A Lightweight Security Scheme (LSS) for Wireless Node Communication for Border Surveillance System

Rajeev Singh* and Sukhwinder Singh

Department of Computer Engineering, College of Technology, G.B. Pant University of Ag. & Technology, Pantnagar, Udham Singh Nagar, Uttarakhand, India
E-mail: rajeevpec@gmail.com; sukhwinder.cup@gmail.com
**Corresponding Author*

Received 31 January 2021; Accepted 10 March 2021;
Publication 14 June 2021

Abstract

The physical breach across the borders is a very common issue these days among nations sharing boundaries. It is controlled via proper border surveillance system. The border surveillance system is trivially a physical border intrusion detection system in which CCTV cameras are used traditionally to observe manually the presence of some intruder. Instead, we utilize the raspberry PI controller board based wireless sensor nodes fitted with raspberry PI camera for identifying the intruder. Once the intruder is identified, the wireless sensor nodes communicate the messages with the next hop sensor nodes and the message ultimately reaches the control room from where army action may be initiated. In this work, we propose a novel lightweight security scheme (LSS) for raspberry PI based wireless node communication for the Border Surveillance System. We have utilized the XBee (Zigbee) serial communication between raspberry PI based wireless sensor nodes. The proposed scheme is based upon the notion of confusion and correct identification of pattern (byte) in the transmitted messages. The entire communication scheme is lightweight and secure.

Journal of Cyber Security and Mobility, Vol. 10_4, 641–662.
doi: 10.13052/jcsm2245-1439.1041

Keywords: Raspberry Pi, wireless security, WSN, border surveillance system, lightweight communication.

1 Introduction

Border surveillance system is a security system that protects the nation's borders by keeping an eye through the persons sitting in the control room. In short it provides physical security from the intruders crossing and defying the border line.

The border surveillance system is trivially a physical border intrusion detection system in which CCTV cameras are used traditionally to observe manually the presence of some intruder. With the advent of newer technologies like wireless sensor networks (WSNs), the semi-autonomous or fully autonomous border surveillance systems are being proposed by researchers (Bhadwal et al. (2019)) that needs much lesser human intervention and takes the decisions on their own regarding use of automatic weapons [1]. In such semi-autonomous or fully autonomous border surveillance system, several wireless sensor nodes are deployed across the border area. These nodes communicate with each other and ultimately send the message to the control station. Singh and Singh (2021) have proposed three such automatic/semi-automatic models [2] and one among them is shown in Figure 1 in which the raspberry PI microcontroller board based wireless sensor nodes fitted with raspberry PI camera and having image processing software like Tiny YOLO are utilized for identifying the intruder. Once the intruder is identified, the wireless sensor nodes communicate the messages with the next hop sensor nodes and the message ultimately reaches the control room from where army action may be initiated.

In the present day digital world such system itself requires security from the attacker. One part of the border surveillance system is the communication methodology between the two communicating peer wireless nodes. This research work is a step towards strengthening the communication methodology between the two communicating peer wireless nodes.

We propose a novel lightweight security scheme (LSS) for raspberry PI based wireless sensor node communication for the Border Surveillance System. In this work, we have utilized the Zigbee serial communication between raspberry PI based wireless sensor nodes.

This paper is further divided into 5 sub sections. Section 2, reviews the related work done in this domain i.e. border surveillance systems. Section 3, presents the proposed lightweight security communication scheme for the

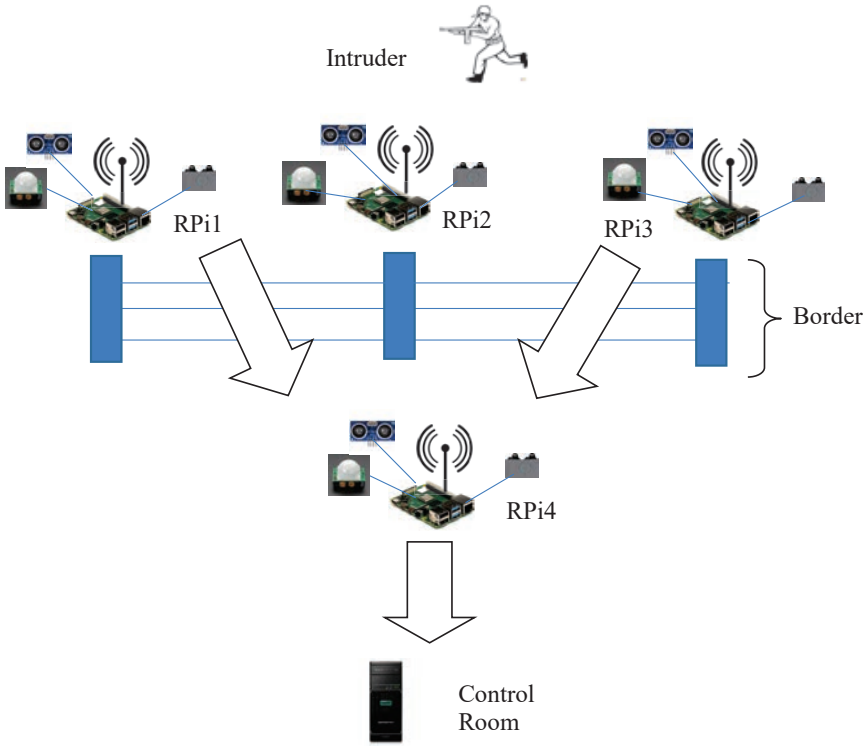


Figure 1 Autonomous Border Surveillance System with Raspberry PI wireless sensor nodes equipped with PIR, Ultrasonic and PI camera sensors for identifying the Intruders.

border surveillance systems. Section 4 presents the results and observations while Section 5 provides security related discussion. Section 6 provides conclusion and future scope of work.

2 Related Work

Bellazreg et al. (2013) proposed heterogeneous hierarchical global framework for Wireless Sensor Network based border surveillance system. The framework depicted Basic Sensing Nodes (BSN), Data Relay Nodes (DRN) and Data Dissemination Nodes (DDN). The BSN nodes lying in the level one of hierarchy, sense the intruder data and events. The DRN nodes lying in the level two of hierarchy, supervises the BSN node and routes the BSN data to the third level hierarchy nodes (DDN). DDN nodes further transfer the data

to the Network Control Center. The BSN nodes work towards effectively and realistically tracking the intruder via a thick line at the border [3]. The author provided only the framework details and no implementation details have been provided in the paper for the realization of sensor node functionality in the border area.

Afzaal and Zafar (2017) have modeled and proposed an IoT based border protection system. The sensor nodes deployed across the border form part of surveillance network and continuously monitors the border area for intrusion activities. The gateway nodes further pass message to the border troops who may take the decision regarding the necessary military action. The communication followed between nodes is graph based RFID. UML based model is presented for understanding the functionality of the system but without any implementation [4].

Felemban (2013) has published a survey that broadens our understanding of WSN based border intrusion detection and surveillance approaches [5]. The survey mainly describes the research efforts of various Universities and education institutions towards improvement and testing various types of sensor nodes capable of sensing some particular properties. University of Virginia and Carnegie Mellon University have used the stealth technology and various sensors magnetometer, acoustic and photo sensors for the detection of moving vehicles [5, 6]. The detection of vehicle motion is targeted mainly in this proposal. Sinopoli et al. (2003) proposed, Pursuer-Evaders Game (PEG) for intruder detection involving Pursuers and Evaders. Here, Pursuers utilize computer vision or ultrasonic sensing within their sensing range for tracking the evaders [5, 7]. The synchronization is required among nodes in this system. The Sand sensor model by Ohio State University researchers (Arora, 2004) is an effort toward differentiating between moving metallic (armed vehicle and tanks) and non-metallic objects [5, 8, 9]. They have not proposed identification of intruders rather utilized micro-power impulse radar sensors with magnetometer for sensing the objects. One hybrid approach is developed by Georgia Tech, King Saud University, and University of Nebraska named as Border Sense that utilizes different kinds of WSNs like ground, underground, multimedia and mobile for border patrolling purposes [5, 10]. However, node coordination and unified framework are the main concern here. Also the two underwater surveillance systems are presented in this survey. In first, acoustic sensor is used to detect the enemy watercraft [5]. In the second, the three-axis accelerometer sensors in shallow water are used for the detection of ship intrusion. In this system, the V-Shaped waves on the water surface, generated by ship the movement are utilized [11]. The entire work pertains to under

water surveillance only. In [12], MicaZ Zigbee nodes were equipped with two only sensors, microphones and light sensors whereas neglecting even the camera sensors. Their proposal uses ANN for analyzing the intrusion data. An interesting border surveillance mechanism under the project named FleGSens [13] suggests two methodologies utilizes PIR motion detection sensor signals for intrusion detection. In the first methodology, the local PIR sensor signals are grouped and authenticated before they flooded the sensing data in the network. The second methodology talks about the node failure by selecting a random number of nodes called buddies for listening messages of other nodes [5, 13]. In the both of methodologies, no camera sensors are used for recording or live streaming for the purpose of further observation whether the motion signal are coming from an animal or human.

Bhadwal et al. (2019) have proposed a Smart Border surveillance system utilizing PIR sensors for sensing the intruder in the border area. The proposed system comprised of sensor nodes and a surveillance camera. Furthermore, two motors are used in this system and these motors control the horizontal and vertical motion of the camera. The movement of motors is governed by raspberry PI microcontroller as it received the sensed data of PIR sensor. If any kind of human activity is found by the raspberry PI controlled camera, a warning is issued and an alert is sent to the control station for the necessary military action including triggering the auto-combat system for targeting the intruder [1]. However, no implementation work of the proposed system has been given in the paper. Also in the proposed system there is lack of placement of surveillance cameras in the border area, any network resiliency. Furthermore no software requirements for identification of intruder along with installation of software on nodes and differentiation of animals & humans during identification of intruder are given.

In one of the recent publications, Bhardwaj (2020) has proposed MEMS microphone array for detecting sounds to identify the motion state of the intruder [14]. In the proposed system, only sound signals are sensed to achieve its goals. Jeevitha and Kumar (2019) have proposed an animal intrusion alert system based on the image processing techniques. This work targets intrusion related with only animals not the human [15].

The handheld computers like Raspberry PI microcontroller, Node MCU and other small microcontrollers are becoming popular nowadays and are being used very commonly by the researchers and industry experts towards agriculture intrusion, home security, and computer network security [16–21]. In one of the recent attempt Yasar (2020) utilized Raspberry PI and open CV [22]. The proposal lacks common border surveillance features like human

and animal differentiation. The results in the proposal appear as if taken from single standalone system.

None of the proposals discussed in this section talks about security of communication process used in the Border Surveillance System. A summary of the research works is presented in Table 1. Our proposed lightweight security scheme (LSS) for raspberry PI based wireless sensor node communication is an effort towards strengthening the communication process used in the Border Surveillance System.

3 Proposed Lightweight Security Scheme (LSS) for Wireless Nodes (Raspberry PI Nodes) Communication

The proposed lightweight communication scheme (LSS) for the border surveillance system assumes three kinds of bytes: 'message byte' (indicating the findings on the sender wireless sensor node – whether the intruder OR intruder with harmful weapon OR an animal has been identified by the sensor node), 'authentication byte' (used for authentication and synchronization purpose between the two communicating wireless sensor nodes) and 'communication message bytes' (which are composed of 'message bytes' and involves uniform mixing of message bytes). 'Communication message bytes' are prefixed with 'authentication byte'. The lightweight communication scheme involves sending 'authentication byte' followed by the intermixed 'message byte' within the 'communication message bytes' (or 'communication message'). Two kinds of communication may exist at MAC layer: Zigbee based serial communication and Wireless LAN based communication. In the former, the notion of 'communication message bytes' whereas in the latter, the notion of 'communication message' may be referred. The various types of messages in the scheme are shown in Table 1.

It assumes that there are fixed numbers (types) of messages being shared between the two communicating wireless sensor nodes. These fixed numbers (types) of messages between sender and receiver are used for indicating the findings on the sender node i.e., whether the intruder or intruder with harmful weapon or an animal has been identified by the sensor node. In this paper we assume that there are four numbers (types) of messages with respective 'message byte' value as one among 1, 2, 3 and 4 being sent by the sender node as per the identified object (Figure 2 shows the structure of the 'communication message'). Message byte value of 1 means that intruder has been detected and identified through PI camera by the communication

Table 1 Summary of the research works

Research Work/ Methodology for Border Surveillance	Major Features	Accomplishments	Major Issues	Any Network Security Mechanism Utilized (Yes/No)
Bellazreg et al. (2013)	Heterogeneous hierarchical global framework for WSN based border surveillance system	Effective and realistic intruder tracking at the border by level one Basic Sensing Nodes (BSN)	Only the framework details are provided, no implementation details provided.	No
Afzaal and Zafar (2017)	IoT based border protection system. The communication followed between nodes is graph based RFID.	Sensor nodes deployed across the border form part of surveillance network and continuously monitors the border area for intrusion activities	UML based model is presented for understanding the functionality of the system but without any implementation.	No
Felemban (2013)	Survey that broadens our understanding of WSN based border intrusion detection and surveillance approaches. It even discusses the underwater surveillance.	The survey mainly describes the research efforts of various Universities and education institutions towards improvement and testing various types of sensor nodes	No novel methodology has been proposed/implemented.	No

(*Continued*)

Table 1 Continued

Research Work/ Methodology for Border Surveillance	Major Features	Accomplishments	Major Issues	Any Network Security Mechanism Utilized (Yes/No)
FleGSens (2009)	Two methodologies suggested which utilizes PIR motion detection sensor signals for intrusion detection.	Methodologies talks about authenticating the sensor signals and about node failure.	No camera sensors are used for recording or live streaming for the purpose of further observation whether the motion signal are coming from an animal or human.	No
Bhadwal et al. (2019)	Smart Border surveillance system utilizing PIR sensors for sensing the intruder. Movement of camera via motors governed by raspberry PI microcontroller is proposed.	Auto-combat system that can take military action for targeting the intruder is activated via an alert sent to the control station.	No implementation of the proposed system provided.	No

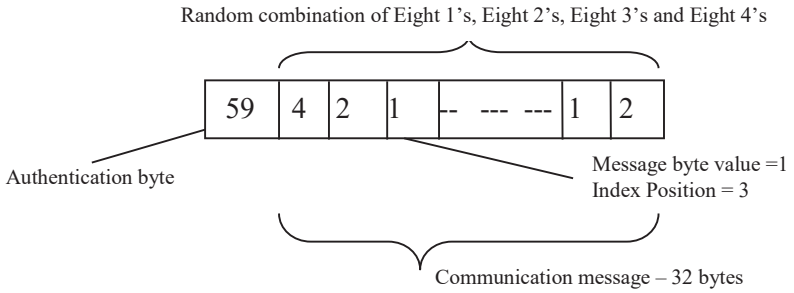
Bhardwaj (2020)	MEMS microphone array utilized for detecting sounds and hence, the intruder.	Motion state of the intruder can be identified.	Only sound signals are sensed for detecting the intrusion.	No
Jeevitha and Kumar (2019)	Animal intrusion alert system based on the image processing techniques.	Early warning mechanism for the farmer/landowner	This work targets intrusion related with only animals not the human.	No
Yasar (2020)	Identification of known faces and triggering an alarm via Arduino controller for an unknown face.	Raspberry PI and open CV utilized for face detection purpose.	The proposal lacks common border surveillance features like human and animal differentiation. The results in the proposal appear as if taken from single standalone system	No

Table 1 Types of messages/bytes used in the scheme

Kinds of Bytes	Purpose	Contents
Message byte	Used for indicating the findings on the sender wireless sensor node – whether the intruder OR intruder with harmful weapon OR an animal has been identified by the sensor node.	Value as one among 1, 2, 3 and 4 as per the identified object.
Authentication byte	Used for authentication and synchronization purpose between the two communicating wireless sensor nodes.	Evaluated using the refreshed initial vector (IVi). It is function of bytes of Ki, IVi and 'communication message bytes' (or 'communication message').
Communication message bytes/communication message	Used for communication between two nodes. Termed as 'communication message bytes' and send one after the other in Zigbee oriented communication. Also termed as 'communication message' for WLAN communication.	Prefixed with 'authentication byte'. Composed of 'message bytes' and involves uniform mixing of message bytes.

initiating wireless sensor node. Message byte value of 2 means that intruder with harmful weapon has been detected and identified through PI camera by the communication initiating wireless sensor node. Message byte value of 3 means that an animal has been detected and identified through PI camera by the communication initiating wireless sensor node. Message byte value of 4 means that neither intruder nor animal has been detected and identified through PI camera by the communication initiating wireless sensor node. Thus, the 'communication message' is in expressed in multiple of four (4) and is in the form of byte combinations comprising of values 1, 2, 3, and 4. These byte values are spread in random order. Here, for simplicity 32 bytes communication messages are considered. In 'communication message' the values 1, 2, 3, and 4 are equally (and independently) distributed i.e. in a 'communication message' of 32 bytes 1 is going to appear 8 times and similarly, the values 2, 3 and 4 are going to appear 8 times.

The working of the proposed communication system involves two phases. In first phase, the master key (MK) and initial vector (IV) are evolved on



Message byte = 01 => an intruder has been detected.
Message byte = 02 => intruder with harmful weapon has been detected.
Message byte = 03 => an animal has been detected.
Message byte = 04 => no intruder has been detected.

Figure 2 Structure of communication message.

the two communicating wireless sensor nodes. In this phase two counter values (C0 and C1) are also evolved. The key and IV will be refreshed whenever sender want to send a message ('communication message bytes') to the receiver node. In second phase, the two communicating wireless sensor nodes utilizes the refreshed key (Ki) for finding the exact position of the 'message byte' and utilizes the refreshed initial vector (IVi) for evaluating the 'authentication byte'. Thus, 'message byte' is placed within the 'communication message bytes' whereas 'authentication byte' is sent along with the 'communication message bytes'.

In this work, it is assumed that the sensor nodes have evolved pre-shared master key (MK) (phase one) and refreshed keys (Ki) & refreshed initial vector (IVi) as per the key hiding communication scheme (KHC) proposed by Singh and Sharma et al. (2014) [23]. To achieve the present day security issues in WSNs, the key size considered is 256 bit. The key and initial vector refreshing is again explained here for the sake of clarity.

New refreshed Ki and IVi are derived (by calculating hash) from the previous (Ki-1, IVi-1) using Equations (1) and (2). Leftmost 256 bits of the MK (ℓ-256) are used for refreshing the key while rightmost 256 bits of the MK (r-256) are used of refreshing the IV. Attacker or any other third person is not aware of the MK. Therefore, it is difficult for them to calculate the new Ki or IVi.

$$\text{refreshed key, Ki (256)} = \text{h}(\text{Ki-1}(256) + \ell\text{-256}) \tag{1}$$

$$\text{refreshed initial vector, IVi (256)} = \text{h}(\text{IVi-1}(256) + \text{r-256}) \tag{2}$$

Process for finding the position of the 'message byte' in the 'communication message bytes' (or 'communication message') to be send by the sender as per the present status of intrusion:

- Refresh the Key K i.e., evaluate the Ki.
- Find the sum of 32 bytes of Ki
- XOR the evaluated sum with the incremented counter0 (++C0).
- Finally take MOD 32. This will give the value of the index (location) between 0–31.
- Place the message byte at this index location/place in the communication message.

Process for finding the authentication byte (to be prefixed with the 'communication message bytes' (or 'communication message')):

- Refresh the IV i.e., evaluate the IVi.
- Find the sum of 32 bytes of IVi.
- XOR the evaluated sum with the incremented counter1 (++C1).
- Take MOD 32. This will give the value/index between 0–31 for selecting the byte values each from Ki and IVi.
- Select the byte values from Ki and IVi at this index location.
- Add the byte values of Ki & IVi. Also select the byte value at the same location from the evaluated 'communication message bytes' or 'communication message'.
- Add it also with byte values of Ki & IVi. Take MOD 32. This will give the 'authentication byte'.

The authentication byte evaluated hence is the function of bytes of Ki, IVi and 'communication message bytes' or 'communication message'. The 'authentication byte' is placed before the entire 'communication message bytes' or 'communication message' whereas the 'message byte' is placed at the index location/place calculated in the 'communication message bytes' or 'communication message'.

Creating 'communication message bytes' or 'communication message'

There are four (1, 2, 3, & 4) possible 'message byte' values considered in this work. These are either send as 32 'communication message bytes' (in Zigbee communication) or are kept in 32 bytes long 'communication message' (in WLAN communication). For 'communication message bytes' the position of the 'message byte' in all the 32 byte sequence is calculated whereas for the 'communication message' index of the 'message byte' is calculated. We discuss here only placing of 'message byte' in the 'communication message'. The 'message byte' is placed at the index location

calculated in the 'communication message'. It is followed by placing the remaining (31) message bytes (apart from the message byte whose location has been found in the communication message) 1's, 2's, 3's and 4's in the 32 bytes long communication message. They are kept to increase confusion for the attacker. For finding positions of these remaining 1's, 2's, 3's and 4's in the 'communication message', a random function is used. For preventing the intruder from disturbing the contents of the 'communication message', the integrity check bytes may be send to the receiver post 'communication message' transfer. Integrity check bytes are evaluated as message integrity check (MIC) value with refreshed key as the input parameter [23–25].

4 Results

The proposed methodology of lightweight communication scheme for the border surveillance is implemented using two communicating wireless sensor nodes. Each wireless sensor node is constituted by Raspberry PI microcontroller board and has set of sensors like proximity infrared (PIR) sensor, ultrasonic sensor and PI camera sensor installed & configured on it. The Raspberry PI configuration used is: Raspberry PI3, Model B+ with WiFi and BLE, OS: Raspbian PI, other accessories that are used during working with raspberry PI are: 7 inch capacitive touch screen, 64 GB Class 10 SD card, Plastic Enclosure Case for RPi, HDMI cable, 5 V USB Power adapter, USB to Micro USB cable and network patch cable.

Each wireless sensor nodes also has USB based XBee communication module installed on it. Xbee is a programmable device and can run various protocols including Zigbee. The Xbee communication range for the border surveillance purpose and node communication is approximately 70–90 mtrs. XBee (Zigbee) module has two parts: XBee board and radio communication module (XBeeZigbeeTHTmodules(S2C)) (Figure 3). It is configured using XCTU software (version 6.3) installed on the PC. Using XCTU software, the Zigbee modules can also be managed and updated. In this work we have used Zigbee protocol on XBee device and therefore we have used name Zigbee instead of XBee henceforth in the paper.

For communicating with the radio modules API and AT consoles are used. One of the Zigbee is configured in the coordinator role while others are configured in the router role. After configuring the Zigbee modules, the changes are saved into the Zigbee device firmware using the XCTU software. The coordinator Zigbee installed on a wireless sensor node having raspberry PI microcontroller can collect the responses from the route nodes.

Figure 3 Zigbee module (XBee S2C).

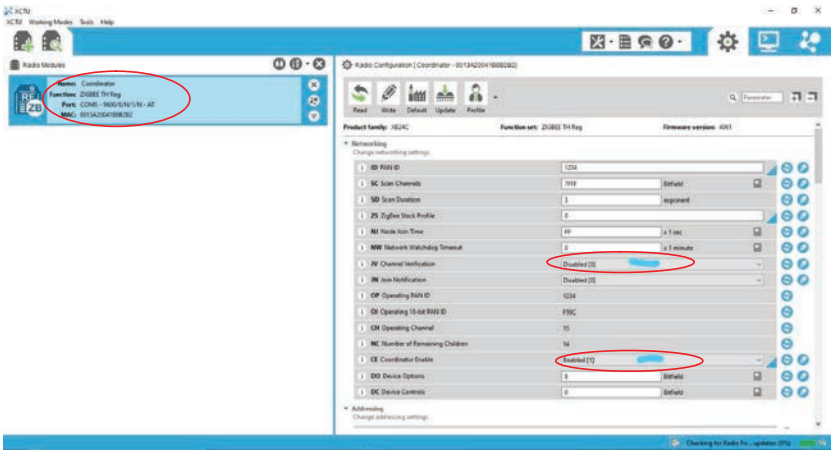


Figure 4(a) (1) Zigbee module configured as coordinator.

The router Zigbee installed on a wireless sensor node having raspberry PI microcontroller can forward the messages of other wireless sensor nodes or can generate their own messages. These router messages are then collected and analyzed at coordinator wireless sensor node. The coordinator node can also transfer these messages to the control station for analysis and further reaction purpose. The settings of coordinator and router on Zigbee modules via XCTU software is shown in Figure 4(a) (1-2), (b) (1-2) & 4(c). The parameters configured are encircled.

Zigbee involves serial communication wherein entire communication is expressed in term of byte sequences. As proposed, the wireless sensor

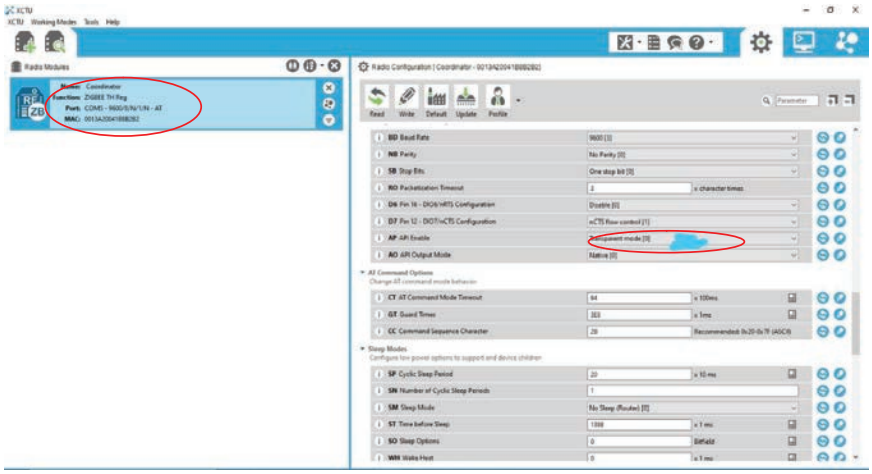


Figure 4(a) (2) Zigbee module configured as coordinator.

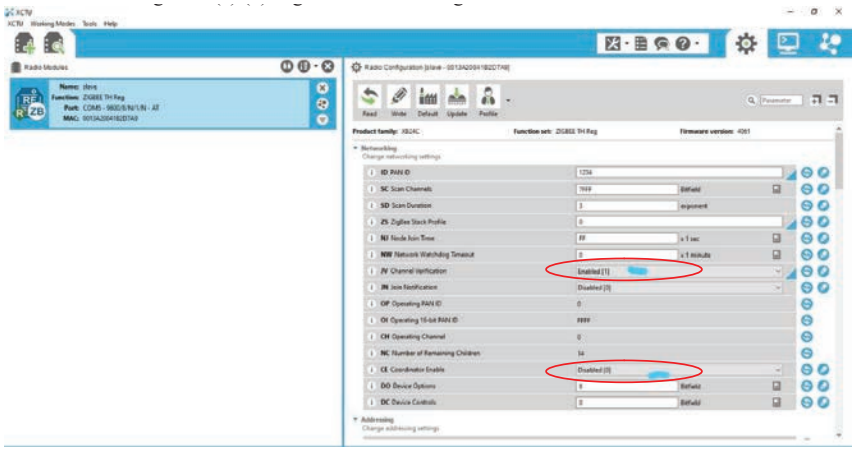


Figure 4(b) (1) Zigbee module configured as router.

communicating nodes have 32 bytes communicating messages. A program has been written in the Python programming language (version 3.9) and is run on the communicating wireless sensor nodes. The algorithm on the sending wireless communicating node uses the key refreshing and IV refreshing tasks each time a message is communicated/send. The refreshing time on the wireless sensor node is recorded. Its average is observed as 0.028 ms. This is justified as the raspberry PI microcontroller has 1 GB RAM and

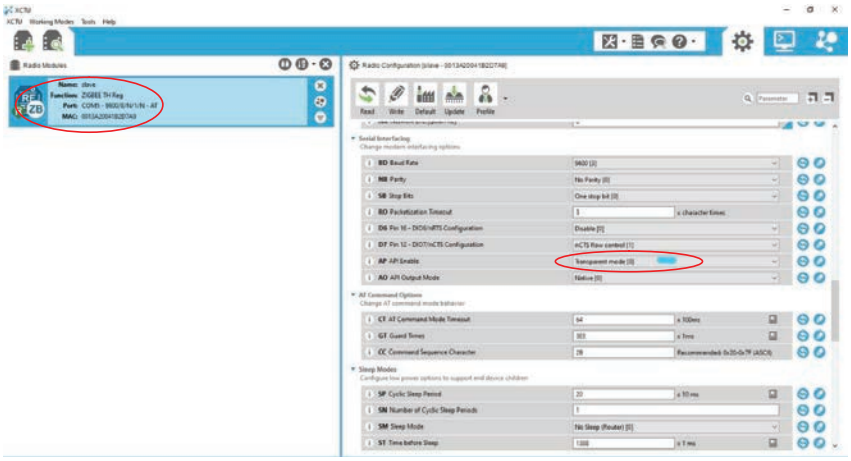


Figure 4(b) (2) Zigbee module configured as router.

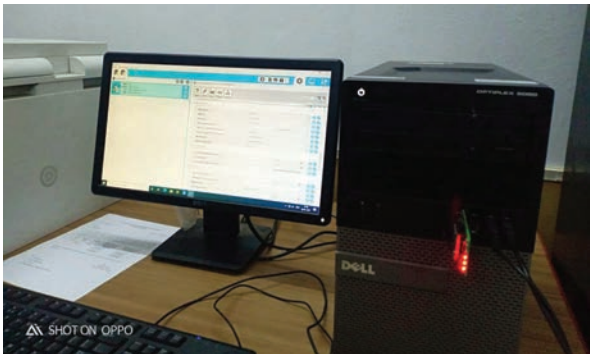
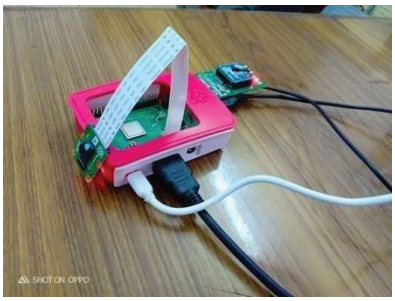


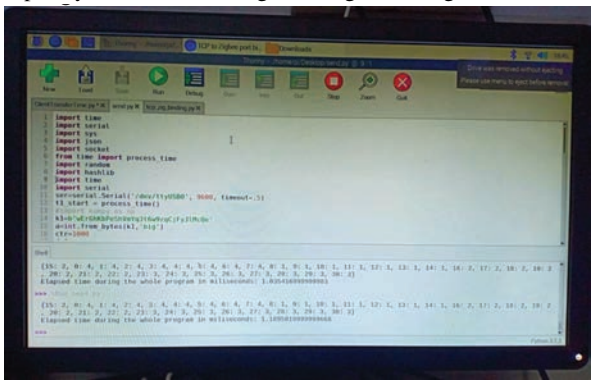
Figure 4(c) Zigbee configuration using XCTU software.

1.4 GHz ARM CPU processor. The processing time for a single raspberry PI microcontroller board for finding the index location for placing the message byte within 32 bytes communication message is observed as 0.74 milliseconds. This justifies the proposed communication scheme as a lightweight scheme. The transmission time of a 32 byte communication message is also recorded. The message is transferred using the serial Zigbee communication and hence 32 bytes are transferred serially from sender to receiver node. The average communication time for sending the communication message successfully is observed as 1.077 milliseconds. Communicating raspberry PI nodes along with the communication snapshot is shown in Figure 5.



(a) Raspberry PI communicating with Zigbee configured as Router

(b) Raspberry PI communicating with Zigbee configured as coordinator



(c) Communication snapshot between sender and receiver raspberry PI nodes

Figure 5 Ongoing Zigbee communication between sender and receiver nodes.

We have also observed the average communication time for sending the communication message successfully via UDP socket and with wireless LAN communication utilizing the TP link access point. It is observed as 1.87 milliseconds. This may be useful if the wireless sensor nodes of the border surveillance system communicate with each via access points.

5 Discussion

The proposed lightweight secure scheme (LSS) provides communication between the sender wireless sensor node and the receiver wireless sensor node. In this method the sending node communicates its 'message byte' (with value one among: 1, 2, 3, & 4) within 'communication message' to the receiver node. LSS utilizes the notion of confusion and correct identification of pattern ('message byte') in the transmitted communication messages for security purpose. The method is secure as the intruder though can see the values (1, 2, 3, & 4) being distributed across the 'communication message' but cannot find the exact position or index of the 'message byte' due to lack of refreshed key and master key. Also, the intruder is not able to calculate the value of the 'authentication byte'. This is because the intruder is not having master key and IV nor is able to calculate the refreshed keys and IVs. The uniform distribution of the message values in the communicating message is the actual cause of confusion to the intruder. The intruder has an option to disturb the contents of the message in which case the integrity check bytes may get changed and hence will result in the dropping of the message at the receiver. The sequence at the receiver is: (1) verification of authentication byte, (2) verification of the integrity check bytes, (3) finding the 'message byte'. In case of failure of verification in (1) and (2), the receiver node will accept or reject the 'communication message'. In case of success of verification in (1) and (2), the receiver node will find the 'message byte'. Depending upon the 'message byte' value, the receiver node will take decision accordingly. The LSS scheme is lightweight which is reflected by the experimental computation and communication time findings.

6 Conclusion and Future Work

In this paper, we have proposed a secure and lightweight communication scheme for the border surveillance system utilizing the Zigbee communication. The wireless sensor nodes of the border surveillance system are constituted of raspberry PI microcontroller 3 model B++ boards, sensors like PIR, ultrasonic & camera and XBee (Zigbee) modules. In the experiment the Zigbee modules were configured as coordinator and router. The computation and communication time for creating and sending the 'communication message' was recorded. The communication time was also recorded for the WLAN based communication of the sensor nodes through an access point. The values of the recorded times clearly show that the scheme is lightweight.

It is because of the fact that LSS scheme involves only the trivial operations like XORing, addition and hash evaluation. The intermixing of the message bytes in this methodology is the main source of protection to the communication message. It prevents intruder from knowing anything about the ongoing message communication between the communicating wireless sensor nodes. In future, we aim towards implementation of a small scale prototype system comprising of several nodes for the border surveillance system utilizing the LSS communication.

Acknowledgement

The financial support provided by AICTE under the Collaborative Research Scheme (CRS) grant is hereby acknowledged (CRS grant No. 1-5748651630). We hereby also acknowledge the support provided by our college, especially by Dr. (Mrs.) Alakhnanda Ashok, Dean, College of Technology, Pantnagar for the continuous support throughout this work.

References

[1] N. Bhadwal, V. Madaan, P. Agrawal, A. Shukla, A. Kakran, "Smart Border Surveillance System using Wireless Sensor Network and Computer Vision," International Conference on Automation, Computational and Technology Management (ICACTM), London, United Kingdom, pp. 183–190, April 2019.

[2] Rajeev Singh and Sukhwinder Singh, "Raspberry PI based models for Smart and Automatic Monitoring Border Surveillance System", submitted to ICTACT Journal on Communication Technology, 2021.

[3] R. Bellazreg, N. Boudriga, S. An, "Border Surveillance using sensor based thick-lines," ICOIN 2013, Bangkock, Thailand, 221–226, January 2013.

[4] H. Afzaal and N.H. Zafar, "Modeling of IoT-based Border Protection System," First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT), Karachi, pp. 1–6, 2017.

[5] E. Felemban, "Advanced Border Intrusion Detection and Surveillance Using Wireless Sensor Network Technology," Int. J. Communications, Network and System Sciences, 6, 251–259, 2013.

[6] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui and B. Krogh, "An Energy-Efficient Surveillance System Using Wireless Sensor Networks," 2nd International Conference on Mobile Systems, Applications and Services, Boston, 6–9 June 2004.

[7] B. Sinopoli, C. Sharp, L. Schenato, S. Shaffert and Sh. S. Sastry, "Distributed Control Applications Within Sensor Networks," Proceeding of the IEEE, August 2003.

[8] http://www.cse.ohiostate.edu/siefast/nest/nest_webpage/ALineInTheSand.html

[9] A. Arora, et al., "A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking," Journal Computer Networks, Vol. 46, No. 5, 2004.

[10] Z. Sun, et al., "BorderSense: Border Patrol through Advanced Wireless Sensor Networks," Ad Hoc Networks, 2011, pp. 468–477.

[11] H. Luo, et al., "Ship Detection with Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 7, 2012, pp. 1336–1343.

[12] A. Mishra, K. Sudan and H. Soliman, "Detecting Border Intrusion Using Wireless Sensor Network and Artificial Neural Network," IEEE DCOSS 2010, Santa Barbara, 21–23 June 2010.

[13] P. Rothenpieler, D. Kruger, D. Pfisterer, S. Fischer, D. Dudek, C. Haas, A. Kuntz and M. Zitterbart, "Flegsens: Secure Area Monitoring Using Wireless Sensor Networks," Proceedings of the 4th Safety and Security Systems in Europe, 2009.

[14] B. Bhardwaj, U. Pallapothu, "Wireless Smart System for Intruder Detection at Borders with Far-field microphone and TDOA," International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, pp. 1257–1263, 10–12 Sept. 2020.

[15] S. Jeevitha; S.V. Kumar, A Study on Sensor Based Animal Intrusion Alert System Using Image Processing Techniques, 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 20–23, 12–14 Dec. 2019.

[16] S. Angadi and R. Katagall, "Agrivigilance: A Security System For Intrusion Detection In Agriculture Using Raspberry Pi And Opencv", International Journal of Scientific & Technology Research, 8(11):1260–1267, Nov. 2019.

[17] S. Sruthy, S. Yamuna and S. N. George, "An IoT based Active Building Surveillance System using Raspberry Pi and NodeMCU," pp. 1–9, 2020. Available at: https://arxiv.org/abs/2001.11340.

[18] T. Prathaban, W. Thean, M.I.S.M. Sazali, "A vision-based home security system using OpenCV on Raspberry Pi 3," Advances in Electrical and Electronic Engineering (AIP) Conference Proceedings 2173, 020013 (2019).

[19] K. Rambabu, V.Haritha, S.Nikhil Srinivas, P.Sanjana Reddy, "IoT Based Human Intrusion Detection System using Lab View," International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(6S4): 557–560.

[20] A.A. Ahmed, Y.W. Kit, A.A. Sallam, "Raspberry Pi-Based Investigating Model for Identifying Intrusion Evidence," J. Forensic Sci. & Criminal Investigation, 7(3):1–9, 2018.

[21] R.A. Nadafa, S.M. Hatture, V. M. Bonal, S.P. Naikb, "Home Security against Human Intrusion using Raspberry Pi," International Conference on Computational Intelligence and Data Science (ICCIDS 2019), Procedia Computer Science 167 (2020) 1811–1820.

[22] Z. A.Yasar, R. D. Kumar, S. Aadarsh, G. H. Kumar, "Border Surveillance System using Computer Vision," 6th International Conference on Advanced Computing & Communication Systems (ICACCS), pp. 623–628, 2020.

[23] Rajeev Singh and T.P. Sharma, "A Key Hiding Communication Scheme for Enhancing the Wireless LAN Security," Springer Wireless Personal Communications, 2014, 77(2):1145–1165.

[24] Rajeev Singh and T.P. Sharma, "A Novel Sequence Number Based Secure Authentication Scheme for Wireless LANs," Journal of Electronics Science & Technology (JEST), 2015, 13(2):144–152.

[25] Rajeev Singh and T.P. Sharma, "A sequence number based WLAN authentication scheme for reducing the MIC field overhead", in: Proc. Tenth IEEE International Conf. on Comp. and Commun. Technologies, WOCN'13, Bhopal, July 2013, pp. 1–4.

Biographies

Rajeev Singh is currently working as Associate Professor in the Department of Computer Engineering, G.B. Pant University, Uttarakhand (India). He received his Ph.D. Degree from N.I.T. Hamirpur (H.P.) and M.Tech. Degree from Indian Institute of Technology, Roprkee (India), both in Computer Science and Engineering. His research interest includes information systems, computer networks and network security. He has published 2 books, several book chapters and research papers in journals/conferences of repute.

Sukhwinder Singh is working as assistant Professor (TEQIP-faculty) in the Department of Computer Engineering, G.B.Pant University of Ag. & Technology, Pantnagar (Uttarakhand) India. He has done B.Tech. and M.Tech. His research interest includes Cyber Security, Machine Learing, and IoT.