Security and DRM in Indoor/Outdoor Heterogeneous Networking Applications for User – Centric Frameworks

T. Fragopoulos*, A. Athanasopoulos*, A. Vogiatzis*, E. Topalis**, J. Gialelis**[(1)], S. Koubias**
*Industrial Systems Institute, Platani, Patras, Greece
** University of Patras, Rio Patras, Greece
[(1)] Corresponding author email: gialelis@ee.upatras.gr

Abstract

As networks become more and more complicated and applications more and more demanding, a very common network topology for state-of-the-art multimedia applications supporting emerging user – centric frameworks is a heterogeneous wired/wireless architecture. A network architecture solution for Indoor/Outdoor heterogeneous networking applications, to support both multimedia and sensor applications suitable for such frameworks is proposed in this paper. Furthermore, an integrated DRM system architecture is proposed for the protection of Intellectual Property, characterized by its interoperability aspect.

1. Introduction

The rapid evolution of technologies for communication between computing systems, the high availability of broadband services at high data rates, the great improvements in technology of hardware components of computers, and the usage of Internet as a communication media for various entities, facilitate the convenient distribution of digital artifacts like audio, video, etc., between users, most of the times illegally and without the necessary licensing. Digital Rights Management (DRM) mechanisms constitute of various technologies that have been developed and deployed by content providers, creators, distributors, in order to protect their digital media from illegally, unauthorized and without the appropriate rights usage of their products, while let them to use possibly unsafe media like Internet for delivering their products with less hesitation and anxiety about non-legitimate usage of their content. Various methods and a numerous DRM systems have been developed for protection of Intellectual Property. What characterizes most of them is the lack of interoperability, i.e. different content providers use different non-standardized non-interoperable DRM systems which may create great problems in contents usage by legitimate users [1].

Wireless technologies represent a rapidly emerging area of growth and importance for providing either ubiquitous access to a backbone wired network or formulate autonomous ad hoc wireless networks. The Access Point (AP)-infrastructured wireless networks architecture is based on at least one AP providing a server function. All kind of communication between all wireless nodes should pass through this AP. This AP might be connected to a wired backbone network as well. On the other hand, mobile Ad hoc Networks (MANETs) are autonomous networks consisting of routing nodes (or some routing nodes with other nodes that do not route) that are free to move about. They may be connected to a larger network e.g. the Internet, or operate as an isolated intra-network. Wireless networks can be categorized according to the extent of their coverage area into:

- Wireless Local Area Networks-WLANs
- Wireless Wide Area Networks-WWANs
- Wireless Personal Area Networks-WPANs.

Recently, industry has made significant progress in resolving some constraints to the widespread adoption of wireless technologies. Some of the constraints have included bandwidth and high infrastructure as well as service cost. Wireless technologies can support and provide cost-effective solutions. Wireless is being adopted for many new applications: to connect computers, to allow remote monitoring and data acquisition, to provide access control and security, and to provide a solution for environments where wires may not be the best solution.

As networks become more and more complicated and applications more and more demanding, a very common network topology for state-of-the-art multimedia is a hybrid wired/wireless architecture. Hence, the need for interoperability of heterogeneous networks with hybrid structure is in doubtfully a major requirement, when integrating communication scenarios for indoor and outdoor applications.

On the other hand, when dealing with a hybrid wired/wireless network, questions arise regarding QoS and power awareness issues especially concerning the wireless part of the hybrid network. Integration of QoS and power awareness in wireless networks is nowadays a growing research area as high throughput, timeliness and power efficiency is demanded by several home and other applications [2], [3]. Thus, trade-offs especially between QoS parameters and power consumption must be

1-4244-0826-1/07/$20.00 © 2007 IEEE

considered to a network with mobile nodes. In this paper, a user – centric framework architecture for indoor and outdoor heterogeneous networking conditions for multimedia and sensor applications, is proposed in regard to both communication and security (including DRM) levels. The structure of the rest of the paper is as follows. In section 2 the proposed framework network architecture based on specific application scenarios is proposed. Then, in section 3 a brief overview of wireless network technologies is provided while in sections 4, 5 and 6 DRM issues in regard to the user–centric framework are addressed. Finally, we conclude in section 7.

2. User – Centric Network Architecture Framework

When dealing with multimedia and sensor applications for both indoor and outdoor networking environments, the user-centric approach should be taken into consideration. Dynamic networking, multimedia sharing, content adaptation, personalized interfaces and data security are only some of the main challenges when dealing with the user-centric approach. This approach involves aspects of both integration and convergence [4]. The term integration refers to the fact that different networking techniques should be incorporated in order transparent network communication to be achieved. On the other hand, convergence in such systems corresponds to seamless content sharing among multiple devices connected to each other. Moreover, as long as both indoor and outdoor networking is concerned, the user-centric approach can be split out into the home-centric and device-centric convergence. Multimedia and sensor convergence allows the end-user to adopt various communication interfaces as they become available, transparently, without any interruption. According to the given parameters, all data are adapted to the available device characteristics.

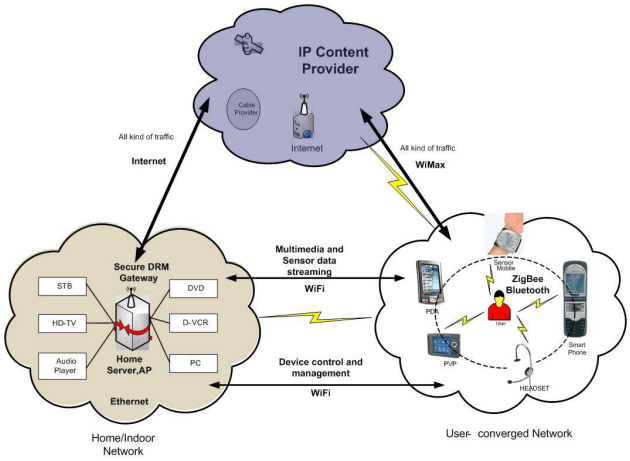

Figure 1. Application driven network framework topology

The framework network architecture, in terms of networking infra-structure, consists of two physical media, one wired and one over the air. The heterogeneous topology corresponds to the wireless WiFi, Bluetooth, ZigBee or WiMax standards and to the wired Ethernet and Internet based protocols.

The above figure illustrates the architecture of a possible application scenario. More precisely, John is listening, through his wireless headset, to his favorite music artist, as well as he is carrying a PDA with wireless access to an indoor AP. A multimedia streaming server is running on his Home Server/Gateway/AP so that multimedia data is being played back. While moving around his house, hand-off occurs between different APs of the house. Hence, John is receiving the multimedia data transparently. Afterwards, John decides to go for jogging without stopping listening to the music. He also puts on a wireless health monitoring wrist sensor. During jogging, John continuous to listen to his favorite music without any interruption, due to the wireless link between his headset/PDA/Gateway and the Home Server.
Technically speaking, in an indoor/home environment, the user, with the aid of a PDA, can communicate with various multimedia and sensor devices as well as the home server through the WiFi (IEEE 802.11b and g) [5] technology, supporting multimedia and sensor content applications. WPAN standards like Bluetooth (IEEE 802.15.1) [6] or ZigBee (IEEE 802.15.4) [7] are more appropriate for connecting to a PDA several wireless devices such as, oximeter sensor, for heath care monitoring or head sets for entertainment, within the body area of the final user. On the other hand, in an outdoor environment, the user has the ability to communicate with the home server through a WiMax (IEEE 802.16) [8] access point and a Home Gateway internet-based link. In that point of view, both ad hoc and infra structured topologies are engaged in regard to wireless communications.

As holds for all multimedia and sensor applications or possible communication scenarios, the user perceptive quality defines tight QoS requirements that the heterogeneous network should support. Hence, the QoS, regarding the MAC sub-layer, should be evaluated for different communication scenarios with respect to power consumption as well. Finally, useful outcomes can be observed regarding QoS and power consumption trade-offs.

3. Wireless Standard's overview

Up to date, the dominant and most widely used wireless standard is the IEEE 802.11b of the IEEE 802.11 family. As the demands of the wireless technology follow the trends of the market, different needs for various wireless

applications have arise. Thus, several wireless standards started to get launched into the market targeting different applications.

WiFi

The IEEE802.11b standard defines 3 different Physical layers providing different data rates. The three PHY kinds are: a) the FHSS, b) the DSSS and c) the IR. Both FHSS and DSSS use the ISM 2,4GHz frequency band. The offered bandwidth is 1 or 2Mbps depending upon the GMSK. Finally, the IR designed mostly for indoor applications. Recently, a proposal for higher data rates (i.e. 5,5Mbps and 11Mbps) was adopted.

The MAC sub-layer defines two access coordination mechanisms, the basic Distributed Coordination Function (DCF), which is mandatory and the optional Point Coordination Function (PCF). Asynchronous transmission is provided by DCF, which is basically a CSMA/CA access method, while synchronous transmission provided by PCF follows a round-robin polling-based access mechanism. The basic DCF is CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Virtual carrier sensing uses the duration of the packet transmission, which is included in the header of RTS, CTS, and DATA frames.

The 802.11g uses the same transmission technology found in 802.11a, which is called Orthogonal Frequency Division Multiplexing (OFDM). This increases the amount of data transmitted in a given time slice (i.e. higher data rates). However, unlike 802.11a, which operates in a 5GHz band, 802.11g uses carrier frequency bands that are around 802.11b's 2.4GHz primary carrier frequency. More precisely, this standard supports the following PHY layers:

ERP-DSSS/CCK (mandatory), ERP-OFDM (mandatory)
ERP-DSSS/PBCC (optional) and DSSS-OFDM (optional)

The ERP-OFDM is the new mandatory physical layer introduced by 802.11g. With the OFDM technique IEEE 802.11g's data rates are provided at the 2.4 GHz ISM frequency band can reach the level of 54kbps. At the MAC layer the CTS-to-self mechanism is used. The main goal of this mechanism is to reduce the overhead caused in the network due to RTS/CTS signaling sequence. Unlike the RTS/CTS, CTS-to-self cannot eliminate the hidden node problem the wireless networks suffer, unless all stations are within the transmitting node's range.

ZigBee

The IEEE 802.15.4 standard was approved in May 2003. The IEEE 802.15.4 is implemented in order to address the special needs of most wireless sensing and control applications for both WBAN and WPAN. The main characteristics of the 802.15.4 standard include extended battery life over current wireless standards, mesh and star network topologies, cost effectiveness, as well as no line of sight demands.

The new IEEE standard, 802.15.4, defines both the physical layer (PHY) and medium access control sub-layer (MAC) specifications for low rate; low power consumption wireless personal area networks (LR-WPANs). There are two different types of network topologies implemented in 802.15.4; an one-hop star, or a multihop peer-to-peer topology. The IEEE 802.15.4 defines two PHY layers according the operating frequency. Thus, both 2.4GHz and 868/915 MHz frequency bands can be supported in this standard. Both bands are based on DSSS. This standard can support data rates of the range of 20kbps up to 250 kbps depending upon the operating frequency band.

The MAC sub-layer employs the *carrier sense multiple access with collision avoidance (CSMA-CA) mechanism for channel access (*does not include the request-to-send (RTS) and clear-to-send (CTS) mechanism*), handling and maintaining the guaranteed time slot (GTS) mechanism and finally, providing a reliable link between two peer MAC entities*. The three data transfers which are classified in accordance to data sender and data receiver station are the following.

- *Direct data transmission*. Unslotted CSMA/CA or slotted CSMA/CA is used.
- *Indirect data transmission* Unslotted CSMA/CA or slotted CSMA/CA is used..
- *Guaranteed time slot* (GTS) data transmission. No CSMA/CA is required.

The 802.15.4 allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator. The superframe is bounded by network beacons and is divided into 16 equally sized slots. The beacon frame is sent in the first slot of each superframe.

WiMax

WiMAX was initially designed to deliver 70 Mbit/s, over 70 miles (112.6 kilometers) when the recipient is moving or mobile. In practice, in line-of-sight environments you could deliver symmetrical speeds of 10Mbps at 10km but in urban environments it is more likely that 30% of installations may be non-line-of-sight and therefore users may only receive 10Mbps over 2km and if the recipient is on the move the bps rates drop significantly.

The IEEE 802.16 Working Group has developed point-to-multipoint (PMP) broadband wireless access standard for systems in the frequency ranges of 10-66 GHz and sub 11 GHz. The standard covers both the Media Access Control (MAC) and the physical (PHY) layers.

A number of PHY considerations were taken into account for the target environment. At higher frequencies, line of sight is a must. This requirement eases the effect of multipath, allowing for wide channels, typically greater than 10 MHz in bandwidth. For sub 11 GHz non line of sight capability is a requirement. The original IEEE 802.16 MAC was enhanced to accommodate different

PHYs and services, which address the needs of different environments. The standard is designed to accommodate either Time Division Duplexing (TDD) or Frequency Division Duplexing (FDD) deployments, allowing for both full and half-duplex terminals in the FDD case. An IEEE 802.16 system consists of a Base Station(BS) and one or more Subscriber Stations(SS). In the downlink direction (from the BS to SS) the system operates in a TDM fashion. In the uplink all SSs share the link capacity on a demand basis. An amendment to the standard, IEEE 802.16e-2005 (formerly known as IEEE 802.16e), addressing mobility, was concluded in 2005. This is sometimes called "Mobile WiMAX", after the WiMAX forum for interoperability

Bluetooth

The IEEE 802.15.1 standard, in practice, finds most applications in point-to-point communications aimed at eliminating cabling in short-range communications between devices. Its main feature is the support of short-range multimedia applications. Indeed, Bluetooth transmission speed of 1 to 2 Mbit/s is sufficient for voice/audio.

Bluetooth operates on the unlicensed Industrial Scientific Medical (ISM) band at 2.4 GHz, which ensures worldwide communication compatibility. Hence, to minimize the risk of such interference, Bluetooth uses a Frequency Hopping Spread Spectrum (FHSS) technology for its air interface. During a connection, radio transceivers hop from one channel to another. This means that after one packet is sent on a channel, the two devices retune their frequencies (hop) to send the next packet on a different channel. When the transmission encounters a disturbance due to interference, the packet will simply be retransmitted on a different channel. Hence, if one frequency channel is blocked, there will be a limited disturbance to the Bluetooth communication. The typical range for Bluetooth is 10m. Two or more Bluetooth units sharing the same channel form a piconet. One device acts as a master and the devices connected to it act as slaves. The slaves in a piconet can only have links to the master. Slaves cannot directly transmit data to one another. Basic medium access method is a TDMA based scheme.

4. Security and Digital Rights Management Overview

One key issue in home networking is related to the Intellectual Property of contents being distributed. As a matter of fact, multimedia distribution across several kinds of devices and networks, which can communicate among them, facilitates the convenient distribution of digital artifacts like audio, video, etc., among users, most of the times illegally and without the necessary licensing. Digital Rights Management (DRM) mechanisms consist of various technologies that have been developed and deployed by content providers, creators, distributors, in order to protect their digital media from usages that may be illegal, unauthorized and without the appropriate rights of their products. At the same time, DRM facilitates the use of possibly unsafe media like the Internet for delivery of these products with less hesitation and anxiety about non-legitimate usage of their content. This problem is even more stressed in PANs, where content distribution among users and their usage generally takes place in an autonomous and uncontrollable form, due to the likely absence of a public connection.

Various methods and numerous DRM systems have been developed for the protection of Intellectual Property, (see [9] for a quick overview). What characterizes most of them is the lack of interoperability, i.e., different content providers use different non-standardized, non-interoperable DRM systems, which may create great problems in contents usage by legitimate users, thus breaking the user-centric concept [1].

5. Components and Requirements for DRM Systems

A typical DRM system comprises of different types of components and should also provide different functionalities; shortly, we identify (a) *Secure Storage Containers*, which are used to protect the digital content from unauthorized access. Such containers can use various security functions like cryptographic primitives, trusted computing modules, etc; (b) *Rights expressions tools*, referring to the ways that the usage rights over a specific digital content are expressed. Basically those tools are combinations of languages (Rights Expressions Languages - RELs) with appropriate dictionaries. We have various examples of such methods like XrML, MPEG REL, OMA REL, etc; (c) *Description* and *identification of digital content*, (digital items and metadata) methods. For example, MPEG-21 standard provides a well defined method for describing all digital content and its relevant metadata; (d) Identification of the involved parties in the chain of a DRM system – Authentication of interacting entities with the digital content; and (e) *Forensic DRM components*, refer to watermarking and fingerprinting techniques for proving subsequently if any rights violation over a digital content has occurred.

The basic requirements that are expected from a DRM system are: a. Interoperability, which refers to the ability of the system to operate under different types of devices, platforms and architectures; Security, which means that the system should provide robustness against possible attacks; and Privacy, i.e. whatever security mechanism is employed by a system, by any means it should take care and protect user's privacy. Especially, in the deployment of secure DRM systems, where there is an explicit relationship between end users and contents providers, with the latter ones having as their primary goal the

protection of their digital assets, protection of end user's privacy is an issue that requires special treatment.

6. Proposed DRM architecture for the User–Centric Concept

As depicted previously in the described application scenario, the user- centric concept introduces the notion of Body-Area Network (BAN), which comprises of various embedded devices like pocket PCs, Portable Data Assistants, etc., which reside on the user. The outer vision is the creation of truly pervasive and ubiquitous computing environments into which the human shall be the foundational stone.

The main target is on the one hand to develop and deploy technologies that shall permit, transparently to our end-user, John, the continuity of various multimedia sessions over heterogeneous networked environments while on the other hand the assurance that the digital rights of multimedia contents are kept secure and under the terms that specified by their licenses. It must be developed a Digital Rights Management (DRM) system that should take in mind issues like interoperability and heterogeneity of environment, weaknesses and constraints of participating entities, various security challenges that may arise, while being scalable and easily adaptable under changing requirements, providing Quality-of-Service, without compromising architecture's primary functionality.

Within this field, much effort should be devoted to develop and deploy technologies that shall permit, transparently to the end-user, the continuity of various multimedia sessions over heterogeneous networked environments; on the other hand, they should guarantee that the digital rights of multimedia contents are kept secure and under the terms specified by their licenses. A DRM system must be developed, by keeping in mind issues like: interoperability and heterogeneity of environments; weaknesses and constraints of participating entities; various security challenges that may arise; scalability and easiness of adaptation under changing requirements; QoS provision, without compromising the architecture's primary functionality; and real-time constraints for real-time (live) contents. This can be achieved, for example, by using a DRM gateway for generation of licenses to be transferred to each device before the multimedia content; the generated licenses could be compatible with MPEG-21 standard's requirements, since that framework works towards the solution of interoperability problems [10]. A possible configuration is depicted in Fig. 2

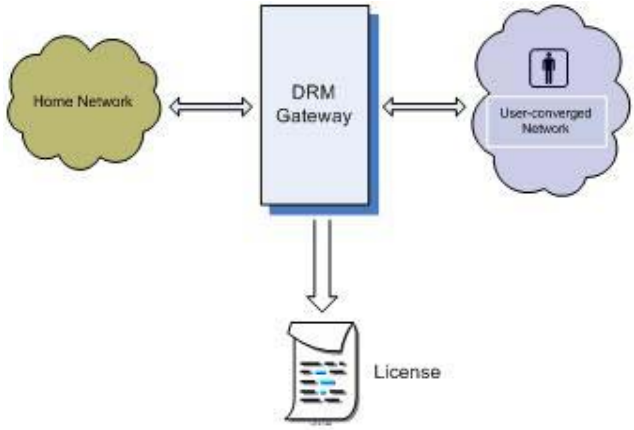

Figure 2. DRM gateway shall generate licenses for contents usage according to Home Network's (HN's) initiative.

In the following figure, a typical scenario is depicted. More specifically: (1) HN initiates a transaction towards a terminal that belongs to the user-converged network, while in (2) HN requests the generation of an appropriate license by the DRM gateway. In (3), (4), the license is transferred to the terminal and finally in (5), (6) the content is transmitted to the terminal, possibly transcoded. In that case, the terminal has the full responsibility for content's usage and enforcement of its license.

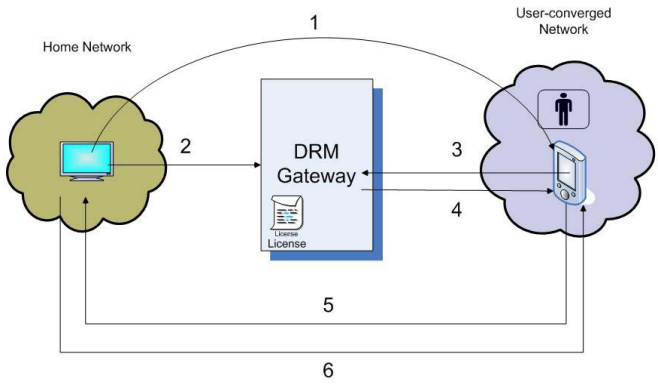

Figure 3. A typical scenario following the proposed configuration .

It should be noted that our vision here is to manage the implementation of a real-time DRM system for live transmitted digital content. In order to accomplish this task, we start with the development of a "near"-real-time DRM system for stored contents between HN and user-converged network; then, we refine our system, by allowing the provision of real-time DRM for stored contents, leading us, eventually, to a DRM system that shall provide real-time DRM for live content.

7. Conclusions

Ubiquitous computing and user-centric computing environments are the future of modern computing technology. The end-user has the ability to carry different types of portable devices, rendering various types of digital contents. Security is an aspect of paramount importance in such environments, while mechanisms for interoperable DRM systems are necessary. In this paper, we have identified the basic requirements for DRM systems and we have also provided a high level view of an interoperable DRM architecture, where licensing is based on MPEG-21 framework.
A framework network architecture for Indoor/Outdoor heterogeneous networking applications has also been outlined. Due to the user-centric nature of the proposed application scenario, the main aspects regarding seamless wireless heterogeneous networking for multimedia and sensor application have been addressed.
The future work will be the further specification of the framework architecture in order to implement real-time DRM for live (real-time) transmitted digital content.

The work presented in this paper has been funded by the Network of Excellence "INTERMEDIA", FP6 – IST-38419. Available at: http://intermedia.miralab.unige.ch:80/.

References

[1] N. Helberger. 2005, "Virgin media versus iTune". Available: http://www.indicare.org/tiki-read_article.php?articleId=150

[2] O.S. Unsal and I. Koren, "System-Level Power-Aware Design Techniques in Real-Time Systems" (Invited paper) *Proceedings of the IEEE,* Special Issue on Real-Time Systems, Vol. 91, July 2003

[3] Hans Van Antwerpen, et al., "Energy-Aware System Design for Wireless Multimedia", Panel on Platforms and Tools for Energy-Efficient Design of Multimedia Systems, Design Automization, 2003

[4]Niebert, N. *et al.*, "Ambient Networks: An Architecture for Communication Networks Beyond 3G," *IEEE Wireless Communications*, Vol. 11, No. 2 (2004), pp. 14-22.

[5] IEEE 802.11 WG, Reference number ISO/IEC 8802-11:1999(E) IEEE Std 802.11, 1999 edition, International Standard [for] Information Technology - Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 1999

[6] www.bluetooth.com

[7] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Standard for Information Technology-Telecommunications, 2003 IEEE.

[8] www.wimax.org

[9] Fragopoulos, A. G., Serpanos D. N., "Intellectual Property Protection Using Embedded Systems," in Serpanos, D.N., and Giladi, R., Security & Embedded Systems, Vol. 2, IOS Press (Amsterdam, The Netherlans, 2005), pp. 44-56.

[10] Burnett, I. *et al.*, "MPEG-21: Goals and Achievements," *IEEE Multimedia,* Vol. 10 (2003), pp.