Chapter XXXII
A Novel Secure Video Surveillance System Over Wireless Ad Hoc Networks

Hao Yin
Tsinghua University, China

Chuang Lin
Tsinghua University, China

Zhijia Chen
Tsinghua University, China

Geyong Min
University of Bradford, UK

ABSTRACT

The integration of wireless communication and embedded video systems is a demanding and interesting topic which has attracted significant research efforts from the community of telecommunication. This chapter discusses the challenging issues in wireless video surveillance and presents the detailed design for a novel highly-secure video surveillance system over ad hoc wireless networks. To this end, we explore the state-of-the-art cross domains of wireless communication, video processing, embedded systems, and security. Moreover, a new media-dependent video encryption scheme, including a reliable data embedding technique and real-time video encryption algorithm, is proposed and implemented to enable the system to work properly and efficiently in an open and insecure wireless environment. Extensive experiments are conducted to demonstrate the advantages of the new systems, including high security guarantee and robustness. The chapter would serve as a good reference for solving the challenging issues in wireless multimedia and bring new insights on the interaction of different technologies within the cross application domain.

INTRODUCTION

With the ever-increasing security demands of military and scientific applications, the development of a highly secure and reliable video surveillance system attracts significant interests from both academia and industry. The implementation and efficiency of such a system are greatly affected

by the techniques in wireless communication, video processing, embedded systems, and security guarantee.

Recent advances in embedded system and wireless communications are enabling cost-effective digital wireless multimedia systems. The forthcoming integration of wireless communications and embedded video systems is a demanding and interesting research topic. Video surveillance has resorted to wireless transmission due to the several serious problems when the traditional coaxial or high-tech fiber-optic cables are adopted to transmit video images from the surveillance cameras to the stations at which the images are monitored and/or recorded. Compared with the traditional wire-line counterparts, wireless video surveillance systems do not require expensive and time-consuming system constructions and civil-engineering work. They can therefore be deployed rapidly with negligible environmental impact. Furthermore, wireless systems generally require lower costs of network maintenance, management, and operation.

However, some fundamental issues, such as framework design of wireless networks, video processing, video data transmission, video quality control, and system security should be resolved before wireless video surveillance systems can be successfully deployed (Garcia-Macias et al, 2003). Among these important issues, the system security is the most challenging problem that becomes the main concern of this chapter. Intel IXP425 network processor provides an ideal choice for implementing secure ad hoc video surveillance system, but the security issue is still a hot-spot that IXP425 cannot handle well. Therefore, an effective video encryption algorithm is necessary and meaningful in a wireless video surveillance system. At the same time, the secure routing protocol and system architecture should be carefully designed to avoid serious security flaws (Yin, Lin, Sebastien, & Chu, 2005).

This chapter explores the state-of-the-art cross domains of wireless communication, video processing, embedded systems and security, discusses the challenging issues in wireless video surveillance, and presents the detailed design of a novel highly-secure video surveillance system over ad

hoc wireless networks. The rest of this chapter is organized as follows. Section 2 provides a review of wireless networks, ad hoc solution and security issues. Section 3 presents the design and implementation for the new video surveillance system and Section 4 evaluates its performance. Section 5 highlights the future trends in the relevant research areas. Finally, Section 6 concludes this chapter.

BACKGROUND

Wireless Networks

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections (without requiring peripheral cabling). Wireless networks serve as the transport mechanism among mobile devices or between these devices and the fixed wired networks (e.g., enterprise networks and the Internet). A wireless network has tremendous advantages in comparison with its wired counterpart: no network cable has to be installed through walls and floors, thus greatly reducing the cost and making the architecture more flexible.

The development of 802.11g (IEEE, 2003) based on the orthogonal frequency-division multiplexing (OFDM) technology allows high-load applications to be adapted in wireless environment. It is claimed that an optimal throughput of 54Mps and a range up to 100 feet indoors can be achieved. As the signal is modulated at 2.4 GHz, it is less affected by walls and physical obstacles than 802.11a (5 GHz). Thus our system is based on the 802.11g wireless infrastructure ad hoc networks.

Ad Hoc Solution

Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Ad hoc networks are designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed "ad hoc" because

Related Content

An Image Steganalysis Algorithm Based on Multi-Resolution Feature Fusion
Zhiqiang Wuand Shuhui Wan (2024). *International Journal of Information Security and Privacy (pp. 1-19).*
www.irma-international.org/article/an-image-steganalysis-algorithm-based-on-multi-resolution-feature-fusion/359893

Enforcing Privacy on the Semantic Web
Abdelmounaam Rezgui, Athman Rouguettayaand Zaki Malik (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 3713-3727).*
www.irma-international.org/chapter/enforcing-privacy-semantic-web/23321

IoTP an Efficient Privacy Preserving Scheme for Internet of Things Environment
Shelendra Kumar Jainand Nishtha Kesswani (2021). *Research Anthology on Privatizing and Securing Data (pp. 492-521).*
www.irma-international.org/chapter/iotp-an-efficient-privacy-preserving-scheme-for-internet-of-things-environment/280190

Role of Cyber Security and Cyber Forensics in India
Gulshan Shrivastava, Kavita Sharma, Manju Khariand Syeda Erfana Zohora (2018). *Handbook of Research on Network Forensics and Analysis Techniques (pp. 143-161).*
www.irma-international.org/chapter/role-of-cyber-security-and-cyber-forensics-in-india/201610

Utilizing Sentence Embedding for Dangerous Permissions Detection in Android Apps' Privacy Policies
Rawan Baalousand Ronald Poet (2021). *International Journal of Information Security and Privacy (pp. 173-189).*
www.irma-international.org/article/utilizing-sentence-embedding-for-dangerous-permissions-detection-in-android-apps-privacy-policies/273597