International Journal of Engineering Research
Volume No.6, Issue No.11, pp : 453-454

ISSN:2319-6890 (online),2347-5013(print)
1 Nov. 2017

Surveillance Networks

Matthew N. O. Sadiku, Mahamadou Tembely, Sarhan M. Musa
Roy G. Perry College of Engineering Prairie View A&M University Prairie View, TX 77446
Email: sadiku@ieee.org, tembely_madou@yahoo.fr, smmusa@pvamu.edu

Abstract-- Surveillance networks have increased in popularity the last decades as safety and security have become critical issues in many infrastructures such as power stations, airports, hospitals, and schools. They are to provide protection from a wide range of threats or attacks and serve as a deterrent to crime. This paper provides a brief introduction to surveillance networks, their applications, and challenges.

Keywords: surveillance network, computer surveillance, sensor network

I. INTRODUCTION

Network or computer surveillance is the monitoring of computer activities or data being transferred over computer networks such as the Internet. This is usually done by governments, corporations, police, and criminal agencies to maintain social control, monitor threats, and investigate criminal activities of citizens [1].

Surveillance technologies are becoming widespread today because of threats like terrorism and crime. They have become part of this era of ubiquitous computing. In fact, surveillance cameras are rapidly becoming part of the urban infrastructure in developed nations. The main justification for the presence of the public surveillance networks is that they are a deterrent to crime [2].

II. Components Of Surveillenace Networks

Surveillance systems may be static or passive, wired or wireless/mobile. A typical surveillance network is shown in Figure 1 [3]. A surveillance network may consist of IP video cameras, analysis devices, and a central node which collects information and displays. Selecting the number of cameras automatically is a high priority. The placement of cameras within a surveillance network is critical. The camera's location is described by its position and orientation. In surveillance networks, video streams are transmitted 24/7.

Wireless sensor networks offer cost effective solutions to various surveillance and tracking networks in which sensor nodes are deployed to operate autonomously in unattended environments. Wireless sensor networks (WSNs) typically consist of large number of sensor nodes with limited memory, computational and communication resources [4]. The surveillance network is comprised of a set of the devices (also referred to as nodes) collaborating to detect the presence/absence of a target by exchanging information through wireless communications. Global Positioning System (GPS) provides a common clock and accurate localization, GPS technology may not work for indoor security applications and may be too costly for large-scale sensor networks [5].

III. APPLICATIONS

Surveillance networks are mainly used for security and health.

- *Security*: Surveillance systems have spread the last decade in response to public security. They are gaining popularity in home, office, hospital, businesses, corporations, organizations, airports, power stations, schools or other security sensitive infrastructures. The networks is to enhance the protection of facilities from a wide range of threats or attacks and serve as a deterrent to crime.
- *Control diseases*: Health agencies use surveillance systems to detect and monitor chronic and infectious diseases. There is global concern about surveillance and control of diseases because the spread of infectious agents is inevitable in a world deeply interconnected [6]. Surveillance network is a network of practices or community based primary care physicians who monitor specific illness problems on a continuing basis. They are used to monitor the health of the entire population. Examples of surveillance systems include the Global Public Health Intelligence Network (GPHIN), the Program for Monitoring Emerging Diseases (ProMED), and Medical Intelligence System (MedISys). The World Health Organization (WHO) is responsible for monitoring and responding to global public health threats, but there is no comprehensive global public health surveillance system.

Surveillance networks can also be used in a smart city to provide citizens with higher-level services and ensure public security and safety. Such networks ultimately aim at the improvement of everyday city life [7].

V. CHALLENGES

New technologies are enabling global surveillance, but in addition to serious technical needs, both sustainability and data-sharing mechanisms remain challenges. Energy-efficiency is an important issue in surveillance networks, since camera sensors are always equipped with limited energy capacities.

Some surveillance networks are multinational. They work when principles of sovereignty are maintained, when trust and confidence are established, and when technical professionals can freely deliberate and make collective decisions.

Developing countries are a weak link in the global surveillance framework. In resource-limited parts of Africa, Asia, and Latin America, basic health surveillance has been lacking because of inadequate funding. In many developing countries, substantial investment has thus been made to strengthen the infrastructure through training, laboratory support, data management, and communications.

Activists around the world have developed practices and are taking distinct measures to resist cyber-surveillance. The loss of an actual expectation of privacy affects identity.

Anonymity and encryption are useful tactics that can be incorporated into the communication practices [8]. Surveillance networks have introduced themes that do not appear in the traditional form of democracy. This has brought about new categories of analysis, digital identity, devices, digital borders, etc. [9].

VI. CONCLUSION

Surveillance refers to the close scrutiny of individuals through the collection and analysis of information via network such as the Internet. The globalization of travel and commerce has led to the globalization of communicable diseases, which in turn has led toincreased need for globalization of solutions to fight the disease [10]. Research in surveillance networks is an active discipline which requires multidisciplinary expertise, including knowledge of signal processing, computer vision, communications, computer networks, pattern recognition, and sensor development [11].

REFERENCES

i. *"Computer and network surveillance," Wikipedia, the free encyclopedia.* https://en.wikipedia.org/wiki/Computer_and_network_surveillance

ii. *J. Bullington, "'Affective' computing and emotion recognition systems: the future of biometric surveillance?" Proceedings of the 2nd Annual Conference on Information Security, Curriculum Development, September 2005, pp. 95-99.*

iii. *F. Oberti, G. Ferrari, and C. S. Regazzoni, "Allocation strategies for distributed video surveillance networks," Proceedings of International Conference on Image Processing, October 2001, pp. 415-428.*

iv. *S. Akbas, M. A. Efe, and S. Ozdemir, "Performance evaluation of PIR sensor deployment in critical area surveillance networks," Proceedings of IEEE International Conference on Distributed Computing in Sensor Systems, 2014, pp. 327-332.*

v. *T. L. Chin, "Vulnerability of Surveillance Networks to Faults," International Journal of Distributed Sensor Networks, vol. 2, 2006, pp. 289–311.*

vi. *S. V. Scarpino, N. B. Dimitrov, and L. A. Meyers, "Optimizing provider recruitment for influenza surveillance networks," PLoS Computational Biology, vol. 8, no. 4, April 2012, pp.1-12.*

vii. *M. Bourmpos, A. Argyris, and D. Syvridis, "Smart city surveillance through low-cost fiber sensors in metropolitan optical networks," Fiber and Integrated Optics, vol. 33, no. 3, 2014, pp. 205-223.*

viii. *O. Leistert, "Resistance against cyber-surveillance within social movements and how surveillance adapts," Surveillance & Society, vol. 9, no. 4: 2012, pp. 441-456.*

ix. *R. J. Firmino, F. Bruno, and A. N. Botello, "Understanding thesociotechnical networks of surveillance practices in Latin America. " Surveillance & Society, vol. 10, no. 1, 2012, pp. 1-4.*

x. *M. Moore et al., "Promising pathways for regional disease surveillance eetworks," Emerging Health Threats Journal, vol. 6, no. 1, 2013, pp. 1-4.*

xi. *K. N. Plataniotis and C.S. Regazzoni, "Visual-centric surveillance networks and services," IEEE Signal Processing Magazine, March 2005.*

ABOUT THE AUTHORS

Matthew N.O. Sadiku is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Mahamadou Tembely is a Ph.D student at Prairie View A&M University, Texas. He received the 2014 Outstanding MS Graduated Student award for the department of electrical and computer engineering. He is the author of several papers.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.