

WIRELESS SENSOR NETWORK MODEL AND PROTOCOL:

SECURE DATA COMMUNICATION BETWEEN FIXED AND MOBILE SENSORS

SIDDHARTH DALAL, YONG MA, MAJD ALWAN, BEVERELY TURNER, STEVE KELL



MEDICAL AUTOMATION RESEARCH CENTER

ABSTRACT

Reliability and security of data are essential to data communications, particularly when the transported packets contain medical information or physiological measurements. This research project focuses on the design and development of a wireless network model and the necessary protocol to be used in home environments for acquiring such data. The protocol is designed as a higher layer over the IEEE 802.15.4 low bandwidth wireless communication protocol, which is expected to become the industry standard in home automation.

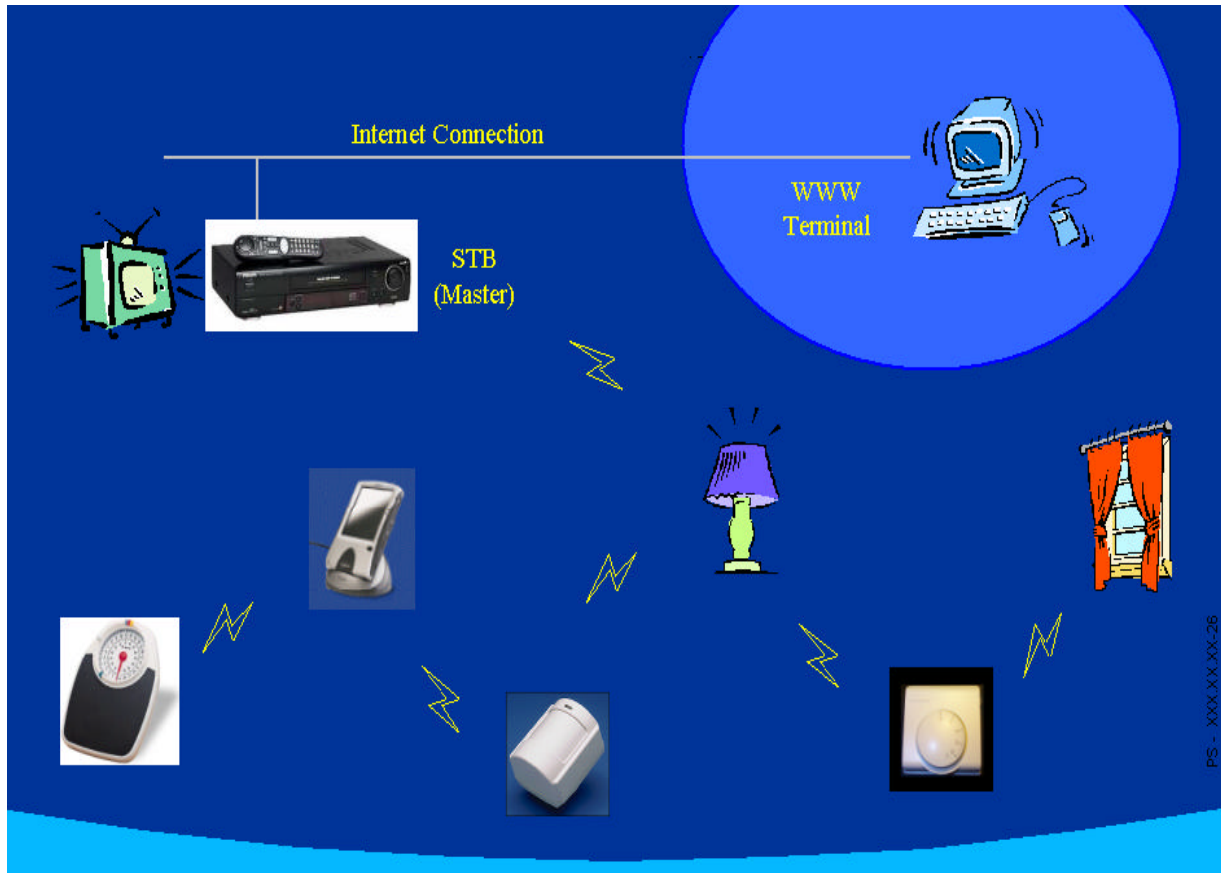
We provide essential network organization specifically targeted for home environments with special consideration to cross-apartment interference issues. The data transmission is reliable (two-way with acknowledgement) and security is provided by encryption. To enable tracking of individuals within the home, the network model contains both fixed and mobile sensors, as well as tagging activity data with identification information.

The proposed network architecture can be implemented with very low cost commercial transceiver chips, soon to be available from several major manufacturers.

NEED

- There is a need for secure, reliable and economic wireless communications
 - Wired technologies require costly and labor intensive infrastructure, and not suited for retrofit
 - Wireless technologies are cost effective: have no cabling and require minimum labor
 - Current wireless technologies suffer from interference and security problems
 - There is also a need for tagging sensory data with identification information collected from mobile sensors
- Appliance connectivity, home and industrial automation, and networking are prime areas of research and present vast potential markets
- Current products that implement standard protocols such as Bluetooth (high bandwidth) are expensive and limited in density and range
- IEEE 802.15.4 protocol is targeted at unifying the market of low cost and low data rate devices

WIRELESS HOME PROFILE



Note: Courtesy of Kursat Kimyacioqlu from Philips

This diagram shows potential wireless appliance connectivity between different devices in the home to a central gateway (the Set-Top Box in this diagram) that provides access to the outside world.

POTENTIAL MARKETS

MEDICAL MONITORING AND ELDER CARE

- Medical information gathered through remote monitoring of elder people can improve the quality of care and life, extend aging-in-place and independence, and potentially reduce the cost of care
- The growing elder population prefers to age in place, and technology has to provide the means to facilitate the fulfillment of this goal
- A secure and reliable wireless protocol is required for medical devices and related applications, such as in-home patient monitoring

HOME SECURITY AND AUTOMATION

- Currently home automation is a \$600 million market and is expected to grow to \$8 billion within the next four years
- In 2000, Americans spent \$17.5 billion on professionally installed electronic security products and services with 8.6% annual growth
- Currently, home automation employs unreliable non-secure protocols, such as X10, complex or limited range protocols, such as Bluetooth
- There is a need for simpler and more secure network protocols to overcome the shortcomings of currently adopted technologies

OBJECTIVES

- Design a cost-effective home network model and protocol to reliably connect all low data rate electronic appliances, including sensors and medical devices
- Design a security model to provide data privacy and eliminate cross-interference; the security layer should be efficient to embed into resource-constrained devices
- Design an efficient data resource tracking and localization method that can tag activity data with identification to enable monitoring and tracking several persons in the home simultaneously



NETWORK MODEL

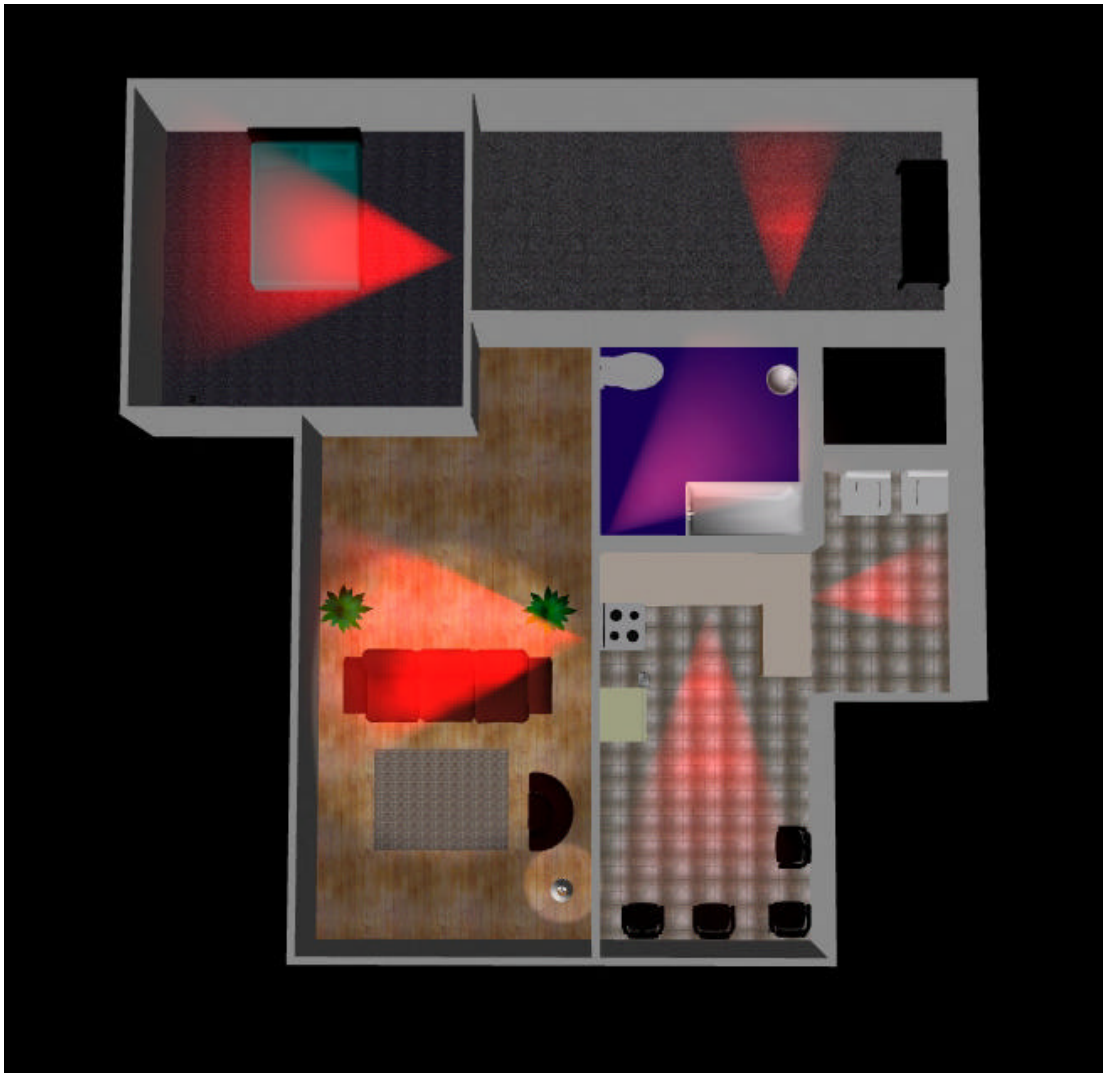
- For the most part appliances are fixed in specific locations in a room, making their network architecture ‘fixed’. A ‘mobile’ network architecture is required for tracking an individual’s activities and for portable devices and sensors
- Combining these two architectures leads to a ‘hybrid’ architecture. We use a hierarchical structure where a fixed sensor serves as a ‘room master’ and manages all of the sensors in its room and communicates with the ‘house master’, which is a central server that provides access to the outside world

CHALLENGES

- Implementing efficient routing algorithms to communicate between mobile sensors and master
- Implementing a security model with limited resources on the fixed sensors and extremely constrained resources on the mobile sensors
- Increasing the resolution of RF-based location tracking of mobile sensors, which is inaccurate due to multi-path fading, through redundancy derived from multiple fixed sensor confirmations

CONCEPT

- The schematic below illustrates sensor placement in our Smart House environment
- The red cones depict sensors and their range

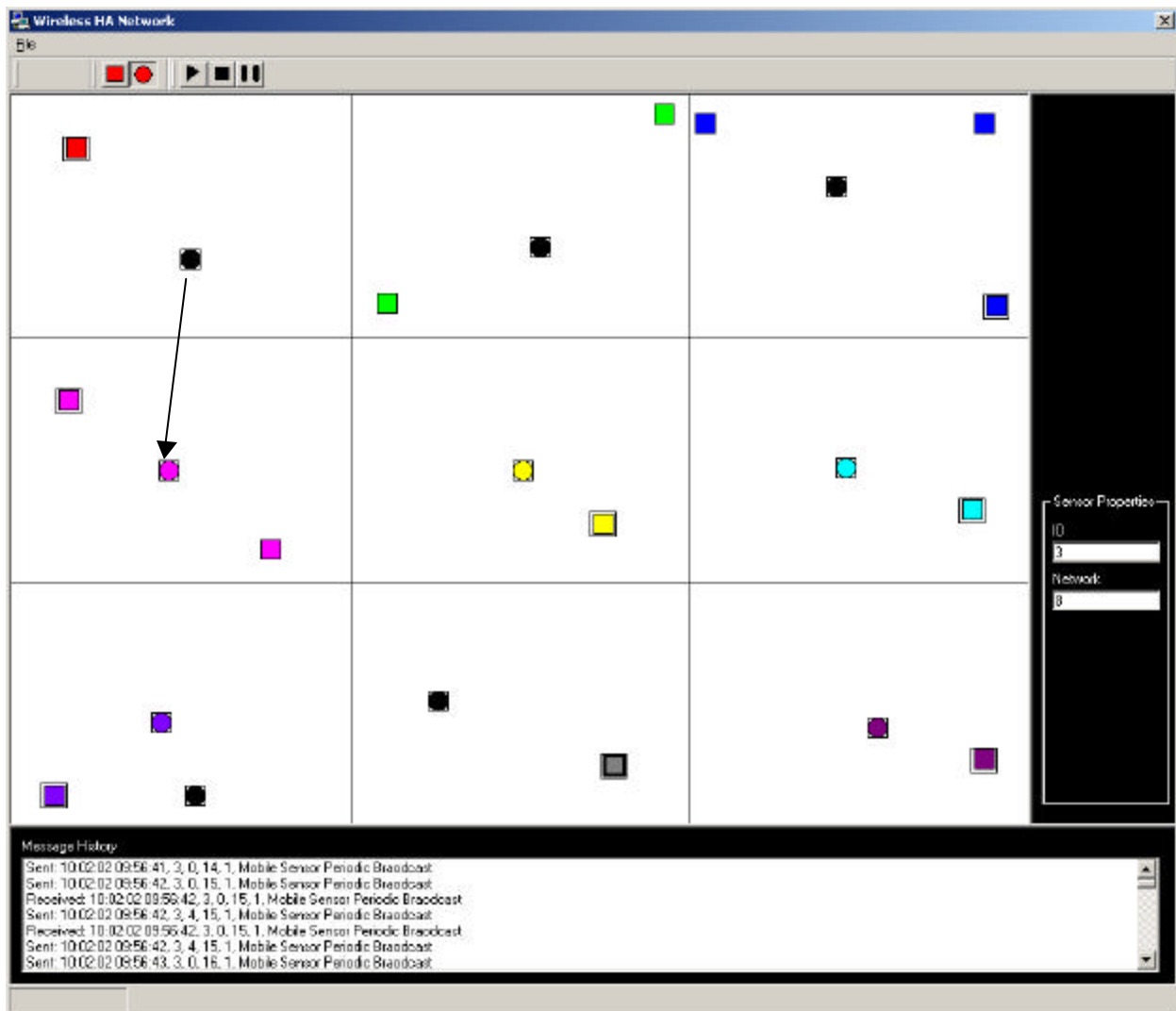


SIMULATION

- We are developing a software simulation of the network (page #9) to test and verify our algorithms and protocols
- The simulation includes the ability to place fixed and mobile sensors and the ability to move mobile sensors around
- We will simulate the message passing and their format
- We plan to add different types of sensors with different characteristics
- We plan to simulate an indoor RF model to help train sensors to track mobile sensors using only RF; this will be refined from multiple fixed sensor confirmations
- Finally we will simulate our security model to demonstrate cross-interference reduction

SIMULATION

- Squares represent fixed sensors and circles represent mobile sensors; different colors indicate being part of different sub-networks
- Mobile sensors can be moved, and will consequently join the sub-network of the room they are in



CONCLUSIONS

- The current market does not meet the present needs and future trends of reliable and secure data communication for applications, such as in-home medical monitoring and home security
- Our network model and protocol are capable of securely handling health data and eliminate the cross-talk between homes and facilities
- Future trends will rely on wireless personal area networks for medical applications, within which our secure protocol plays a significant role

FUTURE DIRECTIONS

- Our model for a wireless Smart House will connect medical instruments, sensors and low data rate appliances. The security model will ensure privacy and protection from unintentional or malicious eavesdropping
- This research will aid in the development and deployment of secure wireless home networks. These networks are suited for a wide spectrum of applications, ranging from medical monitoring and home security to industrial automation applications