

Framework for Smart Surveillance in Konnex environments

Massimo Aliberti

Istituto di Scienza e Tecnologie dell'informazione (ISTI-CNR)
1, Via G. Moruzzi 56100 Pisa, Italy
Tel. 050 315 2974 – Fax : 050 313 8091 (G3) 050 313 8092 (G4)
massimo.aliberti@isti.cnr.it

Abstract

This paper aims at the individuation of novel paradigms for Smart Surveillance applications based on collecting intensive sensor dataflows and providing an abstraction layer for event and activity detection. Konnex network will be deployed as the underlying communication and control bus, in order to evaluate its impact on performance and reliability of the system. The objective is to individuate any difficulties that may arise from usage of Konnex networking in surveillance applications and, eventually providing indications and models to overtake the weak points.

The surveillance system being investigated here leverages the potentials offered by Radio Frequency Identification (known as RFID) even in home environments, where correct, real-time identification of persons and objects may constitute the basis for an intelligent security system, not limited to intrusion detection, but also monitoring other abnormal activities and events (such as abnormal behaviours of elderly or disabled people, i.e. Alzheimer patients). The paper will show a possible model for surveillance systems moving beyond current commercial products' way of operation. While currently alarm systems merely offer the possibility to *switch the full protection on and off*, this work proposes a more *context aware* protection, that tailors itself to the different situations that may take place in a home environment, and a set of *smart behaviours* to define the best reaction to each event, in order to introduce a novel working model for security systems: an *always on* operating mode where it's up to the system and not to the user the responsibility to determine whether protection is needed or not. To accomplish this, raw sensor data will undergo a *pattern recognition* process, where the system gains knowledge even of complex situation, inferring from dataflows coming from the environment (through statistical analysis, artificial intelligence and possibly machine learning). Apart from the always on mode, the introduction of pattern recognition techniques will enable to define a fine grain security model, not only providing *intrusion detection*, but also an *access control policy* where the system gains knowledge of *which subjects* are committing actions on *which objects*, since each of this two elements can be given an actual value if an identification infrastructure is introduced.

The network layer will have to show some specific characteristic in its physical and logical parameters, in order to prove efficient enough to support this security system. Konnex bus will be investigated in this direction, and possibly extended or integrated with the cooperation of other existing network types, both wired and wireless, such as Ethernet/IP, wireless 802.11 and/or 802.15 protocols.

Introduction

RFID technology introduces low cost and battery-less small tags to be integrated into (or even simply attached to) objects. The principle is similar to that of radar technology: a scanner (normally

called a reader) sends a query signal (searching for tags to identify), providing a suitable energy content that enables the tags to simply backscatter a portion of the electromagnetic field, encapsulating some information in the reflected wave. Ubiquitous RFID tagging is going to replace current ubiquitous barcode labelling. Growth of the technology is still incomplete especially as far as operational frequency is concerned: ranging from low (125kHz and 13,56 MHz) to UHF (900MHz) and microwave (2,4Ghz) frequencies have been used up to now. While a number of current applications still rely on lower frequency bands, several elements such as worldwide availability of the 2,4 GHz frequencies and constant cost decrease of the electronic parts make it sensible to believe that a future convergence of present products towards 2,4 Ghz ISM band can be foreseen (see also [8]).

RFID and Ambient Intelligence

Massive introduction of RFID tags in a variety of applications is foreseen within the next 5/10 years. The domestic environment will be “populated” by a number of tagged items ranging from clothes and foods to consumer electronics and personal items such as watches, mobile phones, PDAs etc. Intelligent environments could take advantage of such a presence because of the potential enhancements offered to context awareness. RFID introduces what we may call “last mile computing”, meaning the coverage of the small yet problematic physical distance between information systems and the real world. Covering this last mile will bring ubiquitous computing to a more complete level in which context awareness will also include knowledge of people and objects currently present in a scenario enabling novel applications. Especially as far as home automation is concerned a few ones should be listed here: *smart fridge* (with expiry date detection and food inventory), *smart washing machine* (automatic program selection, alarm generation for incompatible clothes etc.), *remote controls* with adaptive “contextual” interface tuned in with adjacent devices and *smart surveillance systems*, that will be explored more in detail in this paper.

Apart from specific applications, wireless identification through RFID brings to Ambient Intelligence new potentials in context detection and learning. In a RFID-enabled home, an automatic learning period would be possible, partially assisted by the user, during which the information system could infer a number of details about the environment. For example, clothes usually worn by a specific user could be used to recognize the user itself: first matches between users and their clothes could be realized through everyday natural interactions with the system (during a biometric authentication to a display panel in the house, clothes could be scanned to associate the identified items with the user currently recognized). Of course, identification of users could be easily made through RFID bracelet or watches, but what has to be underlined here is that Ambient Intelligence applications should not rely their whole working model on an unpredictable attitude of the user: bracelets may be taken off for any reasons, or lost, and functionality should be ensured anyway, therefore specific tools for human identification should be seen by AmI systems merely as a starting point for the learning process mentioned here. This has to be related to Ambient Intelligence’s declared peculiarity to adapt itself to users’ habits, rather than trying to change them, in order to provide a technology that really is “disappearing”: not perceived as a novelty but as a normal component of everyday life.

RFID and Konnex

Current commercial products for RFID applications are mainly targeting industrial environments: this means that currently available RFID readers are not yet suitable for a straightforward introduction in home automation. Industrial automation requirements are, of course, more sophisticated than home automation ones, but what’s more important is that they do not even overlap: while, for example, industrial readers are required very fast response time and multiple

simultaneous read actions, home readers will just have to manage a limited number of tagged items/people, in a quite static environment (i.e. objects not continuously moving around). Technological trade-off in industrial RFID readers, then, focuses on read speed rather than on read range, which, in those applications may be considered a secondary element. Instead, home applications require an opposite trade-off where read range has to be privileged (in order to introduce field cover of the whole house with a limited number of readers). Below is a list of the main points on which current RFID appliances do not meet home automation needs:

- Cost: home readers will not address specific logistic processes, and will not generate specific economic revenue, so their cost will obviously be considered carefully by end-users. Note that an RFID home infrastructure will probably require at least a reader per room (see below).
- Size: industrial readers may be as big as necessary, home readers have to be small enough to produce a limited impact on the house scenario
- Packaging: home environments do not produce high electromagnetic noise, so shielding here is not an issue, therefore simple packaging has to be preferred (also for cost reasons)



Figure 1: UHF (865-928 MHz) Feig Reader LRU 1000

- Read Range: this is the point where home automation is requiring the most. Industrial readers can provide read ranges of up to some metres (1-3m are to be considered very good values for this kind of devices). Longer ranges cannot be achieved easily in an industrial environment due to noise, high number of tags to be read, and so forth. Home readers, instead, will have to manage only a few tags per minute, in a low noise environment, so specific technological design could come up to providing longer ranges (ranges of 5m or even 10m can be considered as sensible values to expect)
- Interfaces: industrial readers provide typical industrial connections such as RS-232 and RS-485, often along with Ethernet or even Wireless Lan (IEEE 802.11). Connections to Konnex bus media, such as powerline or twisted pair, are rarely available. See sections below for further details

- Power consumption: complex circuits require high power supply, so industrial readers' performance can be achieved only through significant power consumption. Bringing RFID into common house environments will require a more sensitive trade-off between performance and power.
- Ease of installation: industrial readers are designed to be installed and setup by experts, often with pre-installation planning and post-installation fine-tuning activities in order to get the most from the system. Instead, domestic installations require greater flexibility and possibly more automated setup procedures.

Main issues in introducing RFID in Konnex systems are those regarding read range and connection interfaces. Both problems can be successfully addressed during the project phase of the electronics parts involved (aiming at the correct trade-off for home installations). Part of this paper's objectives is related to introducing the need for a class of RFID devices suitable for home systems, and to explaining what can be achieved through exploiting such a technology in Konnex environments and, more in general, in home automation and building automation.

As to read range performance, the present work will rely on the assumption that a 5 to 10 metres read range can be achieved by RFID readers. While this is reasonable from a technological point of view (such systems exist already), it has to become economically accessible for home systems. The author believes that future developments of RFID technology will bring costs down to a suitable level for home automation.

With regard to connection interfaces we should note that it is a temporary issue, to be solved either by the integration of more kinds of connections on RFID readers or by the integration of Ethernet/IP in Konnex Framework.

Context Awareness

Introduction of RFID in common house environments shows to offer interesting opportunities to context analysis. Users can be recognized and, what's more, they can be located (at least at room level). Continuous knowledge of *who* is in *which room* can build awareness of the kind of situation is going on at that moment. The aim of this article is to show how this context awareness can be determinant for Smart Surveillance Systems.

Main weakness of current commercial domestic security systems is that they rely on a number of sensors (peripheral, volumetric, infrared sensors etc.) with an often weak correlation of their data. In the majority of cases, each of these sensors is used to directly trigger the alarm when a given threshold is exceeded for some specific value supposed to remain constant in normal conditions. The resulting usage model is to activate the system when house is unattended and deactivate it on return. In fact users' normal activity in the house would otherwise be identified as malicious. This kind of behavior can be described (roughly) modeling the security system as a logic network constituted by a single OR gate receiving input from all the sensors simultaneously and providing an *ALARM_ON/OFF* output signal (see Fig. 2). It is quite obvious that such a kind of systems is not endowed with satisfactory context awareness and cannot therefore be considered as an Ambient Intelligence environment.

The architecture outlined here aims at establishing a new concept for surveillance systems that gather data from a wide set of sensors inferring a suitable awareness of what is happening in the environment in order to distinguish normal events (everyday activities) from dangerous situations. The objective is to move away from the traditional activate/deactivate paradigm to reach an "*always on*" operative mode where the system and not the user is responsible to detect whether protection is

needed or not. This will be accomplished by exploiting current security model as a basic layer upon which to build a more complex and reliable surveillance environment.

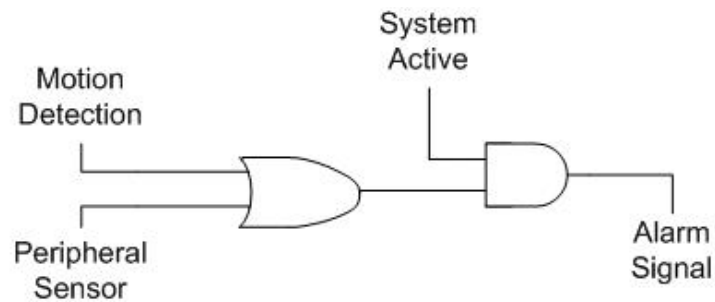


Figure 2: Traditional systems rough model.

Pattern Recognition

The approach explained here relies upon the concept of *pattern recognition*: the ability to detect particular sequences or configuration (patterns) inside sensors raw data. A pattern is described by Watanabe ([11]) as the “opposite of chaos”, an “entity that could be given a name”. This means that sensors dataflows contain data patterns that reveal each and every condition or situation taking place in the physical environment, and that it is possible to “extract” this information through a process of inference as a support for decision making. As a matter of fact, pattern recognition is a wide area of research activities, ranging from statistical analysis to syntactical processing, image and speech recognition, data mining and so forth, leveraging concepts such as neural networks, machine learning, expert systems and cognitive science. Among this scenario, what we want to propose here aims at exploiting what can be considered similar to a *template matching* technique, the most basic approach to pattern recognition. It consists in determining similarity between a prototype of the pattern (i.e. a template) and the actual dataflow.

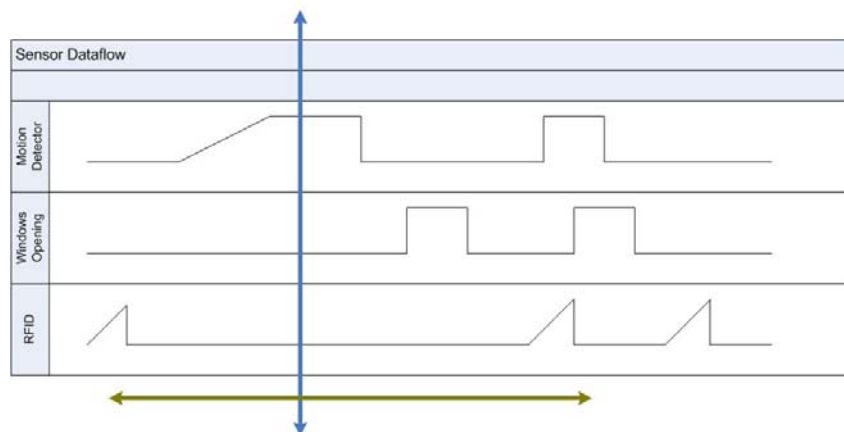


Figure 3: Pattern recognition inside dataflows

This paper focuses on the definition of a smart yet simple and reliable surveillance system, therefore we cannot introduce very complex activities, apart from those whose introduction brings added value in the working model of the system itself. As a consequence, this work will concentrate on basic pattern recognition, as depicted above.

The dataflows coming from field sensors can be scanned, searching for patterns, along two mainlines: a vertical one representing particular *combinations* of sensor values, and a horizontal one gathering *sequences* of sensor values. A combined approach could, eventually, evaluate and detect *sequences of combinations*, thus enriching the reliability and the fine-grain type of the detection process. What we want to realize is a system based on an ECA approach (Event Condition Action). That is, an event-driven system where *event* is an abstract and complex entity (a pattern or a combination of patterns according to what mentioned above) that triggers, on certain conditions, an *action*, where the latter is to be intended as an abstract concept as well (maybe a set of actions, a scenario, or even a *new event*).

A related approach to *Activity Recognition* has been followed at Intel Research division by Gaetano Borriello and Tanzeem Choudhury. They propose a user-centric model where sensors are carried along by the user all the time, embedded on a portable device, either a cellular phone or a wrist watch in future implementations, enabling the system to infer a number of different activity patterns and reacting accordingly ([12]).

Access Control

Another big issue on current security systems is found in the superficial modularity they usually provide: when they are activated *nobody* can do *anything* in the house and when they are deactivated *everybody* can do *everything*. With the introduction of user recognition through RFID systems, a more sophisticated *access control policy* could be defined and enforced. Let's have a look at a couple of possible application examples

- Parents may want to set a specific policy to prevent their child (wearing an RFID bracelet) to approach the staircase. Context detection will inhibit the alarm when the presence of a parent is detected near the child.
- Access to specific rooms (such as father's study where a gun is kept) could be prohibited on a user basis and depending on current context (i.e. the young son maybe forbidden unless his father is already present in the room) triggering an alarm upon violation. The kind of alarm, too, may be fitted by the system to current situation (i.e. an internal audio signal when a parent is detected in the house or an SMS when the boy is alone).

What should be noticed here is that traditional domestic security systems are not conceived to implement an *access control*. Instead they realize an *intrusion detection*, more or less accurate depending on the number, quality and type of sensors employed.

Smart Surveillance System Overview

System Requirements

Main features requested from the smart system can be summarized as follows:

Severe false alarms reduction and high signal to noise ratio

Alarm generation process has to be specifically refined: simple logic conditions (similar to *<if sensor active then alarm on>* type) will have to be replaced by more sophisticated ones gathering data from multiple sensors whose simultaneous or subsequent activation reliably reflect a pattern recognition and thus an event detection. Also, underlying logic will have to take into account

system's current state (for context awareness) accordingly to the ECA paradigm: in this way, the event is somehow "filtered" through the condition, prior to triggering any action.

"Alarm always on" way of operation

Alarm generation described above has to be designed without assuming a specific set of situations. More in detail, malicious activity has to be detected both when users are away and when at home. In this last case, suitable logic robustness is necessary in order to distinguish dangerous situations among normal ones. When this is accomplished, activation and deactivation commands will be eliminated. It should be noticed that this requirement cannot be met by simply providing an automatic alarm deactivation upon RFID detection of a verified user in the house. Instead, this proposal aims at the definition of a security system that continuously monitors the environment tailoring event detection on current context.

Differentiated alarm conditions and protection modularity

Different events should trigger different kinds of system reactions. This requires an evaluation of the different threat levels enabling for a modular policy definition.

Security Sensors

Traditional security systems often require a sensible design as to the number and type of sensors to be employed. In fact a high number of sensors provides a better sensitivity but affects the reliability of the system because it increases the probability of a false alarm.

Instead, a smart system as the one described here takes particular advantage from the presence of multiple sensors because they provide a more consistent and detailed dataflow enabling more reliable event detection. Incidentally, it is clarified here that the smart surveillance system design presented will assume the presence of several different sensors in order to better outline the system's potentialities, apart from the RFID sensors, whose introduction is the main goal of this proposal.

"Emergency" Context Model

It has been mentioned above that traditional system design does not usually model and treat the concept of *emergency events*. A correct identification of what an emergency is, precludes a better treatment of sensors dataflow. For example, an activation of the window opening sensor does not in itself provide a lot of information about current event but in most systems that would mean alarm activation even though it could be happened for normal reasons, especially when users are at home. A first differentiation will be introduced between *complete user actions* and *sensor noise* where the latter indicates all sensor activations that do not reflect a complete action (for example a motion detection not followed or preceded by a peripheral breach: that would mean an inconsistent sensor data or simply an object falling in the room, in which cases an alarm should not be triggered).

Next paragraph will show an example of the logic process needed to provide this distinction. Below is a schematic representation of the different events to be expected in a surveillance system endowed with context awareness (see Fig. 4). Two main regions are reported: *house unattended* (i.e. no *recognized* user is at home, that means no user equipped or wearing any recognized RFID tag) and *house attended*, when at least one recognized user has been individuated in the environment. Traditional systems usually realize this distinction requiring users to activate alarm system on leaving the house and deactivating it on return. This working model eliminates detection of every event appearing on the right-hand part of the diagram. In the security model described

here, instead, *house attended* case is the very application focus, so it will be analyzed in further detail.

Meaning of the schematic diagram is as follows: every sensor-driven data acquisition from the environment will cause the smart system to decide which of the seven possible areas current event should be placed in. The single area will then be associated to a threat level and a consequent alarm mode.

The right-hand part is further divided into two specific areas reflecting the fact that sensor activation took place *near a recognized user* (i.e. windows opening sensor activating in a room where a recognized user is present) or *far from a recognized user*, for example upstairs.

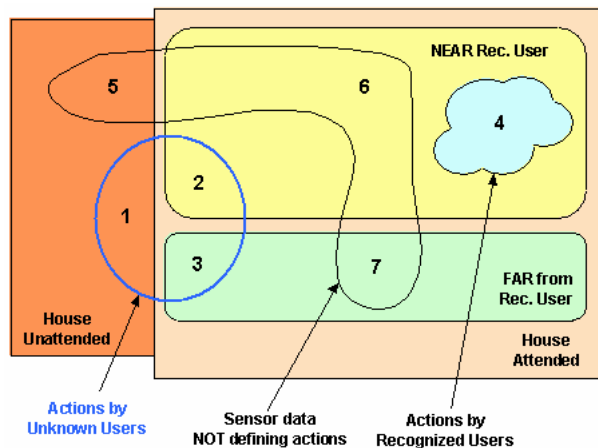


Figure 4: Context Model.

Inside this pattern we find three sets that define different possible events: the blue circle encloses all *complete actions performed by unknown users*, the light-blue cloud represents all *complete actions performed by recognized users* and the third set, spanning through the diagram, contains all the *sensor simple activations not representing a complete action*, as mentioned above. Intersection between these sets and the underlying pattern generates seven different contexts whose significance is here explained.

- 1 – Intrusion: an unknown person has performed a complete action (for example a peripheral breach plus a detected movement) while the house was unattended. Threat level: high
- 2 – Guest action: an unknown person has performed a complete action in a room where a recognized user has been detected. Threat level: none
- 3 – Intrusion: an unknown person has performed a complete action in a room where no recognized users have been detected. Threat level: very high (potential robbery).
- 4 – Normal action: a recognized user has performed a complete action. Threat level: medium (this region has been introduced for access control purposes as explained in section 1.3).
- 5 – Sensor noise: a single sensor activation has occurred. Threat level: pre-alarm (another single sensor activation may cause the system to switch to region 1).
- 6 – Sensor noise: a single sensor activation has occurred. Threat level: pre-alarm (another single sensor activation may cause the system to switch to region 2 or 4).
- 7 – Sensor noise: a single sensor activation has occurred. Threat level: pre-alarm (another single sensor activation may cause the system to switch to region 3).

Introduction of RFID and context-awareness offers a fine grain evaluation of events. In the “unattended” case, region 1 and 5 are distinguished, thus reducing false alarms probability and in the “attended” case, intrusion detection (region 3) and access control (region 4) can be accomplished.

In opposition to a traditional system, smart surveillance systems reliability takes great advantage from usage of a variety of sensors because this enhances the possibility of detecting a complete action eliminating sensor noise as depicted in the diagram.

The state machine depicted below replaces the simple logic network of Fig. 2. A single sensor activation will only trigger a pre-alarm condition with no alarm signal associated (see regions 5, 6 and 7 in Fig. 4). Further sensor data consistently indicating a complete action, will bring the system to an alarm condition that will be checked against current context to determine consequent actions.

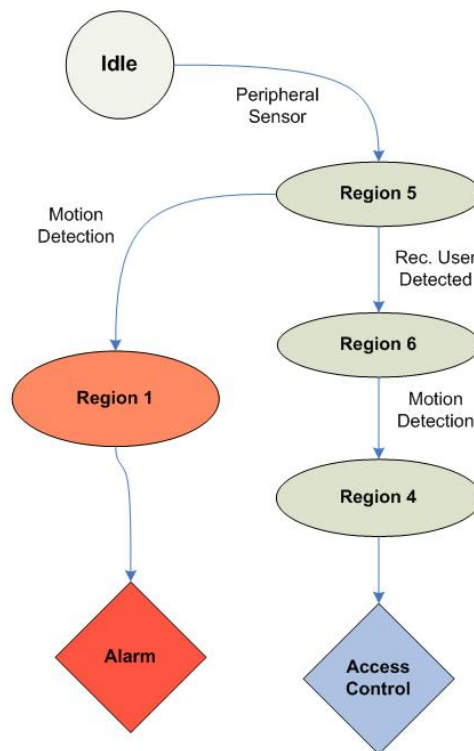


Figure 5: State Machine for alarm generation

RFID – EPC Infrastructure and integration in Konnex Networks

As mentioned above, RFID infrastructure is a critical factor for system’s operation. However, it should be noticed that suitable design here is a requirement for other application fields, too. Several ambient intelligence scenarios do rely on the existence of such an infrastructure. Therefore, an integrated approach, taking into account other future utilization, is the best choice.

Moreover, we should note that, although RFID is a leading technology, likely to be introduced soon in home and building automation, no significant and definitive effort has been dedicated to evaluate and determine how this integration can happen. Being Konnex a widespread bus technology both in buildings and home environments, and since it is going to be adopted in a growing number of future installations, some considerations are needed here in order to try to solve this issue and to state the need for further research activities. Therefore, in the following paragraphs we will address

the problem of integrating RFID readers in a Konnex network, taking into account that neither Konnex nor RFID technologies have been designed to work together. Main obstacle is the lack of suitable physical connections to Konnex media on RFID readers. What RFID readers usually provide is an RS-232 interface and sometimes RS-485, Ethernet or Wireless Lan. Connecting them to twisted pair or powerline currently requires some kind of hardware adaptation.

Another issue that may arise is about bandwidth requirements and message length typical in RFID environments. How will they fit on a Konnex network? This paper will propose a first examination of the problem following a rule of thumb, showing why this integration is possible, at least in home automation.

Connecting RFID Readers to KNX: the proxy box

As noticed above, RFID readers do not currently provide connection to Konnex media such as Powerline or Twisted Pair. In the perspective of an integration of RFID services in home environments, it could be foreseen that future implementations will include those connections as a standard for “home” RFID readers. Although that is true to some extent, a few considerations are required here, in order to propose a solution to this issue.

This paper envisages a multi-level architecture where every room in the house is equipped with a *Proxy Box* acting as a local device coordinating every non-KNX sensor available and one or more RFID reader (depending on room’s dimension). Proxy Boxes will provide suitable connectivity for RFID readers, interfacing them to Konnex media.

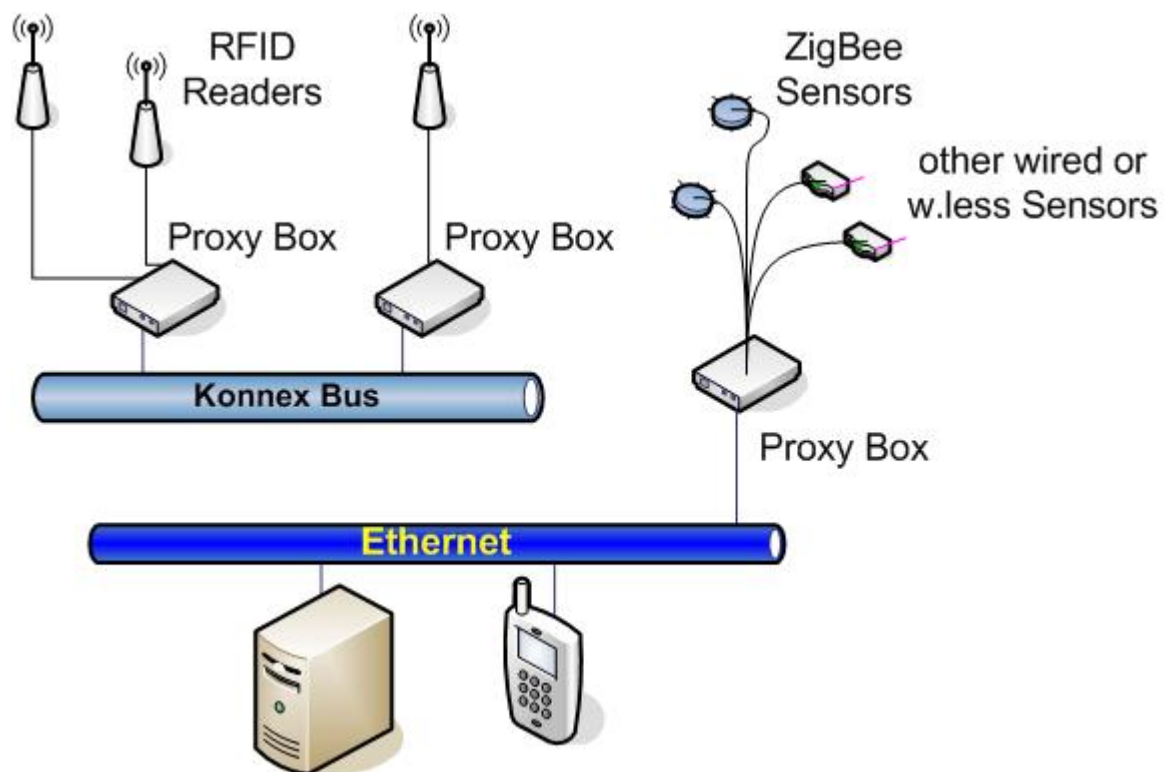


Figure 6: RFID and Proxy Box Infrastructure

Moreover, as the picture depicts, Proxy boxes could interface to Ethernet as well, in order to accomplish various tasks: they could provide *protocol conversions* between different types of sensors and devices (Bluetooth or ZigBee wireless devices and sensors), allow for *external access*

to room's sensors (through a TCP/IP stack that may not be available on small devices), execute *local computation and coordination* tasks in order to support other computational units' job. The reason why proxy boxes are introduced here is not related to smart surveillance in itself. Instead they may be a key factor in building a suitable architecture for ambient intelligence applications at large.

In the remaining part of this paper, RFID readers will be assumed as directly connected to Konnex bus, regardless of the way this is accomplished: either through a Proxy Box or by specific physical interfaces available in the reader itself.

RFID networking: EPC messages and bandwidth requirements

Prior to analyzing the impact of the introduction of RFID in a Konnex network, a brief explanation of Electronic Product Code (EPC) is needed. While the term RFID stands for a wide range of electronic technologies enabling wireless identification of objects and people by means of tiny transmitter chips accessible through radio frequencies, EPC is an international standard that specifies *what data* those chips store and send when interrogated. In other words, the electronic product code is a standardized universal code identifying any object, and the EPCGlobal international organization specifies how this information has to be organized inside the chips: actual number of bits, significance of the various code parts and so on. Moreover the EPC initiative also deals with the global infrastructure required to effectively use RFID and EPC potentiality. It is still to be clearly stated that all future RFID chips will be actually using EPC codes and global services. Nevertheless, the big effort undertaken by many international enterprises on the development of EPC, makes it quite obvious to expect that a deep integration of EPC inside RFID technology is in the near future. Among others, Sun Microsystems is pushing towards the usage of EPC, and they already developed an EPC infrastructure based on Java technologies.

EPC specifications have been defined in several different version, with a close regard to how much will EPC-RFID chips will cost: 64, 96 and 256 bits EPC codes are possible, depending on application requirements and sustainable cost. Figure below shows the 96 bits case.

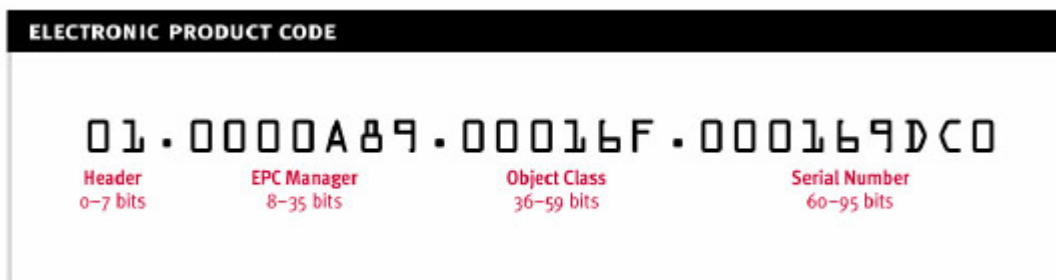


Figure 6: 96 bits EPC code (courtesy of EPCGlobal Inc.)

Purpose of EPC is to uniquely identify any physical object in the world (unlike current bar-code which mainly identifies classes of objects). That's why a 256 bit version has been defined and planned (256 bits provide some 10^{77} codes which, in turn, produce a density of around 10^{63} EPC codes per square meter on the whole earth surface). In the 96 bit case the EPC code is organized as follows:

- Header (8bits) for EPC version number
- EPC manager field (28 bits) specifying the name of the manufacturer
- Object class (24 bits) specifying the class of the product (inside the enterprise production)

- Serial Number (36 bits) that uniquely identifies the single item

This 96-bit string is stored on a tag chip and accessed by an RFID reader, that sends this raw code to a network of EPC services enabled to resolve the code to the associated (set of) information and send it to authorized users (thus resolving many of the security and privacy issues raised around RFID technology). Next paragraph will treat this argument.

In conclusion, EPC messages will typically require to transfer from 12 bytes (96 bits version) to 32 bytes (256 bits version).

Konnex Specification Supplement 13 for extended frame format, both for powerline and for twisted pair, defines a maximum frame length that allows for 64 octets for the Application Data Unit (APDU, i.e. the actual message to be sent to the Konnex network). Therefore, even the longest EPC code will fit into a Konnex frame. Moreover, the fact that only half of the frame length is required (in the worst case) makes it easier to believe that no big impact has to be expected on Konnex networking performance (in terms of collision probability and response time) due to the introduction of EPC - RFID Readers.

Of course, this is especially true in home automation environments, where RFID events are not going to be very frequent. In fact, sending a 256 bit EPC code on a Konnex powerline PL110 cable, requires a time slot of about a quarter of a second (being 1200 bps the line speed and considering a message of approximately 300 bits). This value decreases by a factor of 8 when using a twisted pair TP1 line (9600 bps). Industrial environment, then, will require faster lines, in order to successfully manage the tenth RFID events per second likely to happen in such applications (that's why industrial readers provide Ethernet connections).

Access to EPC service infrastructure

EPCGlobal has defined a complete service infrastructure for distributed and dynamic collection of information regarding tagged items. EPC architecture relies on the following elements

- Object Naming Servers (ONS): they match RFID tags to information on the tagged object by mapping the EPC code to a PML server
- PML (Physical Markup Language) Servers: they store actual information regarding a physical object. This information is formatted in an XML-based language
- Savant: a middleware that establishes a link between RFID readers and the enterprise applications level, and provides some low-level functions like duplicate reads detections, and protocol adaptation

As a whole, EPC information services will have the task to store and send information regarding every product code individuating every single RFID-tagged item ([8]). While not strictly necessary for the security system here proposed, access to EPC services will be required by, for example, smart fridge applications where information regarding official food products may be collected from corresponding ONS/PML servers

For these reasons, suitable connectivity to EPC global services should be introduced into the system described here. In order to fulfill such requirement, two possible solutions are described below.

First and simpler approach consists in setting up a KNXnet/IP gateway server that connects Konnex sub-network to an IP local network and the internet through an access router. This approach is depicted below.

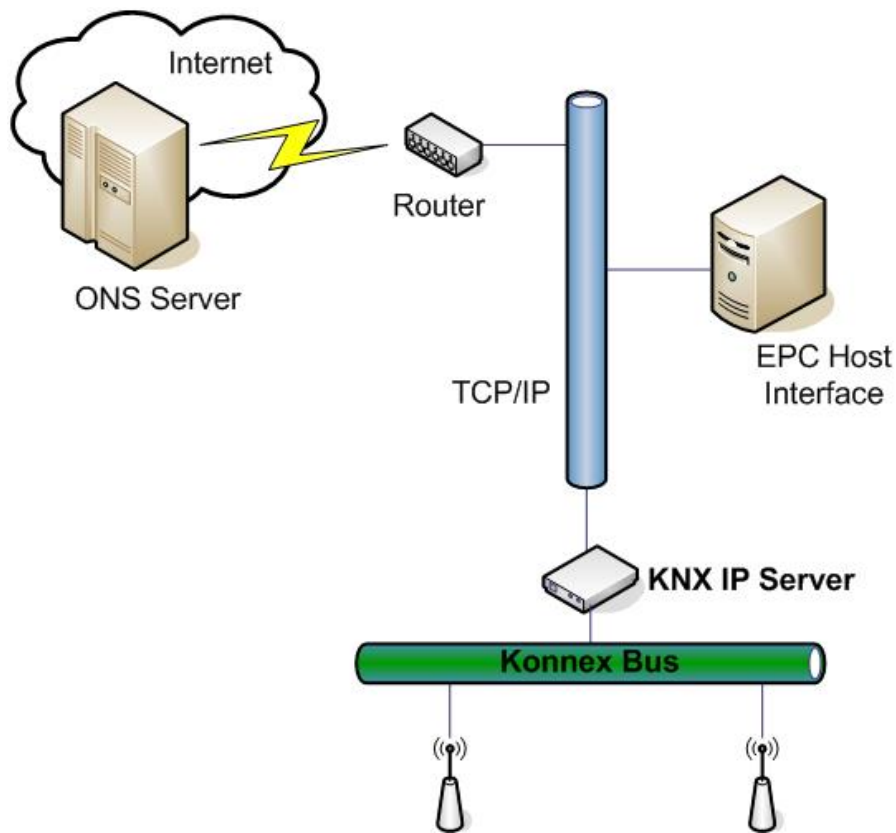


Figure 7: Interfacing Konnex network to global EPC services

The “EPC Host Interface” is a fundamental element because it will contain the logic binding between KNX messages coming from specific devices (the RFID readers) virtualized on the IP network by the IP server, and the external services. In other words a static configuration is required on the EPC host once the RFID infrastructure is setup. This could be a weak point in some applications. Therefore this solution may not be the best choice in some cases.

Another way to address the issue is to exploit the OSGi framework, especially for its discovery features that may help with auto-configurability of the system. It should be noted that Sun Microsystems extensively supports EPC core technology providing a middleware for java-enabled platforms like OSGi. For this purpose, a Konnex driver would be needed in order to establish physical connection to Konnex medium for an OSGi gateway. A comprehensive approach to OSGi integration into Konnex technology has been proposed by Georg Neugschwandtner and Wolfgang Kastner in the 2003 Konnex Conference ([13]) and that work is a reference for the following considerations.

First step is to define and setup an EPC service bundle to deal with EPC requests towards ONS services (this bundle would use the existing Sun core libraries for EPC). Other OSGi modules to be implemented are those entitled to deal with Pattern Recognition and Activity Inference, gathering dataflows from field sensors and implementing the feature extraction process. Furthermore an ECA engine will be necessary, in order to deal with policy management and definition, enabling the end user to control how the system will react to specific events (future developments may define how to avoid accidental misconfiguration by inexperienced users).

Below is a graphical representation of the resulting architecture.

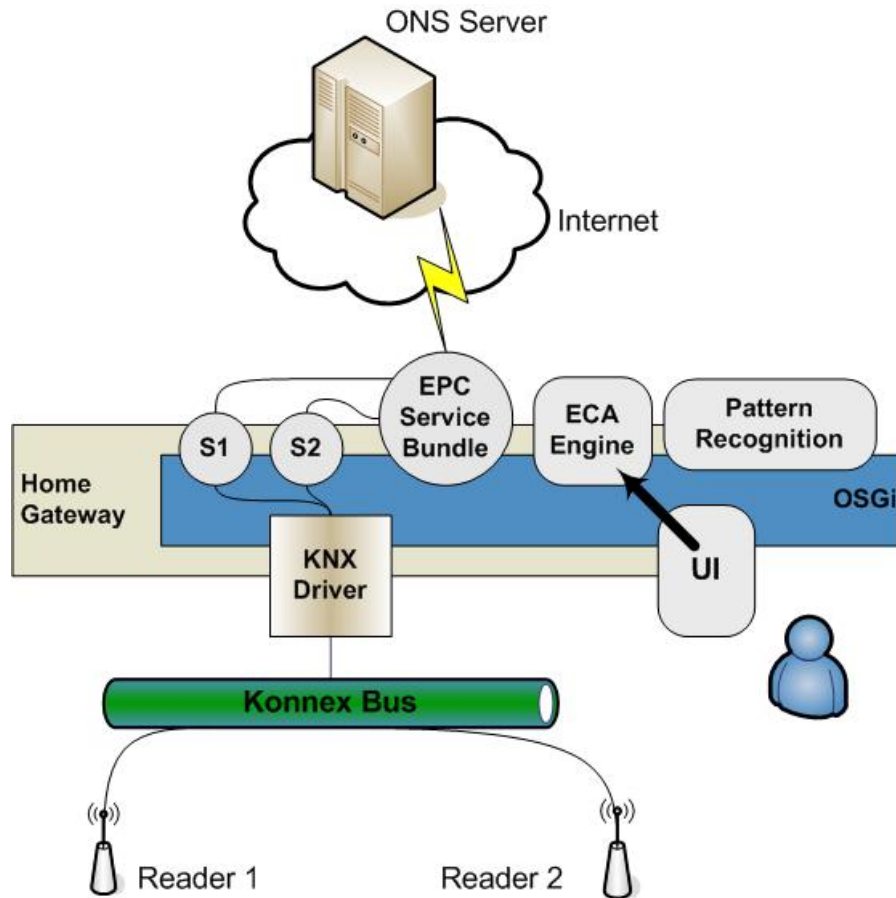


Figure 8: Interfacing Konnex network to global EPC services through OSGi Framework

The RFID readers discovered on the Konnex network by the Konnex driver generate two services S1 and S2. These services interact with the EPC bundle at run-time for ONS resolution. The latter will forward those requests to available EPC services on the external network and report the results back to the system. Further research on this point is required before actual development of such a complex yet flexible system.

Discussion

Still some open issues have to be resolved before Ambient Intelligence applications could take advantage from RFID infrastructures in home environments like the one presented here.

User acceptance of this technology may not be a minor problem both for *privacy* (RFID has recently raised a few reactions concerning privacy about commercial initiatives exploiting this technology) and *health* reasons (users show to be skeptical about the fact that radio frequency technologies are regulated enough to ensure health-safe operation).

Wireless coexistence with other protocols working on 2,4GHz ISM frequency band such as Bluetooth, ZigBee (IEEE 802.15) and Wi-Fi (IEEE 802.11) could also be an obstacle. Presence of devices operating on those protocols has to be surely foreseen in future home environments. Therefore suitable standards' adaptation will soon be required.

Conclusions

RFID technology will soon come to item level tagging, enabling novel applications to be exploited. Home environments will then see the presence of several RFID tags on foods, clothes, devices etc. Among the possibilities offered by this new technology, at least two will create a major interest on users: food inventory and monitoring, and washing machine automation. Therefore, along with RFID tagged items, users will face the need for an RFID infrastructure allowing them to take full advantage of the new opportunities.

Starting from this assumption, this paper has proposed a smart surveillance system that, relying its operation on this infrastructure, provides a new way of conceiving alarm system. Always on mode of operation, better modularity and reliability as to false alarm reduction are key objectives of the system. Users' perception of the underlying system will be minimized and no activation/deactivation will be required from them. Context awareness will provide means to substitute user intervention and to analyze every different scenario, engaging actions sensitively reflecting the situation at hand, also leveraging concepts coming from the field of pattern recognition.

It has been shown how the integration of an RFID infrastructure into Konnex network can be achieved with no performance issues, in home environments. Future development is required on the fields of RFID interfacing to Konnex and of EPC services access from within Konnex.

References

- [1] Radio Regulations, 1998 International Telecommunications Union.
- [2] "An analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design", Tom Ahlkvist, 1998.
- [3] Progettazione di un sistema di controllo dell'accesso basato su ruoli, Università di Bologna, Massimo Aliberti 2003.
- [4] Thierry Roz and Vincent Fuentes, "Using Low Power Transponders and Tags for RFID Applications" EM Microelectronic Marin SA, Switzerland
- [5] Draft Paper on the Characteristics of RFID-Systems, AIM Frequency Forums, 2000
- [6] Klaus Finkensteller, RFID Handbook, John Wiley & Sons, New York 1999
- [7] Bluetooth/802.11 Protocol Adaptation for RFID Tags, Raj Bridgelall, Symbol Technologies, New York
- [8] MIT Auto-ID Center, "The Networked Physical World: Proposals for engineering the next generation of computing, commerce and automatic identification", MIT AUTO-ID-WH-001, 2000
- [9] David K. Cheng, Field and Wave Electromagnetics, Addison-Wesley Publishing, New York 1992
- [10] Vince Stanford, "Pervasive Computing goes the last Hundred feet with RFID Systems", IEEE ComSoc 2003
- [11] S. Watanabe, Pattern Recognition: Human and Mechanical. New York: Wiley, 1985
- [12] Gaetano Borriello & Tanzeem Choudhury, "Activity Recognition: the Next Stage in the Development of Context-Aware Applications", *UW/CSE & Intel Research Seattle*
- [13] Georg Neugschwandtner and Wolfgang Kastner, "EIB Network Access and Configuration Services for OSGi Environments", 2003 Konnex Scientific Conference