Development and Design of the Panic Button System for Community Security in Rural Areas of Pucará-Ecuador

J.D. Jara, Grupo De Investigación De Telecomunicaciones, Universidad Politécnica Salesiana, Cuenca, Ecuador.
L. Caldas-Calle, Grupo De Investigación De Telecomunicaciones, Universidad Politécnica Salesiana, Cuenca, Ecuador.
E. Barbecho, Servicio Integrado De Seguridad ECU 911, Cuenca, Ecuador.
J. Bravo-Torres, Grupo De Investigación De Telecomunicaciones, Universidad Politécnica Salesiana, Cuenca, Ecuador.
J.P. Bermeo, Grupo De Investigación De Telecomunicaciones, Universidad Politécnica Salesiana, Cuenca, Ecuador.
P. Gallegos, Universidad Politécnica Salesiana, Cuenca, Ecuador.

Abstract--- Rural areas, with difficult topography, do not allow easy entry and development of security systems in their localities. Emergency Care and Safety institutions such as: Police, Fire Department and Red Cross need stable and reliable safety equipment to optimize their response time to emergency events. The alarm system proposed in this essay is a panic button system that performs real-time monitoring for emergency events. The Security system uses the Raspberry Pi Zero to send remotely, to Security Services ECU 911 system, an alert when one of the panic buttons is pressed by VPN. The advantage of this alarm system is its low cost, allowing its access to poor people, and its stability for emergency events.

Keywords--- Panic Button, Public Safety, Raspberry Pi Zero, VPN.

I. Introduction

Security is one of the fundamental pillars in the progress of a modern society, being one of the main tasks and objectives of governments [1]. To this end, different state institutions related to security must be coordinated in such a way as to enhance their scope and effectiveness. In this context, the development of information and communication technologies can be a primary tool for achieving this goal.

The advance of microelectronic devices, data networks and wireless communications systems are generating new opportunities to design systems and security services that monitor in real-time different cities' spots and coordinate in a timely manner actions with state institutions to support emergency events. An example of this type of service is provided by the Servicio Integrado de Seguridad ECU 911 (SIS-ECU 911) in Ecuador. Institutions such as police, firefighters, military, public health services, among others, are coordinated from a single emergency center, providing increased efficiency and quality to emergency care and in the use of public resources.

However, the progress achieved in security issues with the implementation of SIS-ECU 911 in Ecuador, its coverage is not enough efficient for the entire national territory. Many places, in especially rural areas with poor people, do not have access to such services. This is due in large extent, to the difficulties to access to mobile telephone networks —the level of penetration of this type of networks is in the order of 72.62% and 14.94% for fixed telephony [2], [3]. In security systems, establishing a reliable communication channel for emergency care has a high priority. Mobile telephony networks offer advantages such as: security, extensive coverage, extensive development and reliable communication channels, increasing the acceptance in the market of security systems.

In the literature, different systems of panic buttons developed for rural and urban sectors can been seen. In [4], for example, a remote security system is presented for home usage. The authors use GSM for emergency notification by sending data and short text messages to users. In [5] a panic button is proposed for users with smartphones. Again a GSM module is used to send messages to applications developed in Android. In [6] a monitoring model is presented for the elderly. Notifications are sent to the authorities, via GSM and GPRS, when the interruption occurs in one of its sensors. In the city of Cuenca–Ecuador [7] a panic button program has been started. This system links the monitored sector to SIS-ECU 911 via a GPRS wireless communication channel. As can be seen, all these proposals make use of cellular systems; however, this solution, for the rural sector of Ecuador, suffers from the problem of low cellular coverage, as mentioned before. An alternative to cellular communication channel is the Internet. In Ecuador, the level of Internet penetration is rural areas is 92% [8].
In [9], the implementation of an intrusion alarm and a web service is described. In this system, the Internet is used to send emergency notifications, by e-mail, to the respective authority. The research concluded that the total integrated system performance was robust in the reliability of signal strength and the web service’s alarm latency. However, this work does not consider the data security when transmitted over the Internet.

This article presents an improvement to the performance of the community security system, specifically in rural areas: Pucará. A reliable, low-cost system was developed based on the ARM processor of Raspberry Pi. For this, a virtual private network (VPN) was used as a communication channel in emergency events. This provided confidentiality and data integrity by encrypting and authenticating traffic between the system to the SIS-ECU 911 emergency and coordination service.

In the following of this article, in section II the architecture of this security system is presented. Section III states the results obtained. Finally, section IV presents the conclusions.

II. System Architecture

The panic button system has the purpose of delivering security and tranquility to the rural areas like Pucará. The system provides a solution to the lack of service coverage of mobile networks that does not allow the monitoring of the SIS-ECU 911 in this area, implemented a stable communication channel, which allows the transmission of emergency signals in real time. Three buttons are used to deal with emergencies in the management of fire, health and safety incidents. The moment a button receives an event, the system will determine the type of emergency and transmit the signal to the security institution, which will dispatch the specialized personnel for emergency care.

This system develops the monitoring of the emergency events in real time and the monitoring of the state of the connection. To do this, the system performs constant reading of the status of the buttons, providing a 24 hours service. When a button is pressed, the type of emergency is determined and automatic notification is given to the Central Station Receiver (CSR), located in the coordinating institution (SIS-ECU 911). The control panel will respond with a confirmation message, giving way to the correct operation of the event; otherwise, the system will repeat the notification until its confirmation.

Monitoring the connection status enables the communication status between the transmitter in the rural area and the CSR to be checked. To do this, a monitoring message is sent periodically. The CSR will respond with a confirmation message, giving way to a correct state. If monitoring message is not received during the monitoring period, a communication failure alert will occur at the central station.

A. Hardware System

The structural diagram of the alarm system is shown in Fig. 1. The Premises Equipment (PE) consists of three parts: the reading module, the output module, and the central module.

Figure 1: Structural Diagram of the Alarm System
Reading module, composed three buttons, allows interaction with the user and reading of emergency events. For the interaction with the user, to the three buttons a different symbol was defined for each emergency type, for easy and intuitive use. This type of interaction allows the transmission of an event automatically and without the need for additional codes or emergency calls.

The output module visually displays the status of the connection and the emergency event. For this, two different types of colors were used for the led's. The red led indicates the status of the communication between the PE and CSR. The green led shows how an emergency event is processed. Using these indicators gives the interaction with the user, who will observe the different states in which the equipment is.

The equipment is designed to wirelessly connect to WiFi networks in rural areas. This is because most rural areas have implemented such wireless networks to access the Internet. The connection between the PE and the central station is by VPN (see Fig. 1). In the PE, the central module is responsible for processing and transmitting emergency messages and channel monitoring through the established VPN. In this way, encryption, authentication, integrity and non-repudiation of the data are obtained, achieving a reliable and secure communication between the PE and the central station.

Raspberry Pi Zero (RPZ) is the center of the core module. This was chosen for its technical specifications, high processing of its Central Processing Unit (CPU), and low cost. The RPZ gives us the flexibility, stability and reliability for the programming languages used in the system software and the ability to become a client of the VPN server, without affecting its level of processing. In addition, its general purpose Input/Output interface (GPIO) allows easy connection to the button module.

B. Virtual Protocol Network

A VPN adds a secure remote extension of a private local area network using a public network. This is done through a point-to-point virtual connection between two devices or more. The connection establishes a secure remote link between the devices, using hash functions, encryption methods and authentication [10]. Thus the remote devices are part of the private network and can be added the same policies of management of the network.

To establish a VPN there are several protocols, each with its advantages and disadvantages. The Internet Engineering Task Force (IETF) established the Transport Layer Security (TLS) protocol to consolidate SSL certificates into a single standard protocol. The SSL / TLS protocol provides security and trust by working in a transparent way for the user [11].

An open source SSL / TLS is used. OpenVPN is software that implements remote connections at the link layer or the network layer making it ideal for wireless networks. The software creates a TUN/TAP virtual interface to establish the connection. This connection has all the essential characteristics to provide security to the data. Security is granted by the use of two methods: the first is with static pre-shared keys and the second is with the use of RSA certificates and keys, which also allow authentication [12]. Thus, this software provides reliability, stability and proven encryption mechanisms.

OpenVPN works with diverse configurations for its implementation, which allows customizing the behavior of the communication channel. In this work, several parameters that are highly relevant to the performance of the network and CPU performance of the RPZ has been chosen, such as: encapsulated the packets in layer three with Tun device, upper limit of the size of the packets of 1280 bytes, fast compression LZO, encrypt the data channel packets with AES-256-CBC algorithm. The other features were chosen by the OpenVPN documentation recommendations [13].

C. System Protocol

There are several protocols and methods for the transmission of emergency events in security systems [14], in this work; Contact ID protocol (CID) of ANSI / SIA DC-09-2013 [15] has been used. The CID is well recognized in the security systems industry, as it establishes a standard for sending emergency signals when using the public Internet network as a communication channel.

The CID is independent of the type of protocol data unit (PDU) used in the transport layer of physical access, so it can use connection-oriented protocols (TCP) or protocols connectionless (UDP), and when working together with the network layer allows establishing IP Sockets. UDP was chosen for the security system since a simple transmission/confirmation sequence is used for communication.

In the same way, the CID establishes two types of messages required for our system: emergency events and link monitoring. Among other parameters, the emergency event message contains an identifier code to determine the
type of emergency required. As shown in Fig. 2, when transmitting a message from our PE to the central station's CSR, it will translate the codes and send an ACK to confirm receipt and interpretation. Otherwise, if the PE does not receive the confirmation, it will forward until receiving the confirmation.

![Diagram of Protocol Communication Sequence for the Alarm System](image)

Figure 2: Protocol Communication Sequence for the Alarm System [15].

The monitoring message is configured to determine the state of the link between the PE and CSR. For this, the PE periodically sends a message with a null identifier code, which is called a null message, in order to verify the link state.

D. System Software

The RPZ uses an operating system (OS) based on Linux, Raspbian Jessie Lite. Raspbian Jessie Lite is a lightweight version of Raspbian and is based on Debian Wheezy which delivers higher RPZ performance. The OS logon configuration was disabled to enforce system security. Also, the IP address configuration was established to access the WLAN of the rural area router.

The system software was developed in the following programming languages: Python and PHP5. As shown in Fig. 3, it is divided into three processes. The first process verifies the state of the connection to the VPN server, located in the central station. The second process checks connection status of the CSR and processes transmission and reception of messages, with CID codes, via Sockets. The third process gives constant reading to panic buttons.

![Diagram of Alarm System Multithreads](image)

Figure 3: Alarm System Multithreads
The software initiates its operation when the remote connection of the PE to CSR is established. When both equipment are connected, all three processes begin. In the first process (PTH1), the central module sends a ping every ten seconds to the VPN Server. If there is a response, PTH1 remains in a latency state. Otherwise, PE will enter a state of alert, which is indicated to the user by a led indicator and PTH1 will send ping every three seconds until obtaining a response from the server.

During the second process (PTH2), the PE checks the link with CSR. This is done by sending the link monitoring message. For this, PTH2 sets up the null message in ASCII code. Thus the process transmits the null message each time the monitoring interval elapses. If a reply message exists, it enters a latency state; otherwise, it forwards a message every three seconds until CSR response is received, and the user is indicated to be unmonitored by using the respective led indicator.

The third process (PTH3), is the coordination between the reading module and central module. The reading module is expecting some change in the GPIO pins of the panic buttons. When a change occurs in the pins, the module determines which button was pressed and sends this information to the central module, specifically to PTH3. PTH3 places PE in a state of emergency. In addition, the process build and sends an emergency event message, with the corresponding CID code. PTH3 waits until the reception of an ACK frame to confirm the reception of the emergency event, by the CSR. Without confirmation, the frame is resent every five seconds.

### III. System Results

The panic button system was implemented in a prototype that was used to evaluate and analyze the different operating cases. In [16], it is pointed out that integral evaluation of the system must be performed in two aspects: (i) management of the system and (ii) technical performance. The first is based on parameters such as: false calls, legal and community considerations. In this study, the management of the system is not evaluated, since extensive analysis is required to solve it. However, currently this aspect is being analyzed.

In regard to technical analysis, with the support and collaboration of technical staff of SIS-ECU 911, evaluation was carried out following a similar approach presented in [17].

Evaluation process was based on four test scenarios. The first measured the performance of the wireless VPN; the second evaluated the Internet connection and VPN server; the third analyzed the monitoring process of communication with the CSR; finally, the fourth scenario checked the operation for an emergency event. The network topology is shown in Fig. 4.

![Network Topology for Panic Button System’s Evaluation](image)

**Figure 4: Network Topology for Panic Button System’s Evaluation**

#### A. First Evaluation Scenario

This scenario reports the performance of the VPN. For this, the performance and latency of the virtual network was measured. Each test was repeated ten times and a flow of continuous datagrams was sent in a time cycle of One hundred and twenty seconds. The results (average values) are detailed in Table I.
Table I: Comparison for Traffic Generated in wireless VPN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Frame width (bytes)</th>
<th>Packages per second (PPS)</th>
<th>Network Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>64</td>
<td>581</td>
<td>427.51 Kbps</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>803</td>
<td>1.002 Mbps</td>
</tr>
<tr>
<td>Latency</td>
<td>64</td>
<td>581</td>
<td>26.13 ms</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>803</td>
<td>36.38 ms</td>
</tr>
</tbody>
</table>

Measurements show the maximum rate at which no discard of the frames sent in the PE occurs. That is, with a frame width of 64 and 120 bytes, the throughput is 427.51 Kbps and 1.002 Mbps, respectively. In addition, results show the positive correlation between rate of packet generation at a given size and the average time for the packet to complete a round trip. Thus, at faster generation speeds, a larger queue is formed in the wireless interface, so the packet suffers a greater amount of queue delay before processing [18].

B. Second Evaluation Scenario

The scenario analyzes the recovery of the system before fall of the link for Internet access. In this scenario, a link failure occurred voluntarily, causing the collapse of VPN tunnel, causing PE to remain in a state of alert. PTH1 process was evaluated; capturing its ICMP packets until VPN tunnel link is restored. For this, attributes of the software were analyzed to restore its level of performance and recovery of the communication in case of failure. The test was repeated ten times and the mean value of these tests was used for analysis. Recoverability of the system was measured in a time of 3.0251s with a standard deviation of 0.001.

C. Third Evaluation Scenario

PTH2 was assessed by the voluntary drop in CSR. Link monitoring messages were captured and measured time for PE-CSR link retrieval. The test was repeated ten times and the average time was set at 3.01485s. In [19], it is argued that for the integrity of the link, the messages of supervision must be received in periods greater than four seconds and less than ninety seconds. Therefore, in case of a link failure, our system would have the tolerance to reestablish communication and declare the link failure to be null. Thus, the system capacity maintains a stable performance within the conditions established during the fault periods that allow for reliability.

D. Forth Evaluation Scenario

The fourth scenario determined the operation of the system by simulating an emergency event. This verifies PTH3 process for the transmission and reception of the event message and its confirmation with its ACK. By prompting a transmission failure, the forwarding messages were captured. Thus it was verified that before an emergency event the emergency datagram arrived at the CSR. Also, for a good operation of the system, emergency events were stimulated, which caused the prototype and system to operate successfully and efficiently with a reliable communication link.

On the other hand, the user's easy interpretation was evaluated when a PE was with and without a monitoring service by the SIS-ECU 911. After a brief explanation to a group of users, they were consulted about its functionality and quality of use. The results were satisfactory for the prototype as it operates efficiently with reliable and stable communication. However, users made advices on the PE interface, for example in button size.

IV. Conclusion

This work presents an improvement to the monitoring of community security, in rural areas like Pucará. Panic button system transmits emergency event information in real time. By means of three buttons dedicated to emergencies in the management of fire accidents, healthcare and incidents of citizen security. The system allows the transmission of an event automatically and with an easy interaction with the user.

The evaluation of the system defined the advantages in reliability, stability and ease of use which focused the interest of the national security institutions. Due to the flexibility and reliability of its communication channel allows an immediate response to an emergency event providing greater efficiency and quality in emergency care. In addition, its ease of implementation and low cost allows it to be affordable to poor people in rural areas. Likewise, the proposed system can be applied to the monitoring of both rural and urban spaces.
Acknowledgment

The authors are grateful for the support of Salesian Polytechnic University of Cuenca-Ecuador and the Integrated Security Service ECU 911 of Cuenca-Ecuador.

References


[12] Baldessari, M. OpenVPN 101: introduction to OpenVPN.


