FMDB *Transactions on Sustainable Computing Systems*

Design of A Ground Based Surveillance Network for Modibbo Adama University, Yola

Wycliffe Kanyimama[1, *]

[1]Department of Computer Science, Kebbi State University of Science and Technology Alerio, Nigeria.
ksustapgs@gmail.com[1]

Abstract: The need for safety is universal in today's society. Surveillance has emerged as an important tool in the fight against terrorism and other forms of criminality in a world that is increasingly seen as unpredictable and unsafe. Sharing information amongst security organisations during a crisis is vital to saving lives and avoiding mishaps. There has been a public outcry to the University government at Modibbo Adama University (MAU), Yola, seeking immediate answers to the rising crime rate. The institution has tried many different manual security protocols in an effort to protect its students, faculty, and staff, but none of them have worked. The norm recently has been armed robbery, among other crimes. IP surveillance systems deployed on the ground, in light of this, can plug these security holes. IP surveillance on the ground is a system of cameras placed strategically around public areas with the purpose of recording and analysing video of the activities taking place there. IP cameras are integrated into the network's design alongside routers and switches to capture high-quality digital video. The designer gathers information through observation and direct contact with the target audience. The designed IP Surveillance system is subdivided into sub-management units, providing flexible, scalable, and cost-effective solutions suitable for Local Area Networks (LAN). With IP-based video surveillance, security personnel can monitor and record video remotely via a sub-LAN network arrangement. The network was simulated using a packet tracer machine to ensure the scanner's and camera's connectivity. IP surveillance offers many benefits previously unavailable with analogue Closed-Circuit Television systems.

Keywords: Ground Based Surveillance; Network; Modibbo Adama University; Closed Circuit Television systems; Local Area Networks (LAN); Nigerian Government; Charge Coupled Device (CCD).

Received on: 12/11/2022, **Revised on:** 10/01/2023, **Accepted on:** 15/02/2023, **Published on:** 05/03/2023

Cited by: W. Kanyimama, "Design of A Ground Based Surveillance Network for Modibbo Adama University, Yola," *FMDB Transactions on Sustainable Computing Systems*., vol. 1, no. 1, pp. 32–43, 2023.

1. Introduction

Humans have always placed a high value on their own lives and the lives of their loved ones. Their property is the next most valuable thing. More than ever before, law enforcement organisations around the world are relying on technological systems to improve operational capacities, expand the reach, and lower the cost of their efforts to prevent crime. Consequently, many nations have installed public surveillance systems. A country's capacity to control its borders is crucial in preventing crimes and terrorist acts. By controlling access to their territory, countries can reduce the risk of crime and terrorism Deisman [2]. Recent innovations and technologies have contributed to adopting security perimeter and access controls designed at government and business facilities to detect and screen any security breaches. Recently, the Nigerian government, through the National Assembly, has been worried over the non-compliance of contractors to install Closed Circuit Television (CCTV) cameras in Abuja and Lagos; these efforts are aimed at protecting the citizens against acts of crimes and terrorism [1]. As Taylor and Francis [9] rightly said, the desire for security permeates modern life and technology. Surveillance has emerged as an important tool in the fight against terrorism and other transgressions in a society that is increasingly seen as unpredictable

*Corresponding author.

and unsafe. There have been various innovations in security to safeguard homes and businesses from would-be murderers and terrorists [4].

Security guards have always been employed by institutions like universities, factories, and government agencies to ensure the safety of their buildings and grounds. These security guards, like police officers, are employed for the same reasons: to keep the peace, protect people from harm, and stop theft. Technology has adopted the guard culture of today, hastening the transition of our inventive system into the digital world, where the computer is the control hub for all information. The emergence of the solid-state video camera in the 1980s was the single most important development in the field of videography at that time. Solid-state cameras using Charge Coupled Device (CCD) image sensors quickly supplanted tube cameras as the standard for new security installations in the early 1990s [8].

It wasn't until the late '90s that computers started being used in tandem with video security systems. After the terrorist attack on Bishopsgate in 1993, the Ring of Steel, a network of cameras, was installed to watch over the major gateways into London. This system was connected to the citywide network of surveillance cameras [5]. Everything was a solid-state component. In order to edit and store video pictures, digital video technology requires massive amounts of digital memory. Compressing video signals before to sending them over the internet's current network channels is necessary for achieving satisfactory video image transmission and storage. With the help of recent advancements in ICT, the scope and depth of surveillance have grown significantly in recent years. In fact, it is being done on a much larger scale and with much more organisation and the use of technology than ever before. Body scan X-ray machines have recently been tested by the Australian government as an alternative to pat down checks for the detection of weapons and explosives worn or carried by passengers [3]. While X-rays have been used for medicine for over a century, many countries are just now starting to implement the technology at their borders to increase security.

This study deploys three different technology approaches to achieve the expected result. These technologies are the use of digital IP cameras to acquire video images, the use of X-rays to scan all objects coming into the system or at the entrance, and the technology of internetwork cameras and scanners. The driving notion is to harmonise a system so that each IP camera sends stream images captured to the operational and administrative centre, where the security monitors movement remotely. The entire system is expected to ensure high security in the university community.

1.1. Statement of the Problem

Security has become a concern around the globe, and governments, organizations, and individuals are worried about the state of security of our communities. Many lives and properties have been lost just because proper measures of surveillance have not been put in place [7]. Ground-based Advance surveillance has significantly reduced lost life and property in developed nations. One potential end state is a full network of surveillance integration that can prevent crimes and terrorism through a proper video surveillance system within the university. The check-points mounted are manually carried out and associated with human errors, weakness and time wasting. Another element is the corruption that the road user and security agency exhibit at our check-point, where a paltry sum or familiarity gives one a pass without checking who and what they are carrying. Computerizing the check-point (University Gate) and mounting IP surveillance can solve these problems because IP surveillance networks store all activities online on the check-point and spaces. This would greatly prevent crime and terrorism because it is the most efficient and effective way of monitoring movement, reducing the time wasted at check-points and associated corruption.

1.2. Aim and Objective

The study aims to design a ground-based security network surveillance to enable monitoring of people as they move in public spaces.

1.3. Significance of the Study

Surveillance systems are of great importance and have attracted worldwide attention since they were used to track many crimes and terror attacks; the recent was the tracked movements of two attacks on January 09 2015, in the office of Charlie Hebdo in Paris that left 12 persons dead in France, which was tracked by surveillance (Hanna and Haddad, 2015). Despite their usefulness, most current surveillance systems only provide reactive security by enabling the analysis of activities after the terrorist attack or crime has already occurred. This study provides proactive security measures to help prevent future attacks because the system allows only scanning of objects before entering the university. The study will be of great value to security personnel in managing security at the University check-point/gate to ensure proper screening and detection of unwanted objects moving into the university system. Time and operation cost are reduced as accessibility to the university are easy and faster. It will serve as reference material and a model for ICT practitioners wanting to improve security systems.

1.4. Scope and Limitation of the Study

The study is limited to ground-based security network surveillance design for the Security Unit, Modibbo Adama University (MAU), Yola, Adamawa State. The University gate, Administrative block, School of Management and Information Technology (SMIT), School of Pure and Applied Science (SPAS), School of Agriculture and Agric Technology (SAAT), School of Environmental Studies (SES), Commercial centre and major roads of the university would be considered under the surveillance network designed.

2. Methodology

2.1. Introduction

When it comes to networks, there is no such thing as a "one size fits all" rule or solution. However, in the face of complex network design, it has been found that understanding the key design factors has helped identify the most critical components needed to confront the complexity of the network and create a solution that fits those key design considerations [6]. The steps and strategies taken to accomplish the mission are outlined in this section. The paper highlights technologies and specifies tools needed to achieve the goal of designing a surveillance network system for MAUTECH.

2.2. Design Objective

The study revealed that the Modibbo Adama University of Technology, Yola surveillance system and security check-point at the gate are presently operating manually and, therefore, are associated with security lapses such as waste of time, poor screening of objects and other human errors. The ground-based surveillance system is a technology that cuts through these problems associated with manual security surveillance systems. The design objective is to design an automated network surveillance system which can detect baggage imagery and scanning that can detect the presence of firearms or explosive devices and other dangerous items at check-points and to prevent security threats to the university community.

2.3. Research Design

This study is required to analyze and determine whether the new system's design is technically, operationally, socially and economically feasible and beneficial to the university security department. However, observation has it that the university network system is not formally designed to carry large data; therefore, there is a need to design a logical and physical surveillance network with a technology capable of carrying images, frames and video streams. The information from the security department and operational security system is to be obtained through observation, physical examination of the system and secondary data from the university security unit. This is because the study's success depends on well-collected and analyzed data.

2.4. Network Requirements

Before beginning a network design, requirements should be clearly articulated and defined; yet, it is not uncommon for a network designer to need to clarify some specifics as the design progresses. The basic objective is to design an IP Surveillance network which connects all the IP cameras with a server in the security Administration Building. The body scanner at the university gate is also directly connected to the server at the security department. The IP cameras are installed within an interval of 50 meters from each other, from the University gate to the security Administrative building. Each camera has its clear standing video zone that has to cover, capture and record a particular space base on the topological nature of the road. Other requirements are: The IP cameras can receive power through the same data cable in the Network, Power over Ethernet (PoE). The IP Vision 4 classes C (192.168.1.0) is adopted. This is to enable for manageable subnet and host to meet up with the future growth.

2.5. Modeling Approach

The Data Flow Diagram and chart models represent the design and how the system would operate and processes to ease understanding and provide an exact snapshot of the procedures involved in the proposed surveillance system. This study's use of graphs, algorithms, flow charts and maps is an essential requirement in the network design. This graphical representation and diagrams are needed to simplify designing the ground-based surveillance network. The system uses flow charts, diagrams, and topographical maps of the study area to illustrate further and maintain consistency in the model. System modelling is a paradigmatic approach to represent the developed surveillance system that integrates different methods and techniques coherently with the theoretical constructs of the designed surveillance. A modelling language creates related guidelines on how the system operates.

2.6. Design Tools

Microsoft Visio and Smart Draw for Network Architectural Design are used in the design model. The study also uses Packet Tracer to detail and simulate the network. Dude software is used to monitor the connectivity of the network. However, the Prototype model and flow chart are important for further illustrating the activities of video streams moving on the network. Some of the tools are:

- IP bass camera(Network Bullet Cameras (IP8362), CISCO Switches and router, Servers and storages, Ethernet and Fibers cables)
- Arc Mapping application that provides the network physical view
- Router Information Protocol (RIP2)

Software for modelling and simulating network behaviour in order to conduct experiments. Packet Tracer enables complicated technological concepts with its simulation, visualisation, writing, assessment, and collaboration features, making it an essential part of the Networking Academy's overall learning experience. Packet Tracer is a useful adjunct to real-world hardware because it enables network architects to set up a virtual environment with an almost infinite number of nodes for the purposes of experimentation, learning, and fixing problems [10]. Designers can improve their problem-solving, critical-thinking, and decision-making abilities in a simulation-based learning environment. Consistency and effectiveness are maintained with the help of all these instruments.

3. Results and Discussion

3.1. Introduction

In this study, we take a look at the findings and examine the implications of the surveillance network layout. The researcher discovered nearly ideal graphs while looking for a class of graphs with desirable qualities for use as computer networks. The design's simplicity and recursive implementation are highly prized since they prevent the need to rewire the network whenever a new node is added. Another characteristic is that every other vertex is connected to the central vertex (MDF or the based station). Third, there must be many paths between every pair of vertices (for redundancy) and some of these paths must have small distances to minimise communication lag. The graphs ought to be cohesive and well-connected.

3.2. Analysis Existing Security System

In 1982, the MAUTECH security team was formed to serve as a local night watch force. This section reports directly to the Vice Chancellor. Since its foundation, the Security Unit has undergone numerous adjustments in response to environmental dynamics in order to meet the societal security and safety demands of the institution as a result of rising student involvement in criminal activity. The purpose of the restructuring is to increase safety on campus as a whole. A Chief Security Officer (CSO) reports to the Vice Chancellor and is responsible for the day-to-day operations of the unit. Various sections of the department are responsible for various aspects of security. The General Operation section ensures that the campus is safe for students and staff. This section provided around-the-clock security for all campus facilities. Vehicle searches, patrolling high-risk areas both on and off campus, police permanent campus fixtures like streetlights and large generators to deter theft of their components, and, of course, the customary manual patrolling of buildings like classrooms and administrative offices.

3.3. Communications and Traffic Unit

The Security Office serves as the headquarters for this organisation. All other campus wireless networks connect to this one main hub. The cone communicates with the zonal commanders and the shift leaders, respectively, and gets information from them. The Communications Unit has access to a walkie-talkie, cell phone, and other security signs, allowing them to get in touch with other campuses and spread information. While the traffic unit regulates the flow of vehicles and pedestrians entering and leaving the campus, this section is on duty around the clock. It provides social services by rushing to the scene of emergencies like car crashes on campus.

3.4. Intelligence and Crime Unit

The Intelligence Group has a sizable security force. These individuals, who are always in mufti, are dispatched to various locations across the university to collect data. They manually relay information from the Head of the Intelligence Unit to the CSO so that appropriate measures can be taken. This section's staff members transmit intelligence to the Vice Chancellor via the CSO, updating the University administration on breaking news as it happens. All incidents of criminal or security nature that are reported or discovered on campus are dealt with by the crime unit. When a prima facie case exists, it influences the

arrest, interrogation, and recommendation of punishment against the perpetrator. It communicates with law enforcement in order to pursue legal action against offenders who occurred outside of the University's authority.

3.5. Local Control and Surveillance

The MAUTECH security operations and surveillance systems are manually carried out; however, this does not completely remove the use of computers in report writing and data processing. The surveillance section comprises security men drawn from the security unit with intelligence capabilities, who manually watch over the campus and gather essential information on wa. The section is nonpartisan and straightforward in-service delivery. The surveillance team members are known in the security circle as undercover agents. They are coded in Eagles for the operative and the head of the surveillance team. They are involved in operations to gather concise and up-to-date information, which could be promptly disseminated either verbally or via report writing to the University management. Other functions of the team are nipping in the bud of fraudulent, nefarious and surreptitious activities which may involve staff and students' sharp practices for the management to take action.

3.6. Data Flow Diagram

This is the representation of the flow of data through an information system. The sensor surveillance network data flow depicts the data flow within the network. However, the designed surveillance network is a one-directional network flow where data flows through a single patent. The data flow below shows that all frame and videos captured are viewed and stored at the sub-based station and then forwarded to the main control station (MDF) where the database stores large frames and videos. Only the control station's main user can access the database and edit or review a passing event. The technology is designed to receive alerts in the sub-control station (IDF) and then forward them to the main station (fig.1).

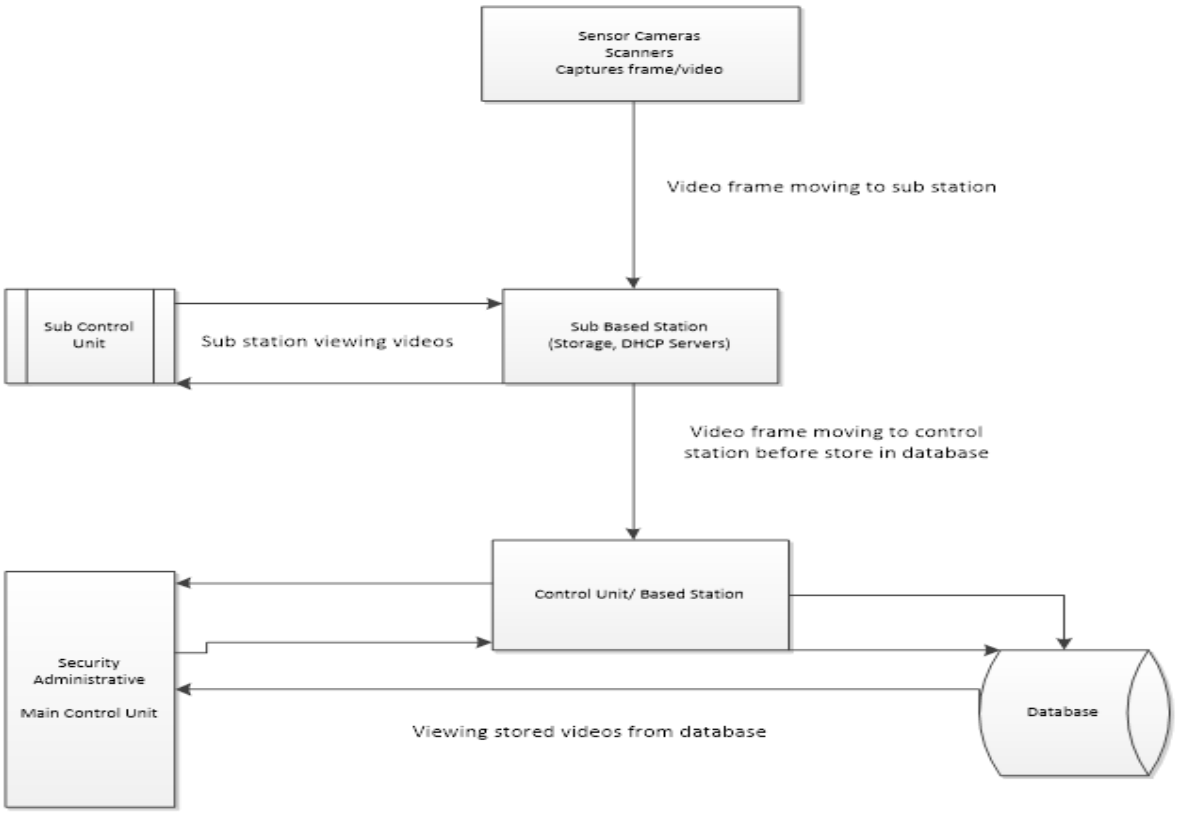

Figure 1: Propose Data Flow of the Surveillance System

3.7. Connection and Power over Ethernet (PoE)

At the access layer, the camera receives power through the same cable used for the data and the switches are powered through solar energy, which provides power to the cameras. Removing the power cabling requires another cable installed for power;

therefore, connecting the cameras with Power over Ethernet (PoE) has reduced cost and complies with the IEEE 802.3af standard. While at the distribution layer, the devices are connected with fast Ethernet. The Intermediary Distribution Facilities (IDF) are located under the distribution layers. In the core layer, the designer used fibre cables. Fibre provides speed communication and volumes of data at a time. Also, the Main Distribution Facility is located in the core layers where the overall video of the system is collected and stored. With Power over Ethernet (PoE), a network camera can get its power from the same Ethernet cable that carries data. With many network cameras connected, the need for power cabling is eliminated, saving both time and money during the cable installation process. PoE is used to connect a network adapter or switch to the system. The surveillance network currently makes use of general IEEE 802.3af compliant PoE devices. (fig.2).

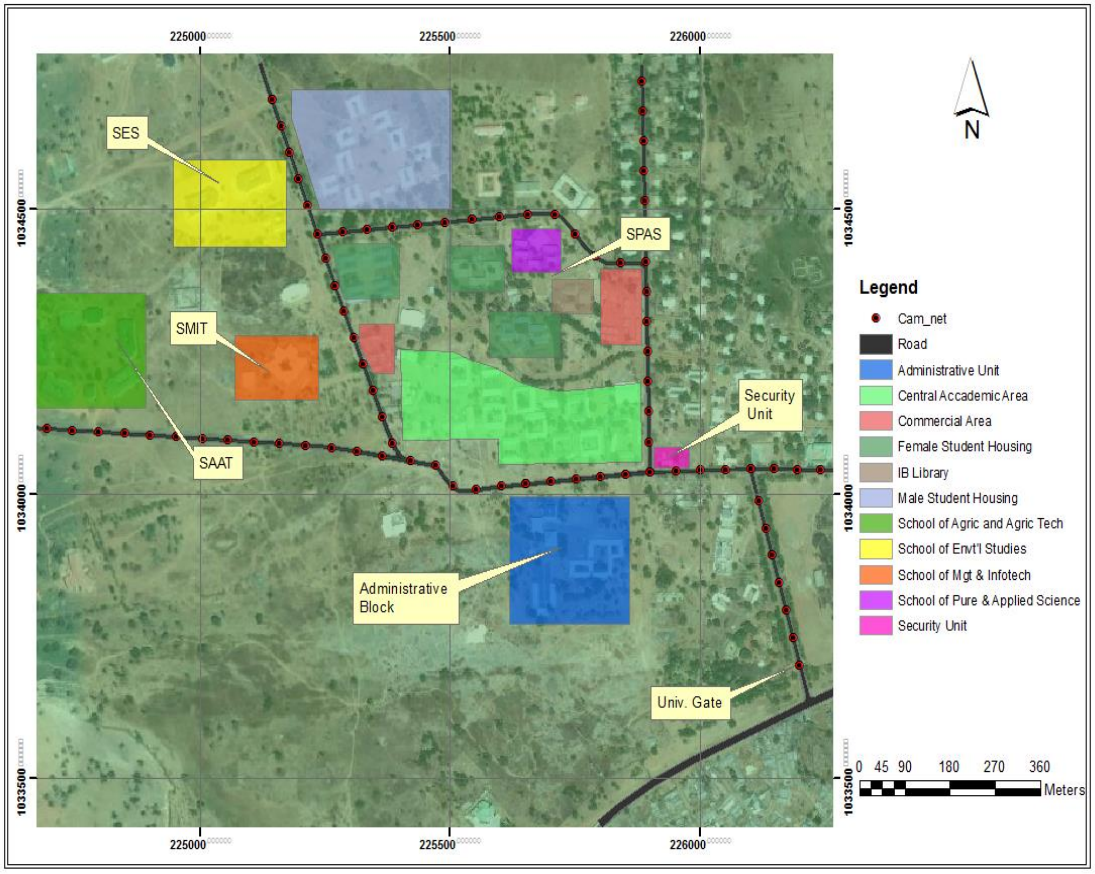

Figure 2: View of Surveillance Area Designed Scope

3.8. Surveillance Area Designed Scope

The above view provides the overall area covered under the surveillance network. The designer groups the above geographical area into clusters or small networks (subnet) to allow for the management of the enter surveillance system. From this view, the designer divides the area into six (6) logical networks. The University gate to the security unit is network one, the Administrative block is network two, SPAS is network three, SMIT is network four, SAAT is network five, and SES is network six. All these networks cover the roads attached to the network.

3.9. Routing Information Protocol (RIP2) and Converged Technique

The aforementioned logical architectures result in a setup with seven networks and five routers. In the event of a link or hardware failure, each network includes numerous gateways to quickly restore service. Routers need to swiftly update routes that are reachable through the routing table if a destination is no longer accessible through the designated interface. As a result, the routing tables in all routers need to be updated if the topology of a network changes due to reconfiguration or failure so that data may be reliably forwarded to its intended destination. Every 30 seconds, the aforementioned five routers update their neighbours on the routes they're taking. By exchanging data with its neighbours, each router eventually gains knowledge of networks further afield. The routing table maintains an accumulated distance vector for each network entry, which indicates how far away that network is in a specific direction. Routing tables are replicated at regular intervals using the RIP2 distance

vector routing algorithm. Routing updates are sent periodically to relay topology changes between routers. Before transferring video, the router takes into account factors including cost, number of hops, and reliability to the next network (fig.3).

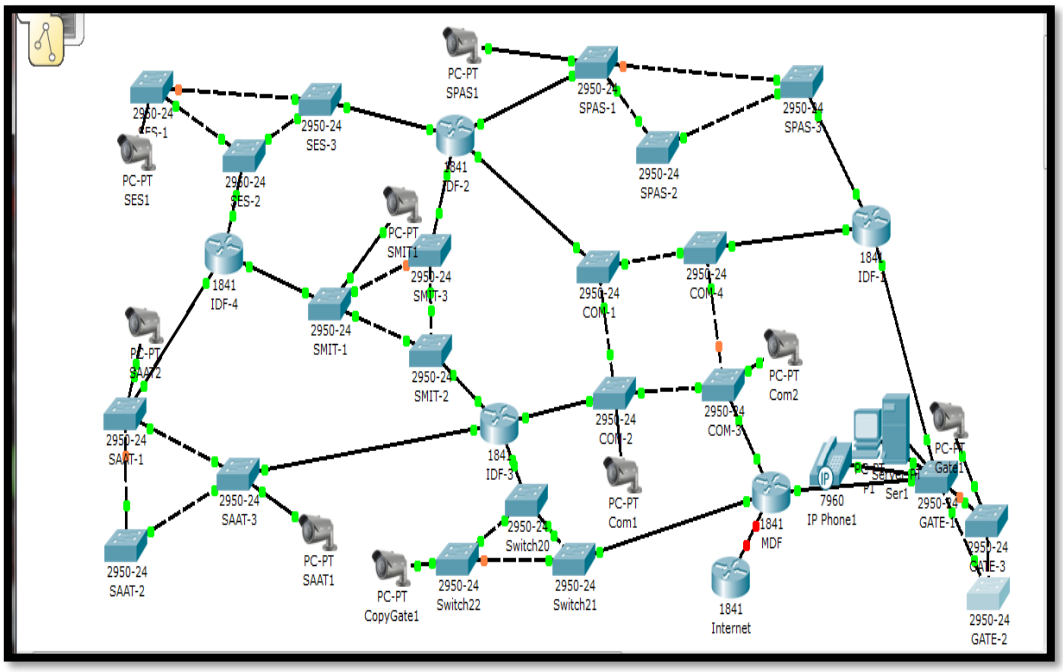

Figure 3: Physical Design View Using Packet Tracer Simulator

3.10. Routing Configuration

The above-simulated network is submitted or segmented into seven networks using five routers that connect these networks. Each subnetwork has more than one gateway through which information can move freely if one link is down. All five routers are configured with Router Information Protocol Version 2 (RIP2). This is to ensure the reliability and flow of videos.

The MDF router is connected to three networks and the internet, with the RIP2 configuration as

Router(config)#router rip
Router (config-router)#version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.1.32
Router(config-router)#network 192.168.1.192

The IDF1 router is connected to three networks, with the RIP2 configuration as
Router(config)#router rip
Router (config-router)#version 2
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.1.64
Router(config-router)#network 192.168.1.192
The IDF2 router is connected to four networks, with the RIP2 configuration as

Router(config)#router rip
Router (config-router)#version 2
Router(config-router)#network 192.168.1.64
Router(config-router)#network 192.168.1.192
Router(config-router)#network 192.168.1.96
Router(config-router)#network 192.168.1.160
The IDF3 router is also connected to four networks, with the RIP2 configuration as

Router(config)#router rip

Router (config-router)#version 2
Router(config-router)#network 192.168.1.32
Router(config-router)#network 192.168.1.192
Router(config-router)#network 192.168.1.96
Router(config-router)#network 192.168.1.128
While the IDF4 router is connected to three networks, with the RIP2 configuration as

Router(config)#router rip
Router (config-router)#version 2
Router(config-router)#network 192.168.1.160
Router(config-router)#network 192.168.1.96
Router(config-router)#network 192.168.1.128

These configurations allow each router connected to a network to broadcast the next attached network for easy information flows.

3.11. Network Address Translation (NAT)

NAT is configured on an MDF to enable cameras and devices with internal private addresses (192.168.1.0) to communicate online. NATs are usually configured at one interface to allow the network to communicate with the internet. NAT must be configured as the outside and inside interface to access the internet. When devices on these internal networks communicate through the external interface, the addresses can be translated to 10.168.1.5 or more registered IP addresses to access the internet (fig.4).

Router # configure terminal.
Router(config)# interface fastethernet 0/1
Router(config-if)# ip address 192.168.1.2 255.255.255.224
Router(config-if)# ipnat inside
Router(config-if)# exit
Router # configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.168.1.5 255.0.0.0
Router(config-if)# ipnat outside
Router(config-if)# exit

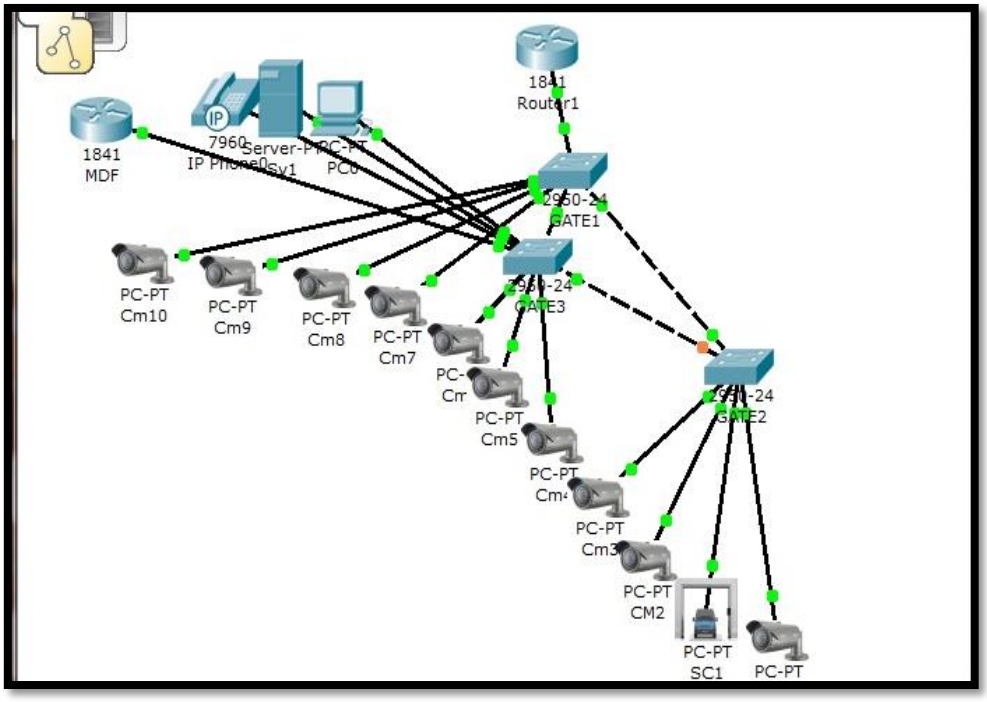

Figure 4: Gate Network Using Packet Tracer Simulator

3.12. Gate Network

The physical view of the above video network is connected with two routers and three switches for two reasons. One is to allow us to cover a range of less than 100 meters based on the road topology. Secondly, it provides reliability and more hosts to be used. The designer also uses a spanning tree protocol (STP) for redundancy.

The redundancy is required in the surveillance network to maintain a high degree of reliability and eliminate any single point of failure. Spanning Tree Protocol (STP) provides a mechanism for turning off redundant links in a switched network. STP is used here to provide redundancy for reliability without creating switching loops. The network is first connected with a scanner from the gate and has a wide range of cameras covering the road. Before entering the university, the scanner scans through any object coming in and is remotely monitored by the security control station (fig.5).

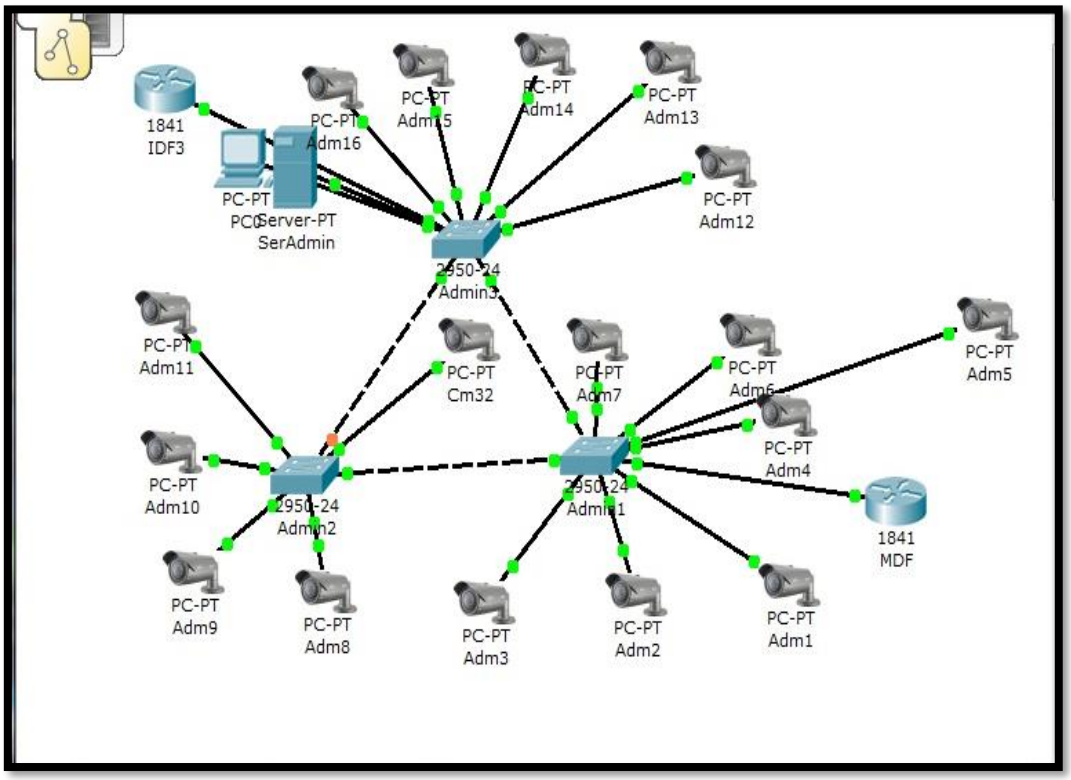

Figure 5: Administrative Network Using Packet Tracer Simulator

3.13. Administrative Network Designed Technology

In this network, just as the gate network, there are also two routers and three switches for reasons: it helps reboot signal based on the topology and allows for more host connection. The second is to create spanning tree protocol (STP) redundancy. The redundancy is required in the surveillance network design to maintain a high degree of reliability and eliminate any single point of failure.

This network has IDF, where video streams are viewed before sending the information to the MDF for storage. In this network, at the access layer, the camera receives power through the same cable used for the data. Removing the power cabling requires another cable to be installed, reducing the cost of connecting the cameras with Power over Ethernet (PoE); using a PoE supporting switch complies with the IEEE 802.3af standard. At the distribution layer, the switches are connected with fast Ethernet; the researcher uses a fibre connection in the core layer. The network address for the Administrative network is 192.168.1.32, and the gateway address is 192.168.1.33, which is also the first address in this subnetwork (fig.6).

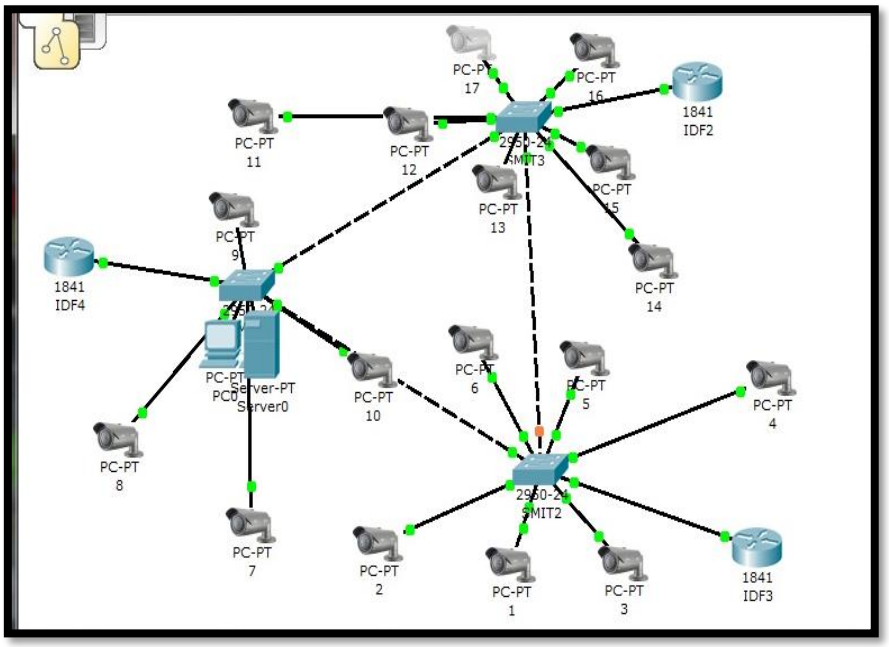

Figure 6: SMIT Network Using Packet Tracer Simulator

3.14. SMIT Network Designed Technology

There are three routers and three switches connected to the said network; each switch is connected to a router, eliminating a single failure point. The design also allows for spanning tree protocol (STP) redundancy. The redundancy is required in the surveillance network to maintain a high degree of reliability and eliminate any single point of failure. This network has IDF, where video streams are viewed before sending the information to the MDF for storage. At the access layer, the camera receives power through the same cable that is used for the data. Removing the power cabling requires another cable to be installed for power; therefore, to reduce the cost of connecting the cameras with Power over Ethernet (PoE), using PoE supporting switch complies with the IEEE 802.3af standard. While at the distribution layers, the switches are connected with fast Ethernet; in the core layer, the designer uses a fibre connection. The network address for the Administrative network is 192.168.1.96, and the gateway address is 192.168.1.97 (fig.7).

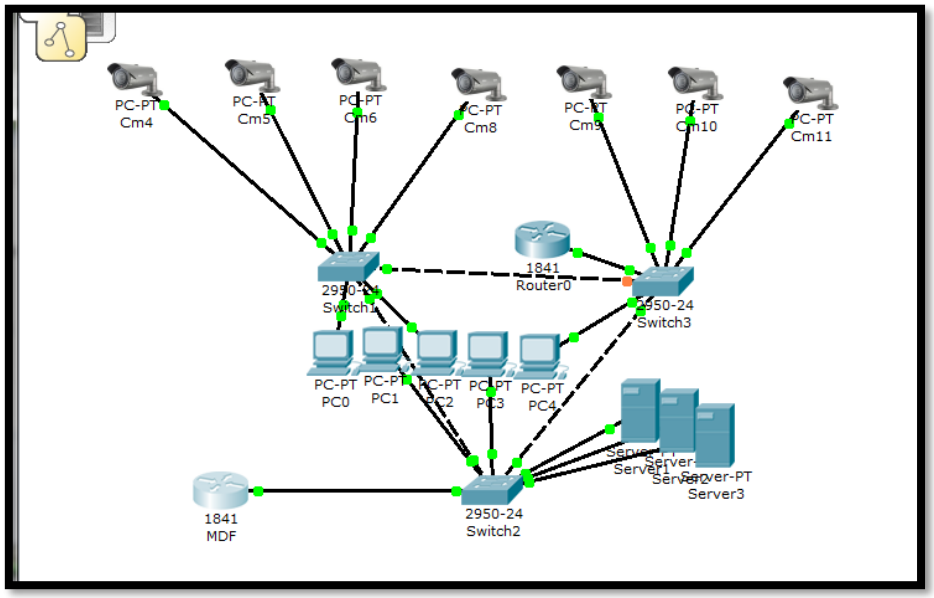

Figure 7: Physical Design View of Based Station

4. Conclusion

The crime rate in Nigeria, especially in the northeast, has escalated to a point where the public is demanding action from the government. To protect its inhabitants and their belongings, the government has tried a number of different security measures, but none of them have worked as effectively as hoped. Crimes such as kidnapping people, armed robbery, terrorism, bombings, and many others have become commonplace there. Therefore, it is imperative that the security agency use IT in order to reduce the number of human errors. Many issues can be mitigated with the use of the ground-based monitoring system. Networked cameras and scanners can now be installed in public spaces to keep tabs on and record activity there. The task has been made, the goal has been reached, and the target has been achieved. Now, the design of a ground-based surveillance network provides an evidence-based approach, which is crucial to understanding where, when, and whether different interventions prevent crime and helping establish why an intervention did or did not work. There is a strong indication that some schools in the northern part of Nigeria are at higher risk than others, and also believe that universities may soon face an alarming array of new and very serious threats of terrorism. Under these conditions, surveillance network architectural system design may be of value, but they are not obviously or universally of value. The design framework enables the screening and monitoring of people for public safety.

4.1. Recommendations

Scanners and other forms of electronic surveillance have been utilised by several affluent nations to cut crime and terrorism by as much as 80 percent. It is uncertain how effective the ground-based monitoring network is in this region at discouraging or reducing criminal activity because it is still so young. To gauge the tool's viability and popularity in public spaces, it was necessary to gauge public opinion. However, the design of the security framework includes pilot implementation and installation of surveillance cameras throughout the campus, as they are an integral part of information technology for national security. A ground-based surveillance network has been shown to be an effective management and security tool in numerous studies. The primary goals of a security system that includes a network of video cameras are crime prevention and detection. The security provided by the ground-based surveillance network is excellent. The footage can be used as evidence in criminal prosecutions and security investigations. The necessity of operational criteria, decision guidelines, performance standards, evidentiary requirements, and ground-based surveillance network operators, among other things, has been emphasised as crucial to the framework's security. The campus needs to install the Ground Based Surveillance Network system. More study is needed to develop a comprehensive Ground Based Surveillance Network security strategy for the entire campus and country. To make the most of the surveillance network cameras, the government and universities must implement a unified security system. The ground-based surveillance network has to incorporate systems like Anomaly Detection Systems for anomalous patterns, Automatic Detection Systems for face identification, and Automatic Number Plate Recognition (ANPR) systems.

Data Availability Statement: This study used online benchmark data in its investigation. This data is fresh, as displayed here.

Funding Statement: No funding has been obtained to help prepare this manuscript and research work.

Conflicts of Interest Statement: The writers have not disclosed potential bias (s). This is brand new writing from the authors. The information used is cited and referenced appropriately.

Ethics and Consent Statement: All data collection was conducted after receiving approval from an institutional review board and the agreement of all participants.

References

1. C.F. Agbal, Punchng.com. [Online]. Available: http://www.punchng.com/business/ictclinic/security-challenges-what-can-ict-do, 2013. [Accessed: 13-Sep-2022].
2. W. Deisman, CCTV: Literature Review and Bibliography. http/Users/oriopogun/Downloads/CCTV_Literature_Review_and_Bibliography.pdf, 2016. [Accessed: 13-Sep-2022].
3. S.M. Herald, Australian airport trials full body X-rays. Article of health science; from http://www.heraldsun.com.au, 2018. [Accessed: 13-Sep-2022].
4. H. Jason and H.Margo, News Report on Charlie Hebdo France attacks. http://edition.cnn.com/2015/02/17/world/france-charlie-hebdo, 2016. [Accessed: 13-Sep-2022].
5. M. Michael and N. Clive, “Close Circuit Television in London centre for criminology and criminal justice University of Hull cottingham,” Journal of centre for technology and society, vol. 5, pp. 1–10, 2004.
6. Moxa. CCTV surveillance system Network Design Guide. www.maxo.com/product, 2015. [Accessed: 13-Sep-2022

7. C. Steven, Report on Nigerian explosion. Voice of America; www.voanews.com/a/explosion-rock-nigerian-town/250683.html , 2015. [Accessed: 13-Sep-2022].
8. S. Livingston, Africa's Information Revolution: Implications for Crime, Policing and Citizen Security Africa Center for Strategic Studies. 2013.
9. F. Taylor, Surveillance and security technology politics and power in everyday life. 2016, [Accessed: 13-Sep-2022].
10. T. Lammle, Cisco Certified Network Associate Study GuideSYBEX Inc. GuideSYBEX Inc. Alameda press, 2000. [Accessed: 13-Sep-2022].