Secure Network Coding for Smart Homes

Alireza Esfahani, Georgios Mantas , Jonathan Rodriguez, and Jose Carlos Neves
Department of Electronics, Telecommunications and Informatics,
Instituto de Telecomunicações (IT), University of Aveiro

Abstract

Technology paradigms such as the "Internet of things" means that in future any device will be able to be remotely controlled, which implies confidential data is liable to be uploaded, and transmitted over wireless networks. One such scenario is video surveillance applications for public safety in smart cities. However, its use in a smart home has been sometimes questioned and argued about, due to privacy concerns. It has been proven that network coding can be a useful tool for efficient transmission of data over wireless networks. This work, called CodeLance, is about an industry-academia cooperation that will exploit the know-how on ICT of both academic and commercial companies, in order to provide an efficient secure product for video surveillance over wireless multi-hop networks to support various services like, traffic monitoring, fire detection and real-time events (such as natural disasters) broadcasting for the societies of the smart cities.

Description and main innovation

Smart homes are increasing in number in North America and Europe. According to a new report [1], the total number of smart homes is expected to reach more than $23 million by 2017 (Fig 1). However, smart homes are vulnerable to security threats and in the new urban environment model, new paradigms in smart cities and smart homes (Fig 2) will be required to provide secure and effective security service to facilitate everyday life. Most security problems are related to weak user- and device-authentication schemes. Security attacks may be generated locally or remotely.

This work, called CodeLance, employs advanced network coding and security techniques for video surveillance applications in smart cities and smart homes.

Overall main objective of this work is the design of a network-coding based software product for video surveillance over wireless multihop networks to provide increased throughput, low latency, energy efficiency and security guarantees. More specifically CodeLance will advance the state-of-the-art through the following innovations:

- ➢CodeLance will propose advanced network coding techniques to support cost effective video surveillance system
- ➢CodeLance will advance network coding to provide error resiliency for multimedia broadcast applications
- ➢CodeLance will exploit Random Linear Network Coding (RLNC) and Xor NC to minimize not only the computational overhead, but also the latency for real-time video streams
- ➢CodeLance will investigate secure network coding for secure and robust data connectivity

Network coding-based wireless networks are susceptible to pollution (data and tag) attack where a small number of polluted messages can corrupt bunches of legitimate messages. In CodeLance, we have presented three homomorphic MAC-based schemes for network coding-enabled wireless networks, providing resistance against tag pollution attacks in RLNC and XOR NC.

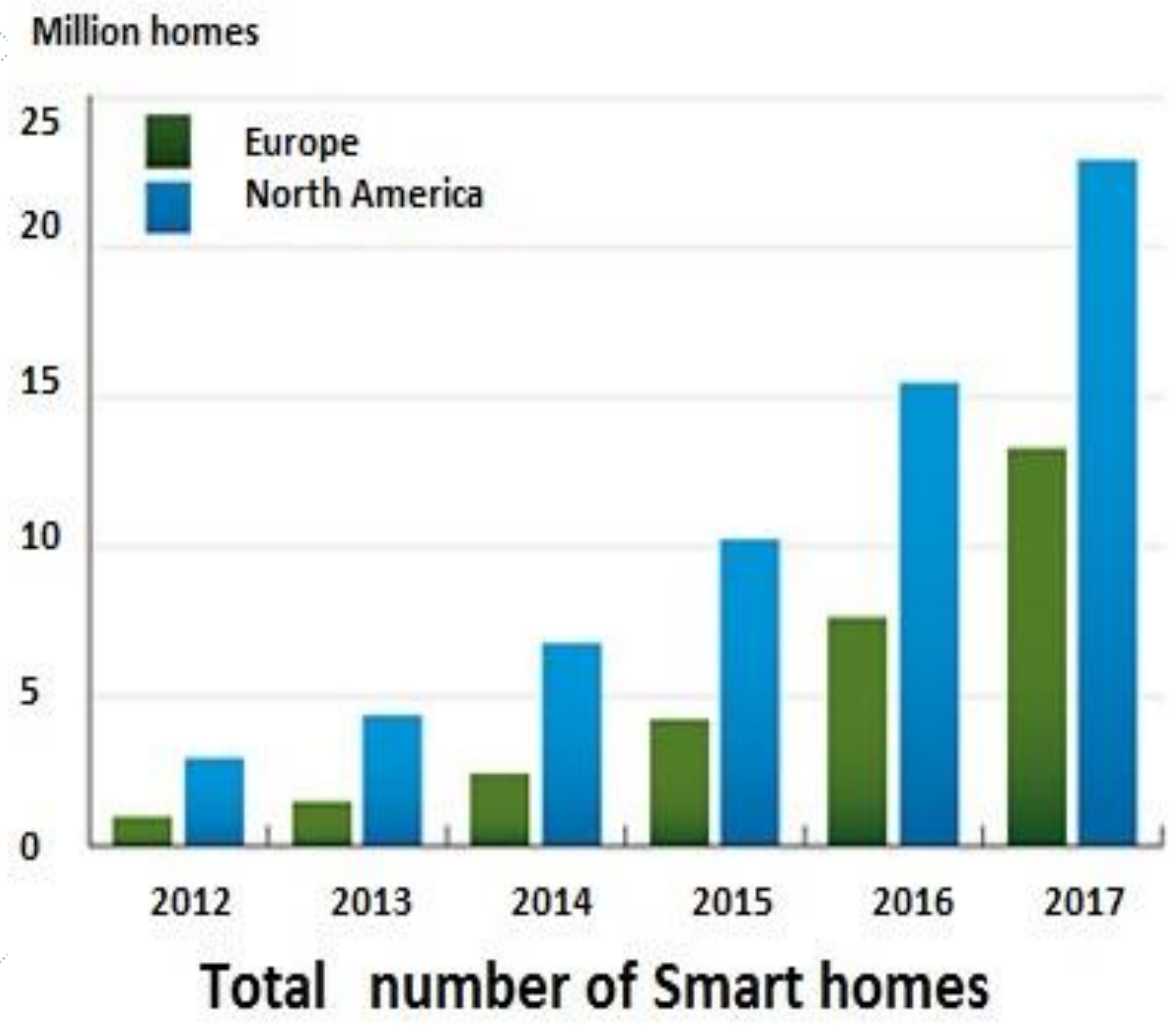

Fig 1 / The total number of smart homes.

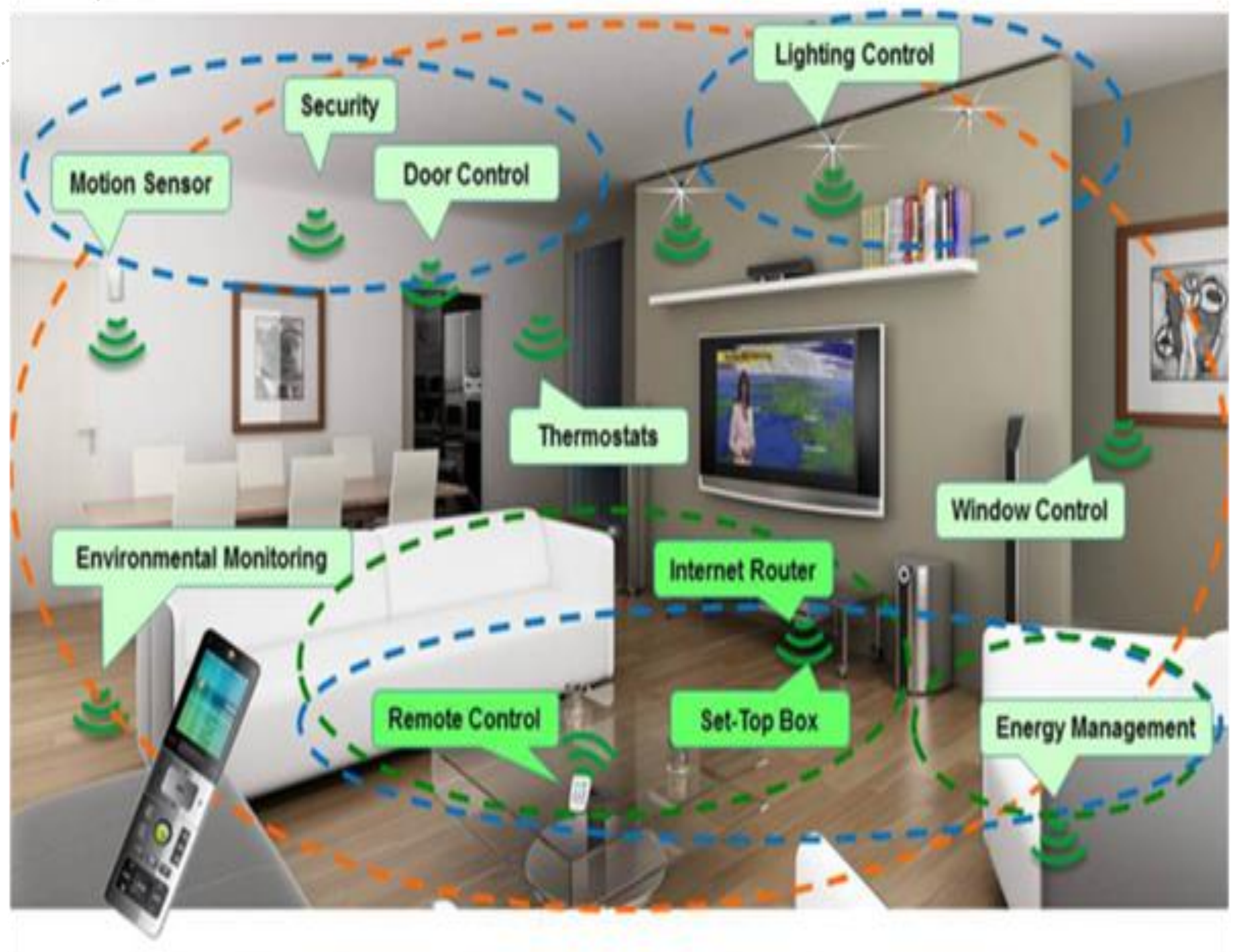

Fig 2 / An illustration of a smart home where the smart connected home's various systems can be controlled via smartphone or smart device apps.

[1] Essence Smart Home Survey: Americans & Europeans Agree Security is Key, Aug 2015.

Achievements

- One book chapter
- 3 published journals + 1 under review
- 6 conference papers

Conclusions

- More precisely, we have focused on mitigating pollution attacks in network coding-enabled wireless networks to provided a secure product for video surveillance over wireless multi-hop networks in smart homes. The performance evaluation of our schemes show that they are more efficient compared to the most competitive tag pollution immune schemes, in terms of computational complexity without incurring additional communication overhead.

www.portointeractivecenter.org