Security Surveillance Architecture: The Wireless Mesh Network Approach

Ogunyinka O.I. *
Soyemi, J. **
Soyemi, O. B. ***

* Department of Computer Engineering, Federal Polytechnic, Ilaro, Ogun State, Nigeria
** Department of Computer Science, Federal Polytechnic, Ilaro, Ogun State, Nigeria
*** Department of Civil Engineering, Federal Polytechnic, Ilaro, Ogun State, Nigeria

Abstract The state of security in the country had been created a lot of panic in many areas to the extent that individuals now send a lot to protect their lives and properties. This state had not justified to a large extent the huge amount the government had spent, presently spending and had budgeted to spend in the present year on providing adequate security for her citizenry. Even at the state level we hear and see several donations running into millions of naira made by state governors to the police force just to increase the level of security in the state. However, all these had been geared towards improving the physical capability of the police force and other security agents rather than improving the technological infrastructure through the use of Information Technology to create a nationwide video-surveillance security system. A Security Surveillance Architecture will be proposed in this paper, and it is believed that it will go a long way in alleviating the security problems of our nation.

Keywords: Security, Security Agent, Information Technology, Video-Surveillance Architecture, Mesh Network.

Introduction

Mention video surveillance most people think of video cameras mounted in the corners of train stations and banks or private detectives videotaping an earring spouse for a messy divorce case. The truth is that the history of video surveillance is much more complex and goes back much farther than most people realize.
Considering video in the simplest of terms, video surveillance began with simple closed circuit television monitoring. As early as 1965, there were press reports in the United States suggesting police use of surveillance cameras in public places. In 1969, police cameras were installed in the New York City Municipal Building near City Hall. The practice soon spread to other cities, with closed circuit television (CCTV) systems watched by officers at all times.

When video cassette recorders hit the market, video surveillance really hit its stride. Analog technology using taped video cassette recordings meant surveillance could be preserved on tape as evidence. The seventies saw an explosion around the world in the use of video surveillance in everything from law enforcement to traffic control and divorce proceedings. England installed video surveillance systems in four major Underground Train Stations in 1975 and began monitoring traffic flow on major highway arteries about the same time. In the United States, the use of video surveillance wasn't quite as prevalent until the 1980 for public areas, but store owners and banks quickly understood the value of it.

Businesses that were prone to theft, including banks, mini-marts and gas stations, began mounting video surveillance systems as a deterrent and in hopes of apprehending thieves, particularly in high crime areas. The insurance industry also found video surveillance compelling worker's compensation fraud; bogus accident claims and a variety of other cases began to turn in the industry's favor when they could provide tapes of supposedly disabled workers doing the limbo at a family reunion.

For the private citizen, analog technology was primarily used in the 1970's and 1980's for capturing the worst side of human nature – cheating spouses and poor parenting. Private detectives were able to provide more graphic and compelling evidence of affairs and parental stupidity with film than with still shots, and video tapes became frequent evidence in family court. The drawback in many cases was that after a while, owners and employees would become complacent and not changes the tapes daily or the tapes would wear out after months of being re-used. There was also the problem of recording at night or in low light.

While the concept was good, the technology hadn't yet peaked. The next step was the Charged Coupled Device camera (CCD), which used microchip computer technology. These new cameras broadened the practical applications of video surveillance by allowing low light and night recording possible.

In the 1990's a new advancement in the history of video surveillance made great strides in practicality – Digital Multiplexing. When digital multiplexer units became affordable it revolutionized the surveillance industry by enabling recording on several cameras at once (more than a dozen at time in most cases). Digital multiplex also added features like time-lapse and motion-only recording, which saved a great deal of wasted videotape.

By the mid-1990's, ATM's across the United States and in most parts of the world had video cameras installed to record all transactions. After the first attack on the World Trade Center in February of 1993, the New York Police Department, FBI and CIA all install surveillance cameras throughout the area. Soon many countries are also using either CCTV or videotaped surveillance to cover major sporting events that could be potential hot spots, including the World Cup Soccer games at Giants Stadium in 1994.

Digital makes video surveillance faster, clearer, more efficient Digital video surveillance made complete sense as the price of digital recording dropped with the computer revolution. Rather than changing tapes daily, the user could reliably record a month's worth of surveillance on hard drive because of compression capability and low cost. The images recorded digitally were so much clearer than the often grainy images recorded with analog that recognition was immediately improved for police, private investigators and others utilizing video surveillance for identification purposes. With digital technology you could also manipulate the images to improve clarity even further by adding light, enhancing the image, zooming in on frames, etc.

The second wave of increased video surveillance corresponded with the emergence of digital in the United States. From 1997 on, police departments across the country installed more and more video surveillance cameras in public buildings, housing projects and areas like New York's Washington Square Park. The NYPD also began using mobile surveillance vans at political rallies and other large gatherings (including festivals and parades) under the auspices of the Technical Assistance Response Unit (TARU).

Evolution of Video Surveillance Systems

The first CCTV system was installed by Siemens AG at Test Stand VII in Peenemünde, Germany in 1942, for observing the launch of V-2 rockets. The noted German engineer Walter Bruch was responsible for the design and installation of the system. In the U.S. the first commercial closed-circuit television system became available in 1949, called Vericon. Very little is known about Vericon except it was advertised as not requiring a government permit.

CCTV recording systems are still often used at modern launch sites to record the flight of the rockets, in order to find the possible causes of malfunctions, while larger rockets are often fitted with CCTV allowing pictures of stage separation to be transmitted back to earth by radio link.

In September 1968, Olean, New York was the first city in the United States to install video cameras along its main business street in an effort to fight crime. The use of closed-circuit TV cameras piping images into the Olean Police Department propelled Olean to the forefront of crime-fighting technology.

The use of CCTV later on became very common in banks and stores to discourage theft, by recording evidence of criminal activity. Their use further popularized the concept. The first place to use CCTV in the United Kingdom was King's Lynn, Norfolk.

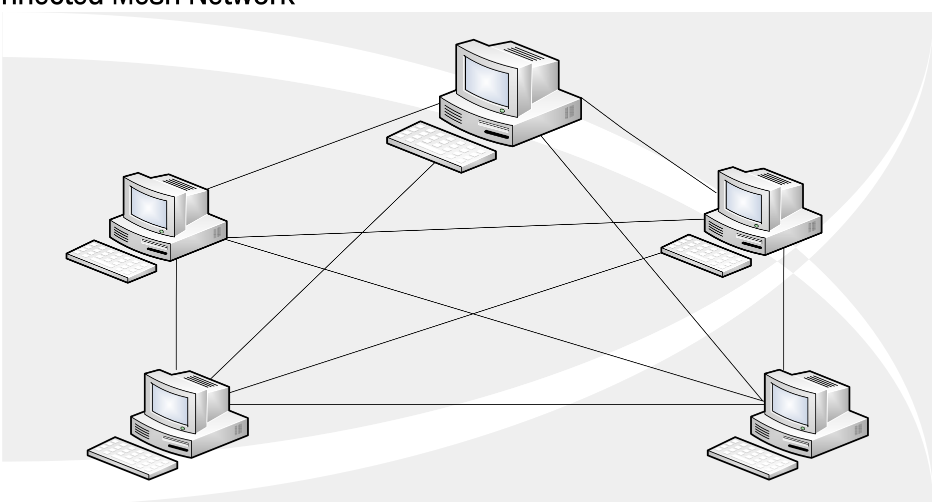
However, CCTV which uses traditional radio frequency (RF) technology, rather than photographic technology, was introduced in the 1980s and provided a more cost-effective and real-time method of video surveillance. This involves changing the recording tapes very few hours since it is the CCTV that feeds a

VHR recorder with images. But as VHS-based systems become obsolete and the production VCRs themselves were discontinued, users were forced into a hybrid solution using Digital Video Recorder (DVR) to digitally record video from analog cameras in the 2000s. But these DVRs still have a short fall, while they provide higher quality recording and faster playback they still tend to be proprietary systems with limited scalability. In this vein, corporations and government agencies had to move to an all-digital component scheme and managing Digital Video Surveillance (DVS) on their information system infrastructure, making video surveillance just another application on their IT network. Centrally controlled digital cameras will have IP addresses that can be monitored by several distinct analytical applications, enabling organizations not only to enhance existing physical security, but make more intelligent and even predictive decisions on security.
Upgrading to DVS solutions provided a significant number of advantages:

1. Major Enhancement in image quality: provide more precise identification
2. Megapixel Cameras can provide two to 16 times the resolution of traditional analog cameras. Megapixel cameras can cover a large area than analog cameras while providing superior digital zoom capabilities that show real detail instead of blurred faces.
3. Better analytics and remote cameras control allow fewer security personnel to monitor more cameras
4. With On-Demand recording, digital systems can be configured to record only when there is motion or some specified actions rather than recording hours of uneventful video or an endless loop.
5. DVS solution requires less manual intervention, since there is no need for the periodic replacement of videotapes. This not only reduces time and cost, but also operator's error causing the loss of critical images, such as by swapping and over writing the wrong tapes.
6. DVS solutions are built on scalable, flexible storage. Storage is no longer limited the number of videotapes on the disks that a company can manage. Images can be stored on traditional hard drives when necessary, and virtually otherwise.
7. Remote accessibility is the core benefit of DVS solution, in that images can be accessed from any secure computer or workstation in the network even via wireless connectivity.

As good as the DVS solution is, its wide use is limited by cost. Due to this the use of DVS solution was limited to banks, offices and generally small areas, in other to reach large areas, town and cities the need to look for a more cost effective solution with good surveillance quality become necessary.
To this end, a Wireless Mesh Network (WMN) powered DVS was introduced in the last 2000s.
Mesh networking is a type of networking wherein each node in the network may act as an independent router, regardless of whether it is connected to another network or not. It allows for continuous connections and reconfiguration around broken or blocked paths by "hopping" from node to node until the destination is reached. A mesh network whose nodes are all connected to each other is a fully connected network.

Fig 1: Fully Connected Mesh Network



As a result, the network may typically be very reliable, as there is often more than one path between a source and a destination in the network. Although mostly used in wireless scenarios, this concept is also applicable to wired networks and software interaction.

Wireless mesh networks were originally developed for military applications and are typical of mesh architectures. Over the past decade the size, cost, and power requirements of radios has declined, enabling more radios to be included within each device acting as a mesh node. The additional radios within each node enable it to support multiple functions such as client access, backhaul service, and scanning (required for high speed handover in mobile applications).

Additionally, the reduction in radio size, cost, and power has enabled the mesh nodes to become more modular—one node or device now can contain multiple radio cards or modules, allowing the nodes to be customized to handle a unique set of functions and frequency bands

.

Existing Wireless Mesh Network Surveillance Architecture

Gauge Architecture

A few architecture had been developed for surveillance with WMN been the backbone for the designs. One of such architecture is the Gauges

Fig. 2: Ganges Architecture

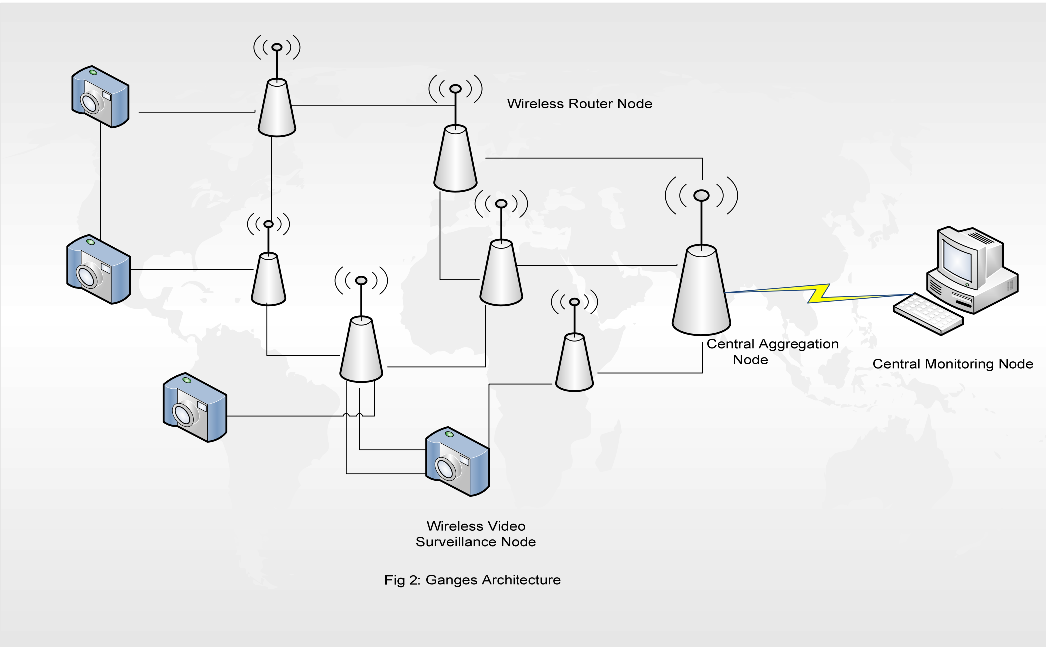


Fig 2: Ganges Architecture

The Ganges architecture consists of several identical video sources such as video surveillance spread over a large geographic region for remote monitoring purposes. They could be mounted on rooftops or lampposts that have continuous supply of electricity. These sources are equipped with a Central Monitoring Node, Wireless Router Node, Wireless Video Surveillance Node, and Central Aggregation Node wireless interface for communication. There is a central monitoring node (CMN) where video streams from all these sources needs to be viewed in real-time. Providing wired connectivity between the video sources and the CMN may be expensive and inconvenient. Due to the significant deployment advantage, we utilize a WMN to transport the video streams from each source to the nearest wired gateway node. The WMN consists of a

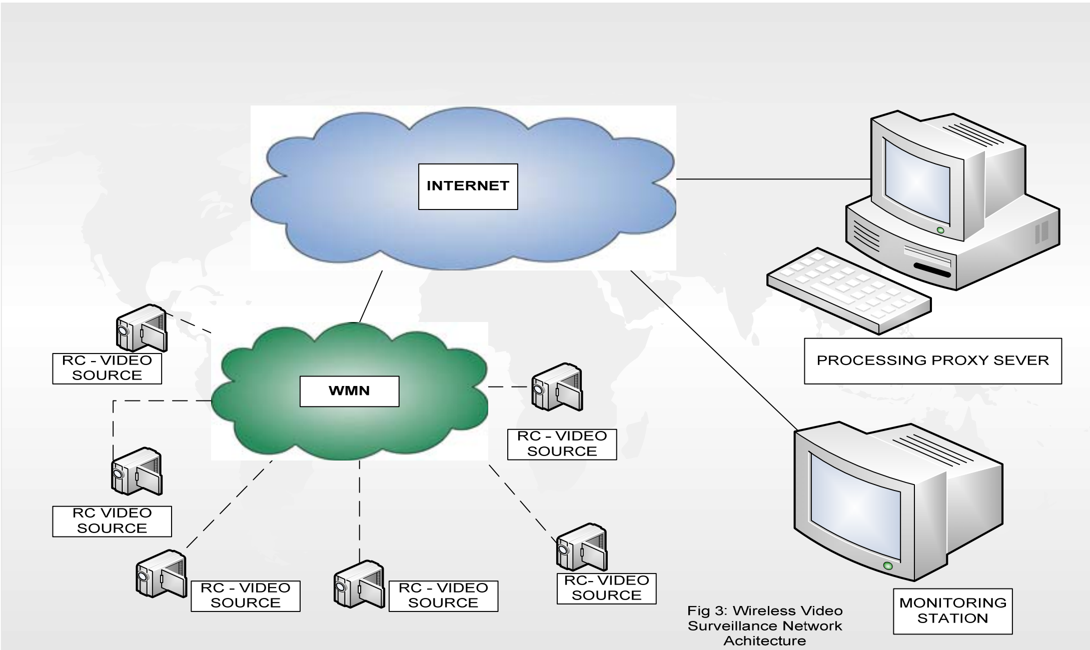
Number of low-cost wireless routers each equipped with a single wireless interface. Some of these nodes (Central Aggregation Nodes or CAN) have an additional wired interface and are connected to the CMN via the Internet or some private network. All video streams are aggregated at the CAN over wireless multihop backbone network and then forwarded over the wired link to the CMN.

Gauges was designed with specialized wireless routers that are optimized to handle real-time traffic efficiently. High bandwidth routes are established between the video sources and the CMN. These routers are capable of reliably delivering high-quality video streams to the CMN using several fine-grained adaptations at different layers to counter the dynamic wireless conditions. Optimizations at the network layer are implemented to efficiently share resources between multiple owns as well as delivering packets in time to reduce the end-to-end packet delay jitter.

Wireless Video Surveillance Network Architecture

Another is Wireless Video Surveillance Network (WVSN) Architecture.

Fig 3: Wireless Video Surveillance Architecture (Francesco, 2007)

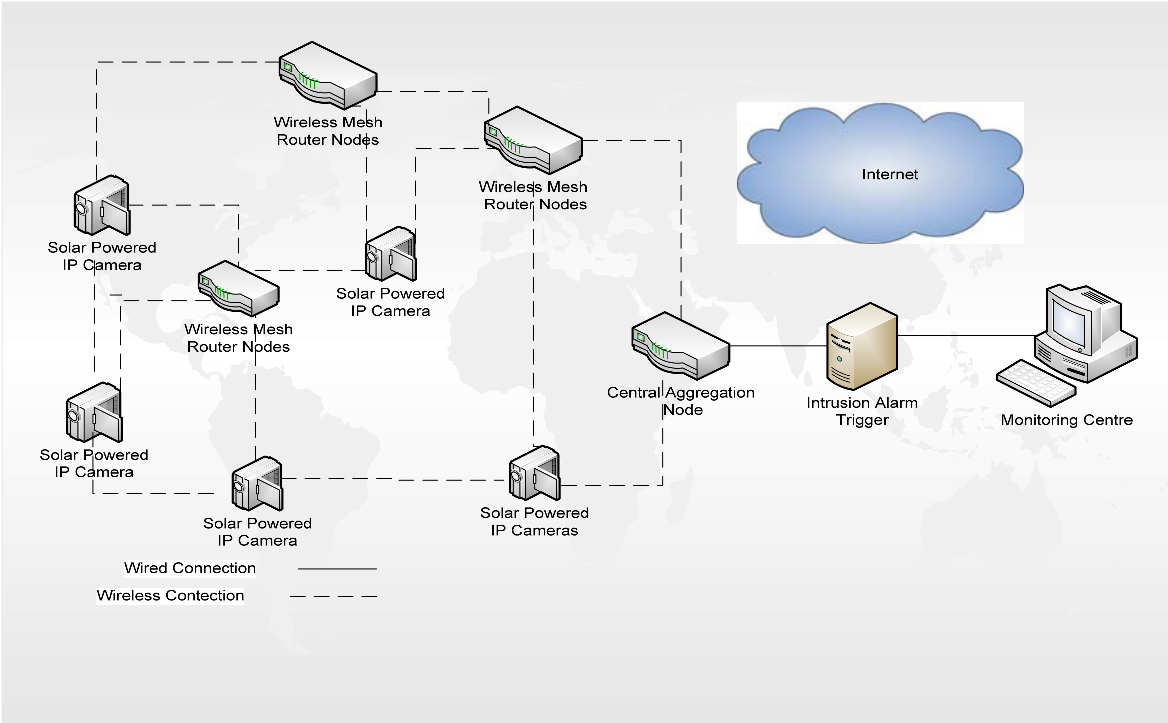


The distributed architecture consists of a number of wireless networked rate-controlled video cameras (RC-video sources) which, thanks to the WMN, access the Internet and continuously transmit their video flows to a processing proxy server (PPS) for processing and filtering. The PPS is directly, or again through the Internet, connected to one or more monitoring stations (MS). Not every video stream that is sent to the PPS for processing is shown to the end user at the MS. In fact, the PPS analyses all the received video flows, and alerts the MS only if a suspicious event is detected. The focus of our paper is concentrated on the RC-video sources (and video stream destination at the PPS) and the wireless mesh network.

Proposed Architecture

The proposed surveillance architecture consist of Solar Powered IP Cameras spread across a large area (e.g School Campus, Town) and the choice of a Solar Power is to guarantee constant power supply added to the architecture is Wireless Mesh Router node that carries the video signal across any free node to the Central Aggregation Node (CAN).

Fig 4: Typical IP-BASED Surveillance System Transmitted over a MESH NETWORK.



The CAN take a record of the entire video signal and pass them in the over serious security treats based on pre-determined conditions put programmed in the cameras. This signal will go through the intrusion alarm and if there is any security treat in any of the camera signal the alarm will be triggered and the image from the camera with the highest security bridge will be displayed at the monitoring centre and an auto recording of that event will be done. However, the monitoring centre screen as the capacity to display images from six cameras at the same time and record same.

This architecture will be part of a website so that authorized personnel form the website owner can gain access to the cameras through the WMN and view real-time images from any of the cameras as the event is happening in such areas.

Conclusion

The use of this architecture will bring about adequate surveillance to a large geographical area at a cheap rate because of the mesh network used for connection since each item on the network serves as a transmitter and receiver thereby removing the cost of repeater on the network. Comparing this architecture with other, the ability to view real time images as the events are unfolding is an advantage since it will make surveillance every body’s duty wherever this architecture is in use.

References

Anthony C. Caputo (2010). Digital Video Surveillance and Security

Clarke R. (1988). Information technology and dataveillance. Communication of the ACM, 31(5), 498-512

D. Agrafiotis, T.K Chiew, P. Ferre, D.R. Bull, A.R. Nix, A. Doufexi, J. Chung-How, D. Nicholson. Seamless Wireless Networking for Video Surveillance Applications.

David Evancha (March, 2007). The Benefits of using Digital Video-Surveillance.

Francesco Licandro and Giovanni Schembra (Jan., 2007). Wireless Mesh Networks to Support Video Surveillance: Architecture, Protocol and Implementation Issues.

Troops Network (April, 2007). Wireless Video-Surveillance with Troops Metro Mesh Network: A Business White Paper.

Lyon, D. (2001). Surveillance society: Monitoring everyday life. Buckingham Open University press.

Marx, G. (2002). What's new about the "new surveillance"? Classifying for change and continuity surveillance & societyi(1),9-29

Mason,D.,Button, G., Lankshear, G.& Coates. S. (2002). Getting real about surveillance and privacy at work. Surveillance & Society 4(1/2).

Vishnu Navda, Anand Kashyap, Samrat Ganguly and Rauf Izmailov. Real-time Video Stream Aggregation in Wireless Mesh Network

www.surveillance-and-society.org 24th of October, 2010 6.00pm

www.surveillance-source.com 23rd October, 2010 9.20am

www.video-surveillance-guid.com 23rd October, 2010 3.22pm