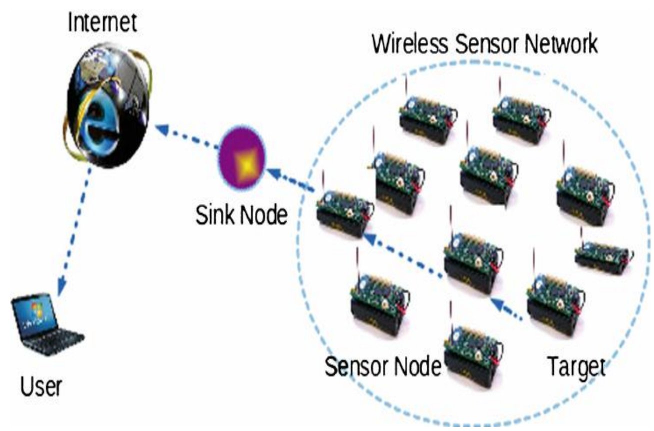

Fig. 1. Wireless Sensor Network Architecture [10]

B. OPNET

This simulator is developed by OPNET technologies; Inc. OPNET had been originally developed at the Massachusetts Institute of Technology (MIT) and since 1987 has become commercial software [11]. OPNET simulator is a simulation tool to simulate the behaviour and performance of any type of network. The main advantage of Opnet Network Simulator as compared to other tools lies in its power and versatility. It provides pre-built models of protocols and devices and allows creating and simulating variety of network topologies. The set of protocols/devices is static – one cannot create new protocols nor modify the working of existing ones. The OPNET is a very powerful network simulator. The main purpose of using it is to cut short cost, increase performance and make sure high availability thus leading to an optimized environment.

The OPNET simulation software is very costly as of several thousand dollars for a single license. But there exists free license for educational purpose, it comes with a graphical user interface that permits the researcher to create networking simulation models using a pick and drop method. It is developed using a discrete event driven simulation (DES) approach [12]. In addition, OPNET uses a hierarchical [13] modelling strategy that allows the user to choose the desired specifications and protocols including physical layer components such as transceivers, antennas, queue management, nodes having process modules, and a network models that are used to connect them. In addition, packet formats that are to be used with the communication protocols can be programmed into the model.

The hierarchical model building has the following modules [14]:
(1) Network Editor which allows the user to build the network topology (2) Node Editor which is used to describe flow of data, (3) Process Editor which is used to specify control flow models.

Using these editors, one can specify models at three different levels: the network domain, the node domain, and the process domain. Modelling in the network domain can be used to hide the complex structure of the lower level component which would be invisible to the user. For running simulations, it has a simulation tool to define and run the simulation, and a debugging tool. For analysing the results, probe editor is used to specify the points where data needs to be collected, an analysis tool, data filtering tool, and an animation viewer. It introduces the creative method for teaching and learning computer networking and hardware [15].

C. ZigBee

ZigBee is one of the most popular wireless sensor network standards with low power, low data rate, low cost, simple to develop and deploy. It provides robust security and high data reliability. The name ZigBee came from zigzagging patterns of honey bees between flowers, it represents the communication between nodes in a mesh network [16]. ZigBee is a wireless technology developed and originated as an open global standard that addresses the exclusive needs of low-cost and low-power wireless (Internet of things) networks. The ZigBee standard runs on the IEEE 802.15.4 physical radio specification and handle in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz [17].

The specification is a packet-based radio protocol which supports low-cost. This protocol enables devices to communicate in a variety of network topologies and can have indelible battery life of several years. The ZigBee 3.0 protocol is aimed to communicate data through noisy RF environments. Many small equipment are coming with embedded ZigBee technology chips and really works like a wonder. ZigBee technology came in the market introducing devices like smoke and heating sensors, medical and control units for domestic and industry use and wireless communication devices. It would provide reorganized statistics in the upcoming years which would entirely change the wireless world. It's revenues would increase more and more by astonishing 3400% in next four years [16]. Some features include low latency, provides long battery life and support mesh networks and up to 65,000 nodes per network.

D. RASPBERRY PI

Raspberry Pi is a series of single-board computers made by the Raspberry Pi Foundation [18], a charity by UK, they aim to upskill people in the field of computing and fabricate technically uncomplicated approach to computing education. The Raspberry Pi was launched in 2012; thereafter it came up with a number of iterations and variations. The basic Pi had a single-core 700MHz CPU with 256MB RAM, and the latest model has a quad-core 1.4GHz CPU with 1GB RAM. The price range for Raspberry Pi has never crossed $35, including the Pi Zero, which costs $5 only. The three generations of Raspberry Pi are Pi 1, Pi 2, and Pi 3, and there exists a Model A and a Model B of almost all three generations.

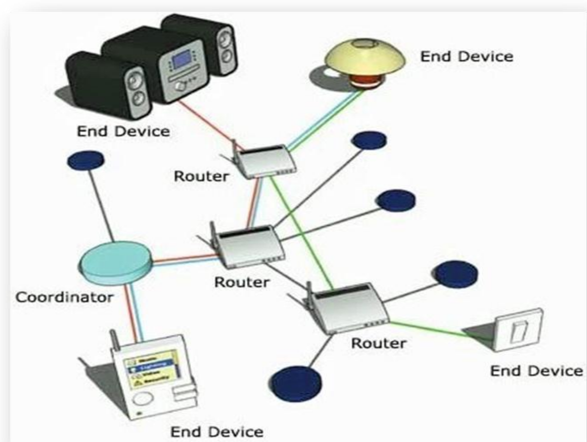

Fig. 2. ZigBee Network [19]

The Pi Zero is a better version of the original (Pi 1) generation, made even smaller and cheaper. It is used all over the world to learn programming technical skills, develop hardware based projects, in smart home and office automation, and also in industrial applications. It runs Linux and delivers a set of General Purpose Input/output (GPIO) pins that enable the user control electronic devices for manual computing and traverse the Internet of Things (IoT). It has been extensively used to create projects in variety of fields like medical science, military defence, farming and industries [20].It also includes software like Python, Java, Scratch, Sonic Pi for designing animation [21].

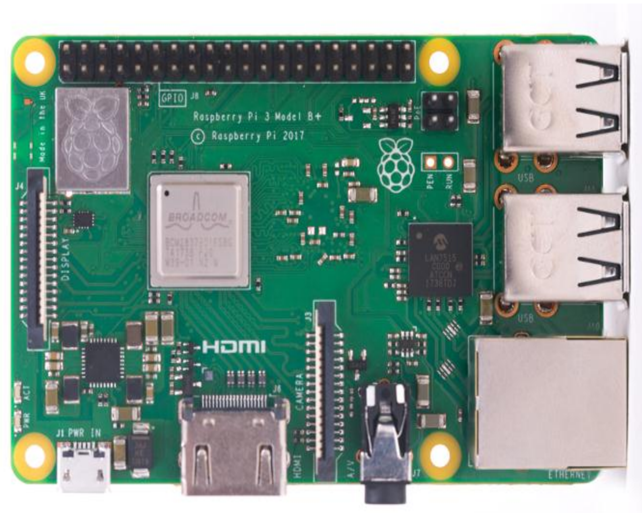

Fig. 3. Raspberry Pi [22]

E. RFID

RFID stands for Radio Frequency Identification System that refers to small electronic devices which consists of small chip and antenna. RFID is a technology based identification system which helps associate objects just through the tags that are attached to them, without need of any light of sight between the tags and the tag reader. The three main components of an RFID System are RFID tag, it is composed of a silicon microchip which is attached to a small antenna and mounted on a stratum and wrapped in different materials like plastic [23];

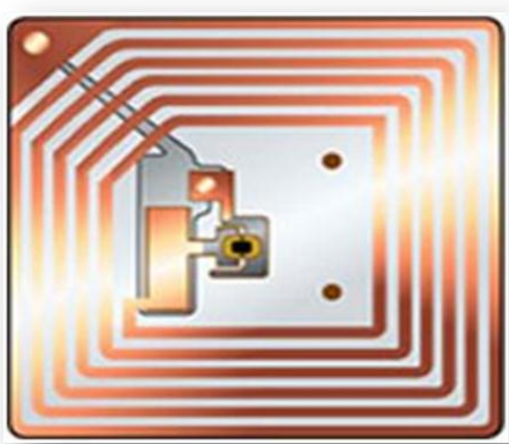

Fig. 4. RFID Tag [24]

Reader, it is composed of a scanner with antennas which transmit and receive signals. It is responsible for to and fro communication with the tag and a Processor or Controller, it could be a host computer with a microcontroller or Microprocessor that receives the input from the reader and processes the data.

Fig. 5. RFID Reader [25]

The two types of RFID systems are passive system and active system. Passive systems are used for short range transmission. The tag gets its power from a reader antenna to the tag antenna while active systems are used for longer distances and to track vehicles with high value. In these systems the tag has its own power source such as an external power supply or a battery unit. The only disadvantage of the active system over passive is the life span of the power sources which is less due to extensive use of battery throughout the lifespan.

IV. LITERATURE REVIEW OF BORDER SECURITY TECHNIQUES AND THEIR ANALYSIS

A. Distributed WSN

Mostafaei H [26] proposed the system to devise a full and a new distributed approach to the border surveillance in wireless sensor networks which aims to maximize the number of barriers, also minimize their energy consumption by using learning automata (LA) to extend the network's overall lifetime and solve this problem by finding more available BPs. Further, it represents distributed border surveillance (DBS) algorithm which finds the minimum possible number of nodes in each barrier to monitor and control the network borders. In the DBS approach, learning automaton facilitates to find the best node to guarantee barrier coverage at any moment. By utilizing the concept of LA each node helps the node to discover the minimum number of the nodes between west and east borders and left or right. It holds the number of activating nodes to evaluate and measure the goodness of the BP rather than using the shortest length metric.

There is a deal between the BP length and the number of nodes in each barrier. On the other hand, if we consider the effect of sensing range we identify that as the sensing range of each node increases, it leads to the number of barriers that will increase and increasing the deployed network height, the number of barriers decreases in all approaches.

At last, we conclude that an increase in the network width has a very low impact because DBS tries to locate the number of barriers in the network based on network height not on network width[26]. So in distributed manner wireless sensor network will allow military forces to blanket a battlefield with easily portable and low-cost sensors, acquire fine-grained situational consciousness that enables friendly forces to see via the ‘‘fog of war’’ with accuracy formerly incredible.

A deliberate evaluation workshop regulated by the US Army Research Lab concluded: It is impractical to rely on highly developed sensors with large power supply. It also consists, inexpensive individual devices establish in large numbers that are likely to be the source of battlefield realization in the future. When the number of devices is increased in distributed sensing systems from hundreds to thousands and millions, the amount of surveillance paid to networking and information processing must growth sharply [27].Barrier coverage enhances the intrusion detection that can be done with a directional sensor[28].

B. OPNET Simulator

Alkhathami M [12] talks about usage of the OPNET Simulator to simulate a WSN and propose that it will make the WSN nodes more robust and highly efficient by streamlining the geographical coordination and network design. The WSNs' work is to facilitate the exchange of information between the sensor nodes and an application platform [29].

The proposed system is competent of detecting a security violation and tracking the direction of the intruder to a notable location, which the officials in border surveillance can then target on. Therefore, it would be a real-time, whole time border security and surveillance system that could render a nation and its people protected.

There are two methods of deployment in the OPNET. First is to use OPNET provided utility for deployment of the nodes in the network editor, but its limitation is supported option for that case is limited. The approach that is followed in this paper is the use of manual method for deploying nodes. The area chosen for simulation is 2x2 km in the clustered tree and mesh topologies. By default, OPNET does not support clustered tree. Open-ZigBee is used for the open source clustered tree model [30]. The model is integrated with the OPNET to activate the clustered routing features and mesh routing is also supported by the default ZigBee libraries.

C. Cluster and Mesh Tree topology

The cluster tree topology requires an efficient planning before being deployed because of the cl addressing requirements. The network behaves in the hierarchical manner moving from the coordinator at depth 1 from the tier 1 routers, from tier 2 routers at depth 2 and the corresponding nodes. Here the planning has been done by keeping the maximum number of nodes as 500. The highest number of nodes will be 20 per parent. The addressing values depend on the Cm, rm and lm where Cm depicts the maximum number of children of a router, Rm represents the maximum number of child router of a router and lm is the maximum depth of the tree. The design developed is as shown in the Fig. 6.

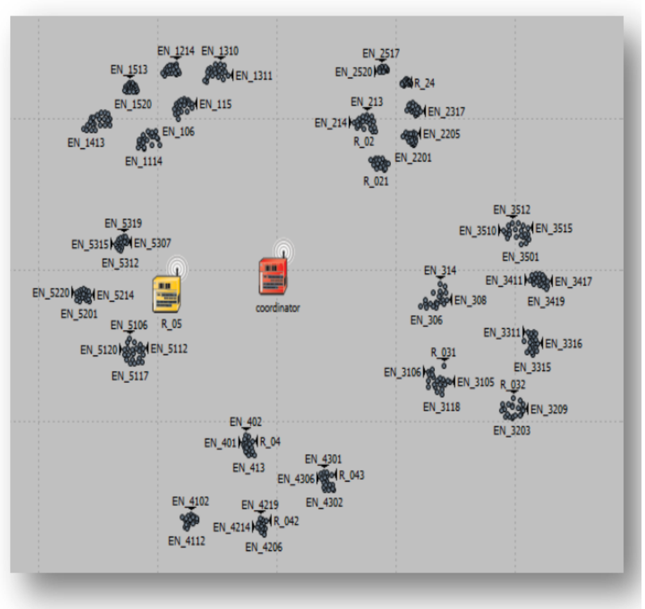

Fig. 6. Cluster Tree [12]

Mesh routing is comparatively easy to deploy in the OPNET because of the default libraries. The addressing is quiet simple and the OPNET itself takes care of all the auto assignments in each node rendering it needless to configure the addresses manually, which otherwise is very time consuming if we talk about when it comes to assigning manual addresses to 500 nodes.

The only configuration required here is for the coordinator that acts as the central point for configuring the routers and the end sensors. It is important to wisely place the routers by considering the number of end sensors as each sensor automatically connects with one of the best path available on the router. Fig. 4 shows the Mesh router placement covering the sensor communication and providing the path towards the coordinator.

OPNET has three different techniques for collection of the results, as global statistics, node statistics and link statistics.

Global statistics compute the average for all the nodes in the Network, e.g. global end to end delay means the average end to end delay of all the nodes in the graph.

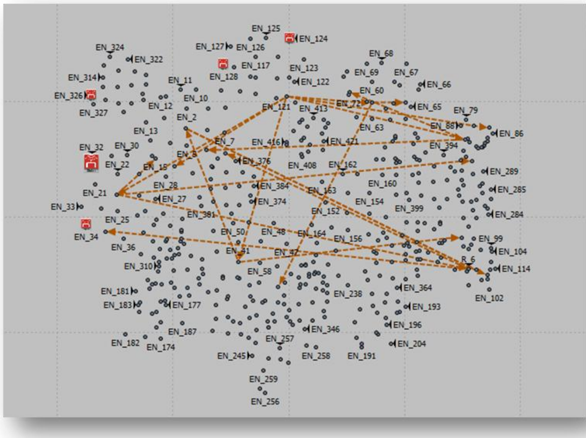

Fig. 7. Mesh Tree [12]

Node statistics provide the statistics at the each node level, e.g. end to end delay will give the end to end delay of one particular node and the link statistics outputs the link level performance. In the terms of overall performance, it can be noted that the network performs optimally well at 100 nodes, but when the number of nodes increases to 500 then the performance continues to degrade and the throughput falls down. The mesh topology performs better than a cluster tree in terms of end-to-end delay because of the flat network architecture and due to multiple path availabilities towards the coordinator with less hop count. In mesh routing sensors are independent of parents, and so the failure of parents does not affect any child, as long as the second active router readily available on the network avoiding complete network isolation problems. Wireless mesh is a costly solution when compared to clustered tree due to many backbone routers, but at the same time network performance is improved and this solution is highly recommended for close placement of the sensors. In terms of performance, the breakout point is 300 as the network performance degrades with an increase in the number of nodes to 500. The additional parameters, the addition of a coordinator and more mesh routers, can be taken in to consideration to improve the performance.

D. WINS

WINS can be defined as a signal processing, sensing, decision capability, and wireless networking capability in a compact and low power system. WINS network is supported by large numbers of sensors in a local area with a short-range which has low average bit rate communication less than 1kbps. The network layout must support the requirement to service dense sensor distributions with prominence on recovering environment information, in which, first it associates the node where the harmonic signals are produced by the unusual objects after that the intensity of that signal is collected. The signal will be sent to the main or header node. Further, it organizes the regular interval data from the nodes which will be analysed and based on changing intensity of the signals and the direction of the nodes will be discovered and the results will be sent to the satellite system or satellite communication system.

The metal detection sensor system first captures the images of that particular area where the actual detection takes place and it will gather all images by the direction of the sensors. The identification of the objects is made and these images are controlled by the system of image scanning and object detection. For the military security, the WINS sensor systems must run at low power, sampling at low frequency. The micro power interface circuits can be a sample at dc or low frequency where “1/f” noise in these CMOS interfaces is large. The micro power signal processing system must be executed at low power and with limited word length. So, WINS applications are usually tolerant of latency. The WINS node or their event recognition may be delayed by 10–100 msec, or more[31]. WINS Gateways allocate the WINS network and access between conventional network and physical layers along with their low power protocols. The depletion on link range through multi-hopping is victimization in the WINS system design to provide advantages or benefits that may be selected from the set of reduced operating power, low cost, improved bit rate, and error rate, improved communication privacy, simplified protocols. These benefits are not obtained simultaneously, but instead must be removed on design emphasis [32]. WINS will allow supervision of land, water, and air resources for environmental monitoring. Borders will be monitored for efficiency and security. Multi-hop communication comes with large power and scalability advantages for WINS networks. So, it allocates an instant advance in the potential for the WINS narrow Bandwidth devices. Figure 7 represents the structure of the wireless integrated network sensors (WINS) arrangement.

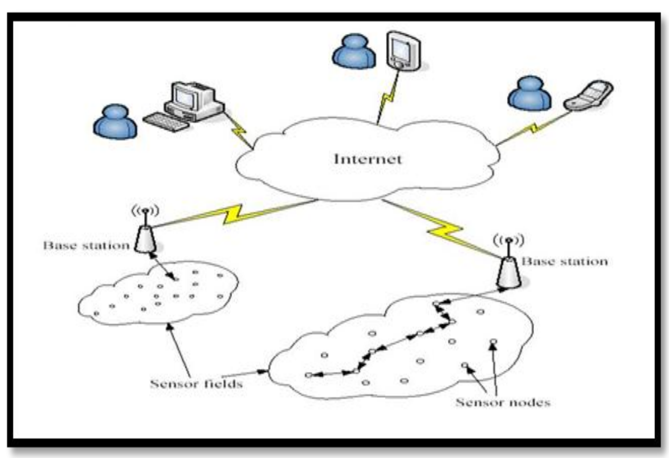

Fig. 7. WINS Arrangement [31]

When an intruder enters the border then the footsteps will create harmonic signals and it recognizes the characteristic feature in the signal power spectrum. Due to this the spectrum, analyser is executed. The spectrum analyser rectify the Wireless Integrated Network Sensors input data into a low resolution power spectrum and WINS spectrum analyser must run at low power level. The WINS spectrum analyser system consist a set of 8 parallel filters. So only if an event appears, does the microcontroller run. Microcontroller can support additional composite algorithms at higher power for event identification [33].The advantages of WINS are, it provides less amount of delay and power consumption in the form of a microwatt. It defers a lot of wiring and can assist new device at any time. The disadvantages include low speed of communication and now it is getting abstracted by components like Bluetooth and it may be costly.

E. Spy Robot

The system proposed by Abdalla GOE [34] is a Spy Robot based on Raspbian operating system with remote supervision and control algorithm through IoT. The system consists of the Raspberry Pi night vision pi camera and sensors. The data about the detection of living objects by PIR sensor is sent to the official user through the web server and using the pi camera images of the moving object are captured which is posted on the webpage for further inspection. The user in the control room is able to control the robot using wheel driver control buttons on the webpage. Obstacle detecting sensors are used to control the movement of a robot with an aim to avoid collisions.

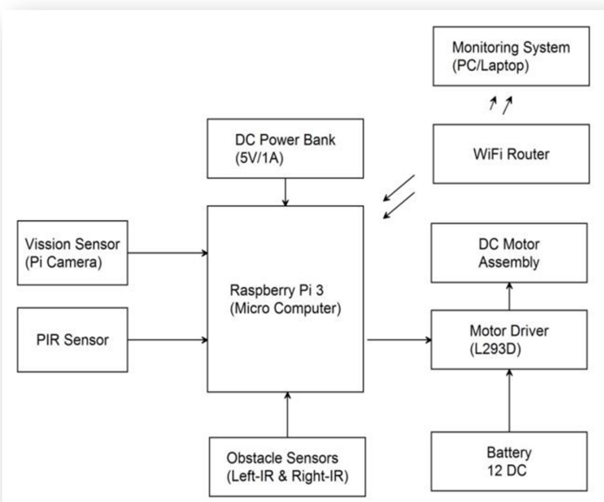

Fig. 8. Block Diagram of Spy Robot System [34]

The main high level language used in this work is Python as it permits the user to code in lesser lines of code than Java or C++.HTML JavaScript is used for web server development. As the main code executes, firstly, the robot will step forward, examine for human presence in the field, and IR sensors will check for obstacles, the robot perform these processes simultaneously. On the control end, the user will give inputs from the webpage; it is stored in server as a text file. At robot end, the Raspberry pi which runs the python script will read the text file and execute the commands per the inputs from the user. The Raspberry pi is connected with the HbridgeIC L293D which will monitor and control the direction of gear motors depending on commands received from the user. When the user clicks on the forward button, the robot moves forward and same movements are achieved for reverse, left and right. When the spy robot is turned on, the user can visualize the photographs of moving living objects on web page captured by pi camera.

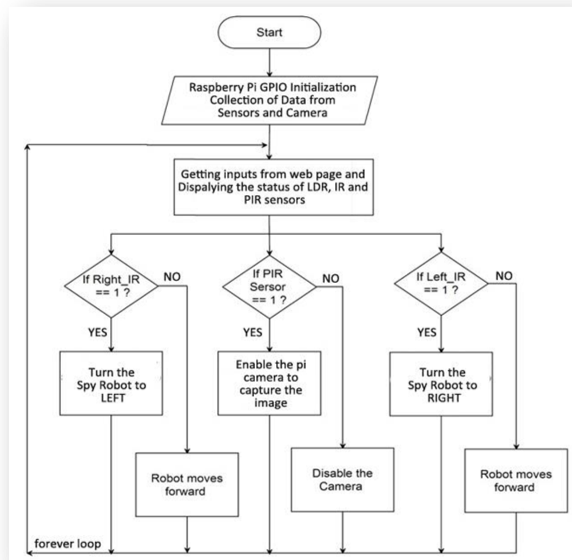

Fig. 9. Design Flow of Spy Robot System [34]

F. Modelling of IoT

Border security is a critical issue for all countries. Several enhancements are made to protect the border but still, there is a hard need to work in this area. The Internet of Things (IoT) is a new model that is promptly acquired ground in the layout of modern wireless telecommunications. The basic idea or the idea behind of this concept is the epidemic presence around us of a variety of things or objects such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. which has unique addressing schemes, are able to interact with each other and merge with their adjacent to reach common goals [35].

The conventional border protection systems made up of border troops that cannot deliver protection all the time.
That's why the Internet of Things (IoT) based model for border protection is represented in this work to contribute continuous monitoring at the border. In this model, it is assumed or pre-supposed that sensors have RFID tags and are deployed on the border in the form of subnets to detect

intrusions. A subnet consists of or made up of a collection of nodes with a gateway node having an RFID tag. A gateway node is used to connect subnets which help to receive invasion information reported by the sensors. A gateway node describes a border troop to catch the intruder [36]. Formal methods are introduced to process the informal or semi-formal requirements or needs to a well-defined formal system which sure about the correctness of the approach. Formal methods are mathematics based techniques that are used to develop or create systems in a systematic manner and also help to analyse critical systems both at an abstract level and a detailed level. A graph-based model is developed or established as graphs are more effective for communication systems. VDM-SL is used as a formal specification language that analyses the systems at a detailed level. That's why the border protection is analysed by developing a formal specification in VDM-SL. It can be validated, verified and analysed using VDM-SL Toolbox [37].

In the security world, the more significant form of the potential of IoT devices is how all the components or elements work together to solves a concrete challenge. One of the advantages is IoT-based security systems must be easy to design, use, install and maintain. In the security and surveillance field, if we want to maximize the potential of an IoT it requires an in-depth knowledge by who can understand all the information about how each feature or component works together and to solve specific challenges, also provide a solution. IoT-based Border Protection System proposed in this work provides continuous all time monitoring and surveillance on the border. Even if an enemy is not captured by a border troop, he is identified, reported and found with the deployment of this. At first, graph-based model is created as graphs are effective way of communication systems. Further UML based model is used to implement better understanding of the system. Use Case is defined and it represents functional requirements while sequence diagram is developed to describe the communication of the system. After semi-formal models are developed, i.e., graph-based model and UML-based model, the algorithm is proposed to overcome the drawbacks of simulations and therefore formal methods are used as specification language, i.e., VDM-SL to define the algorithm. The formal specification is analysed through VDM- SL toolbox which identified a number of errors at early stages of the system development.

If we consider a national perspective, IoT technology is playing a key role or significant role as the Indian government encloses its border with Pakistan and installs advanced security and surveillance pieces of equipment. In which devices would have integrated IoT modules and applications which can talk to one another irrespective of distance and time. So, Fast communication and action would be critical in protecting or securing our borders from unwanted trespasser and terrorists [38].Border Gateway Protocol(BGP) has been suggested to secure the border[39].

V. COMPARATIVE ANALYSIS OF DIFFERENT BORDER SECURITY AND SURVEILLANCE METHODS

Table I shows the comparison among different border security and surveillance techniques surveyed in this paper. The comparison is made on parameters as technique used to implement the security measures, technology being implemented, efficiency of each model with respect to another, functionality of different methods, performance of all the systems, merits, demerits, outcome measures on the basis of which outcome is calculated and the future scope for each research technique.

Table II Comparative Analysis Of Different Border Security And Surveillance Methods

Methods	Distributed Manner	OPNET Simulator	WINS	Spy Robot using Raspberry Pi	Modelling of IoT
Technique	Deploys WSN using Distributed Approach as contrary to traditional methods which use centralized approach.	WSNs are established using the OPNET simulator tool. It will simulate the real network and provide a clear understanding of real scenario.	It combines sensing, signal processing, decision capability, and wireless networking capability in a compact, low power system together with satellite communication and GPS Tracking.	Raspbian operating system based spy robot platform with remote monitoring and control algorithm through Internet of Things (IoT) has been developed which will protect human lives, reduces manual faults and save the nation from enemies.	Using IoT it provides continuous monitoring of the border area in which sensors have RFID tags to detect the intrusions.
Technology	WSNs, LA, DBS Algorithm which ensure barrier coverage.	WSNs, ZigBee, OPNET Simulator Tool.	WINS, Metal and Bomb Detection Sensors and Object Identification System	Raspberry Pi (small single-board computer), night vision pi camera and PIR sensor.	UML, Formal Methods, VDM-SL.
Efficiency	Using distributed approach and	Using OPNET to simulate a WSN	It detects people in images by selecting a 128	The movement of robot is automatically	This model is efficient in terms

	scheduling algorithm it saves energy of the sensors and increase the number of barriers.	will make nodes robust and efficient by optimizing geographical coordination and network design.	X 64 pixel window from the top left corner of the image as an input which is then classified as a person/nonperson. It divides the image in parts of legs, head, left and right arm. It saves computational time and power.	controlled using obstacle detection sensors. It can be extended to fields like industries, banks and shopping malls [34]	of energy as subnet-based deployment is assumed which localizes the processing at subnet level [36].
Functionality	DBS try to find the minimal possible count of nodes in each barrier to supervise the network borders, and LA helps to find the best node to ensure barrier coverage at any moment[26].	It implements the simulated network using cluster and mesh technology and captures the result with different number of nodes to with 100, 300 and to a maximum of 500 nodes.	It finds the node which produces harmonic signals and collects the intensity of the signal. It will be sent to the main node. This data will be analyzed and sent to the satellite communication system and then metal detection sensor system will capture the images.	Robot operates in three modes. Firstly, initialize the code and let the Robot to navigate freely based on the sensor status. Secondly, control the movement in a specific direction by the Keyboard. Thirdly, monitor the information available on the web page, and act accordingly, using various buttons.	Sensors and gateways are deployed in form of subnets in specified areas with higher chances of intruders. Graph-based model is developed then UML based modelling is used to develop better understanding of the system. Use Case is defined to represent the functional requirements and sequence diagram is used to describe the communication in the system.
Performance	Average Sensor Node Degree is where O(ø)=E/N=Number of edges and N= Number of nodes so overall time complexity is O(KE)	OPNET has 3 techniques for collecting results as: • Global, • Node and • Link statistics. Considering overall performance, cluster tree with large scale is more suitable than mesh routing.	WINS network provide large number of sensors in a local area with short range and low average bit rate communication (less than 1 kbps) [31].	Robot has sufficient intelligence to supervise the largest area providing a secure space. The intelligent robots can perform preferred tasks in unstructured environments with or without human direction [40].	To identify run time errors, dynamic checking is performed. The integrity properties of the specification are generated by integrity examiner. These properties are further evaluated thus proving the correctness of the developed specification.
Merits	It considers 2 BPs along the border giving high security and saves energy of the sensor nodes using scheduling algorithm thereby making it optimized and feasible. Usually one path is considered in others works of same type making this more robust and less dependent.	Supports a large set of network environments from a simple LAN to space communication. It facilitate researchers with the standardize environment to effectively study the effect of network behaviours before deployment in the real world thereby saving costs.	System not only monitors the area but also captures the images and processes them by automated approach. GPS allows a user to view the current or previous positions of any object on Google Map. Another benefit is that it provides a high probability of correct detection and identifies doubtful materials so there are very less chances of false results.	Design and development cost of a robot is comparatively less than hiring a human workforce. A single camera is used instead of multiple cameras making the system flexible to capture pictures using PIR sensor [41]. Power consumption is minimized by use of minimum number of two gear motors for movement of the robot.	Facilitates efficient data collection as no human intervention is required. The proposed formal specification is analysed using VDM-SL toolbox that captures errors at an early stage of the system development. IoT provides continuous monitoring of the border.

Demerits	The performance of DBS depends majorly on network height and not on network width i.e. on changing the network area the number of barriers is not affected which seems unrealistic.	The supported options in OPNET provided utility are limited and the network chokes beyond 500 nodes in case of mesh technology. Also simulation lacks in assuring the correctness of the proposed model [36].	Identity of the strangers is not verified from the officials and therefore no stringent action can be taken on the intruders.	The system is more suitable for flat surface on which the robot can easily operate. This design would not suffice in case of rough or irregular terrain environments like rocky or hilly areas due to wheeled mechanism. Also a human intervention is required at all times for controlling the robot actions.	Failure of the node may disrupt the network connectivity thereby disconnecting it from the subnet and the neighbouring nodes [37]. IoT is based on internet connectivity therefore in case of poor network this system may not work as desired.
Outcome Measures	It analysis the effect of :changing number of nodes; sensing range; network height; network width and states that with increasing network height barriers will decrease and capability also decreases while network width has no effect on the outcome.	In terms of overall performance, it can be seen that the network behaves optimally at 100 nodes but at 500 nodes the performance degrades and throughput falls down. The mesh topology performs better than a cluster tree in term of end-to-end delay [12].	Once the object is identified and the metal detected system will have an idea about animals/humans or other objects like tankers crossing the border area.	The information regarding detection of living things using PIR sensor is passed on to the users via web server and pi camera captures the moving objects, images are posted on the webpage simultaneously. The user in the control room is able to access the robot with wheel drive control buttons.	To overcome the drawbacks of simulations, formal methods based specification language, i.e., VDM-SL is used to specify the algorithm. In case an enemy is not detected by a border force, s/he is identified, reported and caught.
Future Scope	The study can be extended to increase the number of barrier paths. Also the effect of changing network width can be analysed in more detail.	Network can be setup with different topology like star[42] or bus To improve the coverage territory, prolong the network life span, load balancing and to send the objectives with the minimal resources [43].	Authentication of data can be confirmed with the higher authorities and after confirming the capacity of the weapons correct action can be taken using automatic approaches. Further details of the strangers from the criminal database can be fetched.	Quad copter Spy robot can be built using this technique and it can be used in war fields, hilly terrains, terrorist prone and hotspot areas with non-flat terrains.	Trespassers Favorite Paths (TFPs) [44] can be determined as a tool to predict the detection probability of a surveillance network which will further improve the capability of the system.

VI. CONCLUSION

We surveyed different methods targeting border security and surveillance, which could help in better and technology driven mechanism to ensure protected nations. For a system that has to consider a number of different parameters, for security, it is not likely that any of the surveyed methods alone would be enough to cover the entire range of security concerns, starting from resource constrained devices over to the trespassers coming from any direction. The survey found that the two most mature choices to be considered are the combination of OPNET based simulation and WSN system in a distributed approach which further can be enhanced with robotic intelligence. In future this combination as a whole would render the checks on the practicality of the work through simulation and the applying them in the real time to cover the border areas with double check of top-bottom and left to right barrier path. This combo package could further be enhanced by combining it with methods of robotic automation to take decisions as quickly as desired in the times of battles or cross borders. It is also analyzed that the selection of best methods depends on the different input parameters under consideration such as security concerns, cost effective type of areas where such systems are implemented and the motive behind implementation of these techniques.

REFERENCES

[1] P. Andreas, "Perspective: Border Security in the Age of Globalization: How Can We Protect Ourselves without Losing the Benefits of Openness?," 2003.

[2] T. Academy, R. Academy, and S. S. Trakt, "Border Management Security Council," *Appl. Phys. A*. [Online]. Available: https://www.un.org/sc/ctc/focus-areas/border-control/ accessed on August 2,2019.

[3] N. Paudyal, "10 Toughest Borders In The World." accessed on August 7,2019.

[4] UN, "Border Management," *2013*. [Online]. Available: https://www.un.org/counterterrorism/ctitf/en/uncct/border-security-initiative, accessed on August 12,2019.

[5] PIB, "Smart Fencing Indo Pak Jammu Border," *2018*. [Online].

Available: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1546376, accessed on August 12,2019.

[6] PIB, "Smart Fencing Indo Bangladesh Border," *PIB 2019*. [Online]. Available: https://pib.gov.in/Pressreleaseshare.aspx?PRID=1567516, accessed on August 20,2019.

[7] WCO, "Smart Border World," *2019*. [Online]. Available: http://www.wcoomd.org/en/media/newsroom/2018/november/world-customs-organization-dedicates-2019-to-transforming-frontiers-into-smart-borders.aspx, accessed on August 21,2019.

[8] M. A. M. and M. M. I. Additional, "Overview of Wireless Sensor Network Chapter."

[9] X. Hu, "Wireles ss Sens sor Ne etwork k : Cha aracte eristics s and Ar rchitec ctures," vol. 6, no. 12, pp. 1398–1401, 2012.

[10] M. R. Senouci, "WSN Image." [Online]. Available: https://www.researchgate.net/profile/Mustapha_Senouci/publication/265396190/figure/fig2/AS:295817744273409@1447539854939/A-typical-WSN-architecture.png, accessed on August 23,2019.

[11] S. Siraj, A. K. Gupta, and Badgujar-Rinku, "Network Simulation Tools Survey," *Int. J. Adv. Res. Comput. Commun. Eng. Vol. 1, Issue 4, June 2012*, vol. 1, no. 4, pp. 201–210, 2012.

[12] M. Alkhathami, L. Alazzawi, and A. Elkateeb, "Large scale border security systems modeling and simulation with OPNET," *2017 IEEE 7th Annu. Comput. Commun. Work. Conf. CCWC 2017*, pp. 1–8, 2017.

[13] S. Mittal, "OPNET: An Integrated Design Paradigm for Simulations," *Softw. Eng. An Int. J.*, vol. 2, no. 2, pp. 57–67, 2012.

[14] G. Gao, "Deployment of WirelessHART," no. Fskd, pp. 2120–2124, 2012.

[15] A. Kuki, "Modeling computer networks by the help of OPNet tools," vol. 1, pp. 251–258, 2015.

[16] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, "Study on ZigBee technology," *ICECT 2011 - 2011 3rd Int. Conf. Electron. Comput. Technol.*, vol. 6, no. April, pp. 297–301, 2011.

[17] D. Products, "Zigbee Wireless Mesh Networking Link." [Online]. Available: https://www.digi.com/resources/standards-and-technologies/zigbee-wireless-mesh-networking, accessed on August 24,2019.

.[18] Raspberry Pi Foundation, "Raspberry Pi." [Online]. Available: https://opensource.com/resources/raspberry-pi, accessed on August 25,2019.

[19] Gadget Geek, "Zigbee image." [Online]. Available: https://i0.wp.com/www.gadgetgeek.info/wp-content/uploads/zigbee_network2-3.jpg?w=413, accessed on August 29,2019.

[20] A. Imteaj, T. Rahman, M. K. Hossain, and S. Zaman, "IoT based autonomous percipient irrigation system using raspberry Pi," *19th Int. Conf. Comput. Inf. Technol. ICCIT 2016*, pp. 563–568, 2017.

[21] R. Karthikeyan, S. Karthik, T. R. Prasanna Vishal, and S. Vignesh, "Snitch: Design and development of a mobile robot for surveillance and reconnaissance," *ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst.*, pp. 5–8, 2015.

[22] Raspberry Pi Foundation, "Raspberry Pi 4 Image." [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-4-model-b/, accessed on August 29,2019..

[23] E. – E. P. for E. Students, "RFID web link." [Online]. Available: https://www.elprocus.com/rfid-basic-introduction-simple-application/, accessed on September 2,2019..

[24] E. – E. P. for E. Students, "RFID tag image." [Online]. Available: https://www.elprocus.com/wp-content/uploads/2013/09/RFID-Tag.jpg, accessed on September 2,2019.

[25] E. – E. P. for E. Students, "RFID reader image link." [Online]. Available: https://www.elprocus.com/wp-content/uploads/2013/09/An-RFID-reader.jpg, accessed on September 2,2019.

[26] H. Mostafaei, M. U. Chowdhury, and M. S. Obaidat, "Border Surveillance with WSN Systems in a Distributed Manner," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3703–3712, 2018.

[27] A. Arora *et al.*, "A line in the sand: A wireless sensor network for target detection, classification, and tracking," *Comput. Networks*, vol. 46, no. 5, pp. 605–634, 2004.

[28] A. S. Anand and V. S. Anitha, "Implementation and Analysis of k-Barrier Coverage in Wireless Sensor Networks," *Int. J. Comput. Sci. Eng.*, vol. 06, no. 06, pp. 26–31, 2018.

[29] M. Alkhathami, L. Alazzawi, and A. Elkateeb, "Border surveillance and intrusion detection using wireless sensor networks," *Int. J. Adv. Eng. Technol.*, vol. 8, no. 2, p. 17, 2015.

[30] G. Gao, H. Zhang, and L. Li, "An OPNET-based simulation approach for the deployment of WirelessHART," *Proc. - 2012 9th Int. Conf. Fuzzy Syst. Knowl. Discov. FSKD 2012*, no. Fskd, pp. 2120–2124, 2012.

[31] P. Perugu, "An innovative method using GPS tracking, WINS technologies for border security and tracking of vehicles," *Proc. Int. Conf. "Recent Adv. Sp. Technol. Serv. Clim. Chang. - 2010", RSTS CC-2010*, pp. 130–133, 2010.

[32] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors (WINS): Principles and practice," *Cacm'00*, pp. 1–10, 2000.

[33] I. Journal, O. F. Engineering, A. R. On, and O. Detection, "International journal of engineering sciences & research technology a review on obstacle detection and vision," vol. 4, no. 1, pp. 1–11, 2015.

[34] G. O. E. Abdalla and T. Veeramanikandasamy, "Implementation of spy robot for a surveillance system using Internet protocol of Raspberry Pi," *RTEICT 2017 - 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc.*, vol. 2018-Janua, pp. 86–89, 2018.

[35] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[36] H. Afzaal and N. A. Zafar, "Modeling of IoT-based border protection system," *2017 1st Int. Conf. Latest Trends Electr. Eng. Comput. Technol. INTELLECT 2017*, vol. 2018-Janua, pp. 1–6, 2018.

[37] H. Afzaal and N. A. Zafar, "Formal localized reactive subnet-based failure recovery model for sparsely connected wireless sensor and actor networks," *ICOSST 2015 - 2015 Int. Conf. Open Source Syst. Technol. Proc.*, pp. 64–71, 2016.

[38] Telecom, "Security and surveillance: Role of IoT technologies in protecting India." [Online]. Available: https://telecom.economictimes.indiatimes.com/tele-talk/security-and-surveillance-role-of-iot-technologies-in-protecting-india/2530, accessed on October 2,2019.

[39] T. K. Mendhe, P. a Kamble, and A. K. Thakre, "Survey on Security, Storage, and Networking of Cloud Computing.," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 11, pp. 1780–1785, 2012.

[40] J. Zhang, G. Song, G. Qiao, T. Meng, and H. Sun, "An indoor security system with a jumping robot as the surveillance terminal," *IEEE Trans. Consum. Electron.*, vol. 57, no. 4, pp. 1774–1781, 2011.

[41] M. S. Mukundaswamy and G. L. Bhat, "Embedded controller based wireless power monitoring and controlling," *2015 Int. Conf. Emerg. Res. Electron. Comput. Sci. Technol. ICERECT 2015*, pp. 392–397, 2016.

[42] open-ZB, "OPNET Web page." [Online]. Available: http://www.open-zb.net/, accessed on October 12,2019..

[43] S. Sharma, D. Kumar, and K. Kishore, "Wireless Sensor Networks - A Review on Topologies and Node Architecture," *Int. J. Comput. Sci.*, vol. 1, no. 2, pp. 19–25, 2013.

[44] C. Komar, M. Y. Donmez, and C. Ersoy, "Detection quality of border surveillance wireless sensor networks in the existence of trespassers' favorite paths," *Comput. Commun.*, vol. 35, no. 10, pp. 1185–1199, 2012.

Authors Profile

*Ms.Palak Sood pur*sued Bachelor of Technology from Guru Nanak Dev Engineering College,India in 2015 and worked as Quality Assurance Associate at Sapient Corporation Pv Ltd till 2017.She is currently pursuing Master of Technology from Guru Nanak Dev Engineering Collge,India.Her interest areas are Networking,Machine Learning and Information Retrieval.

*Ms.Himani Sharma pur*sued Bachelor of Technology from Guru Nanak Dev Engineering College,India in 2017.She is currently pursuing Master of Technology from Guru Nanak Dev Engineering Collge,India.Her interest areas are Machine Learning and Information Retrieval.

Ms. Sumeet Kaur Sehra is working as Assistant Professor at Guru Nanak Dev Engineering College, Ludhiana. Her areas of interest are Software Engineering, Machine Learning, and Information Retrieval. So far She has published around 50 national and international articles in various domains.She has 14 years of teaching experience.

