Intruder Alarm Systems - The Road Ahead

Rui Manuel Antunes and Frederico Lapa Grilo
Escola Superior de Tecnologia de Setúbal (Setúbal Polytechnic Institute)
Portugal

1. Introduction

This chapter presents today's state of the art intruder alarm systems and detectors, giving special focus on the several technologies applied, including the wireless transmission and reception of alarm messages and commands through GSM/GPRS, TCP/IP, and the project and development of web-based intruder alarm monitoring and control hardware and software. Useful project techniques are also described in detail, concerning the installation of intruder alarm systems for homeowners and for commercial/industrial use.
New developments for distributed web-based intruder alarm systems, which can include not only traditional signaling functions but also new "smart" decision functions are challenging thrills today for the intruder alarm designers. Web-based intruder alarm systems may include the use of distributed nets ("grids"), giving each node the ability to dynamically configure its functions within entire respect for the security scope issues. By this approach, distributed network intelligence will allow an intruder alarm system to react to multi-signalization intrusion situations in a much more efficient way, being also able to distinguish more accurately real security violations from unadvertedly operations.
The development of web-based intruder alarm systems from the evolution of the new APIs, and from new languages based on the web 2.0 philosophy will lead to a new level for intruder alarm monitoring and control, with the integration of several new features such as, for example, using signal pre-processing and Geo-localization.

2. Today's Intruder Alarm Systems

2.1 Intruder Alarms and Detectors

Security alarm systems for intrusion prevention is massively present in our own homes and Companies.
A basic intruder alarm system consists of a control panel, with rechargeable battery power backup and internal or external keypads, several interior and perimeter intrusion detectors, and one external sounder, at least.
An intruder alarm system can be classified as an hardwired , wireless, or an hybrid system. Wireless systems are used when there is not pre-wiring, operating at 433/868 MHz.
Most secure intruder alarm systems are hardwired systems, because wireless systems will use additional battery power and, even with Anti-jamming protection, still can be affected

by radio-frequency interferences. Hybrid alarm systems allow simultaneously the installation of wireless and hardwired detectors, being the most versatile.

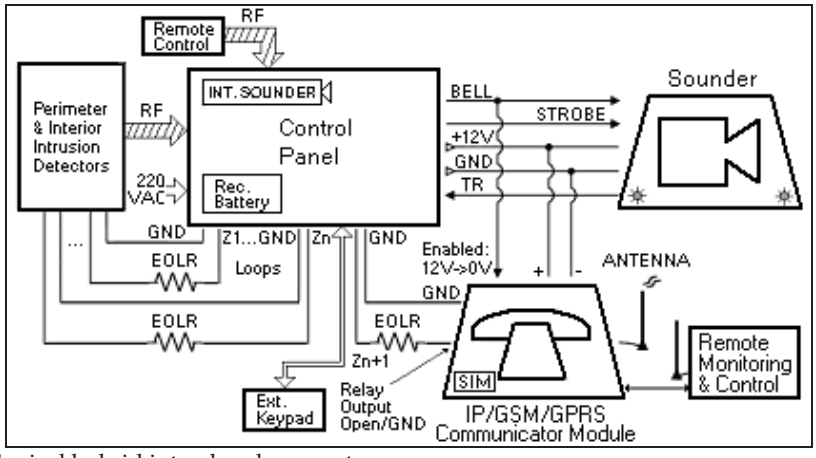

Fig. 1. Typical hybrid intruder alarm system

The STROBE signal is the output from the alarm control panel that will enable the flash lamps from the external sounder. The BELL signal is the output signal from the alarm control panel, used for triggering the alarm sounder devices. Both signals trigger from 12V to 0V.

VBAT (+12V) and GND are the power source terminals for the alarm control panel and the external sounder. Finally, Tamper Return (TR) is the external sounder output signal, used to indicate an opened sounder cover tamper.

In hardwired intruder alarm systems each protected zone is a closed loop circuit, where a fixed current flows. The first protected zones are usually door entry zones, for manual or remote entry and for exit pre-time arming and disarming. Several commercial intruder alarm configurations are available: NO, NC, EOLR, 2-EOLR, and 3-EOLR (End-of-line-resistor loop circuits).

Most common intrusion detectors, that can usually be classified as perimeter and interior detector devices are: PIR (passive infrared motion detectors), PET (pet immune motion detectors), dual technology motion detectors, acoustic glass break detectors, vibration/chock detectors, magnetic contact detectors and others (such as IR beam barrier or ultrasound sensors).

A PET immune detector is made by two PIR motion detectors, specially developed to detect simultaneously a high and low layer pre-assigned beam. As pets under a certain amount of weight are not large enough to hit both beams, the PET motion detector does not feel them.

Outdoor PIR and dual technology motion detectors, commonly named WatchOUT detectors, are also being used as an important additional perimeter motion detector. Pet immune 360º ceiling PIRs and dual technology motion detectors are also present in industrial facilities.

Dual technology motion detectors can have Anti-cloak technology (ATC) to thwart camouflaged burglars. A moving cloaked intruder will emit a weak IR signal that has characteristic shape. This technology applies recognition algorithms that disregard the

signal strength and focuses on its pattern. Once verifying that it matches with the signal of a burglar, ACT immediately switches to the microwave triggering mode.
A dual technology motion detector can be Anti-masking, by using an active infrared channel located behind the lens to protect against spraying and covering burglar techniques. Also, this detector can bring Anti-fluorescent signal processing to avoid the fluorescent light flashes false alarms.
Quad element PIR technology can improve intruder catch and reduce false alarms, because are used two PIR channels/twin-elements with separate Fresnel lenses that can distinguish more effectively between humans and other infrared sources.
The use of Grenline technology is increasing, because a dual technology detector will disable its microwave sensor when a building or zone is occupied. Thus, there is no need to constantly send high frequency microwave signals to areas occupied by humans, reducing also the power consumption.
Magnetic contact detectors do not need to be powered at all. The presence of the magnetic field is enough to trigger the embedded relay from the detector that is attached, needing only a two-wire cable for its installation.
Acoustic glass break detectors add important perimeter protection by detecting potential burglars, while them are still outside. The main problem concerning the acoustic devices is that an intruder can still achieve to force to open a window without needing to break the glass. So, these kind of perimeter acoustic detectors should be installed along with other interior intrusion detection devices.
Vibration/chock sensors are a good alternative for acoustic glass break detectors, by sensing the vibration on a window even before it breaks, thus providing a reliable perimeter protection.

2.2 Project Techniques

In an hardwired alarm system End-of-line-resistors (EOL) can supervise the wires, preventing wire tampering. The burglar when shorts loop wires together hides the End-of-line-resistor from the control panel, letting the control panel know that something is going on. The EOL resistor value is usually provided by the alarm system manufacturer, typically 5.6KΩ. The right placement of an EOL resistor is always at the last detector, on the loop circuit. We should never mount EOL resistors at the control panel, because it will act as if it has no EOL resistors.
A Double-End-of-line-resistor (2-EOLR) will allow to distinguish between an opened cover tamper from the trigger detector motion condition, and Triple-End-of-line-resistor may trigger the Anti-masking detector or a fault.

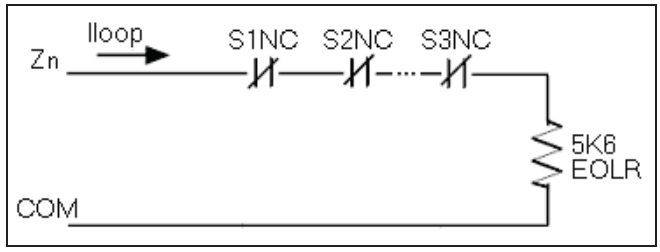

Fig. 2. EOLR circuit configuration

In a 2-EORL circuit configuration a (S3) tamper output normally closed detector terminal must be serial wired with the normally closed detector terminal, as shown in figure 3:

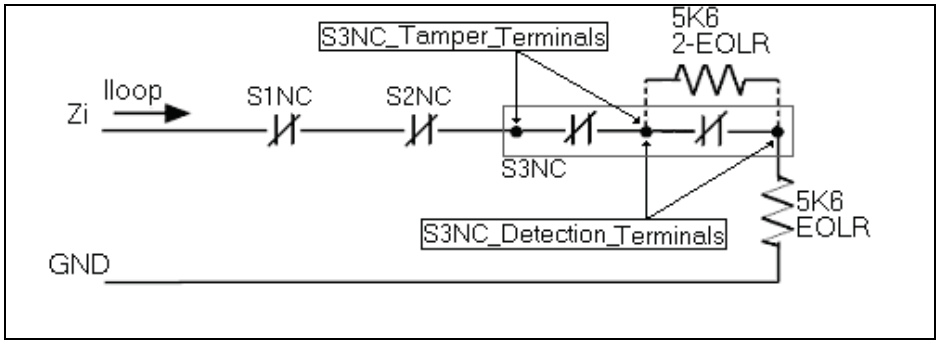

Fig. 3. 2-EOLR circuit configuration

For a 3-EORL circuit configuration the Anti-masking/fault terminal must be also serial wired with the normally closed detector and tamper output terminals , as shown below:

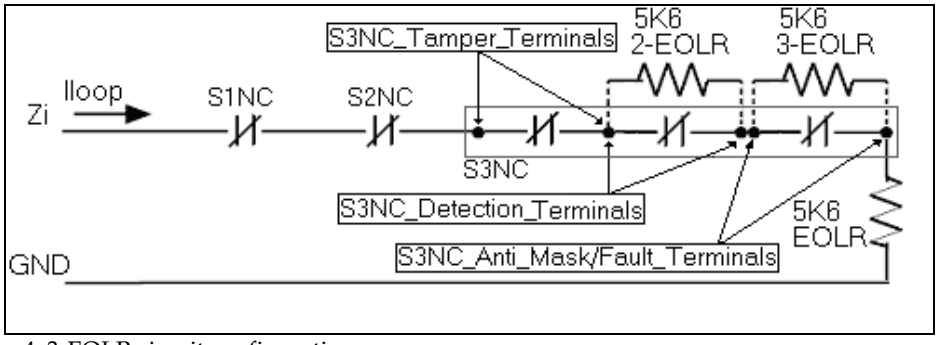

Fig. 4. 3-EOLR circuit configuration

Most recent intruder alarm systems allow now programmed supervision for both single, double, or triple End-of-line-resistor loop circuit configurations.
Remote monitoring/control can be made using the telephone line or with a GSM/GPRS/IP module. Both allow a connection with any person, or to a dedicated monitoring station.
GSM/GPRS modules have entry channels usually enabled to the negative transition (from 12V to 0V), thus being able to be directly connected to the STROBE and BELL control panel signals. These modules can be programmed from a mobile phone or from an USB port, pre-defining the destination phone numbers with SMS/MMS or simple alarm voice messages. Existing control panel telephone lines can also be directly wired to a GSM/GPRS/IP module communicator, and be used to send intruder alarm messages.
To adapt an older alarm system to send GSM/GPRS or IP alerts, the BELL output may be wired to an input terminal of a GSM/GPRS/IP module. This simple arrangement will avoid the need for extra month fees in contracts with security companies. GSM/GPRS/IP modules can also be used to arm, disarm and even to verify all detectors, or a ready-to-arm condition.

Also, a bidirectional module can be used when an intruder alarm control panel has already built-in an arming/disarming loop (programmed as maintained key switch arm).
Next table shows some important rules and advices, concerning the project of intruder alarm systems for homeowners (Antunes, 2007a):

PIR/PET motion detectors:
1- Before mounting a detector, always read carefully the manufacturer installation manuals.
2- When installing a detector, care should be taken to check if manufacturer infrared and microwave radiation diagrams fills the area to protect.
3- The detector must be fixed approximately 2 meters from the floor (depends also on the module), and should always be identified with a stick number.
4- The detector must be pointed to the opposite direction of light entries and windows, and never directly to sun light.
5- A detector must preferentially point to frequent passage areas, such as door entries and corridors.
6- Avoid mounting the detector in areas near air conditioning, heaters, fans and ovens, where it could detect air flows.
7- Avoid installing a detector near areas where high humidity or vapor exists, that could easily cause condensation.
8- Avoid screens and moving curtains that may divide any infrared protected zone.
9- A 90º detector must be preferentially mounted to a corner, while a 360º detector should be mounted on the ceiling.
10- Screw the detector only to fix parts, like consistent walls.
11- Try to avoid using wall swivels, that could rotate, modifying the position of the detector.
12- After the installation check if all motion detectors are installed by performing always in the end a "walk test".
Dual Technology motion detectors:
1- Dual technology detectors should not be used in wireless alarm systems, because the power consumption will be much higher than using wireless PIR detectors.
2- Not recommended for pacemaker owners.
Acoustic glass break detectors:
1- Should be avoided installing acoustic glass break detectors in kitchens, or near audio speakers.
2- The detector's microphone should be pointed towards the direction of all windows, never more than 9 meters away (straight line).
3- A perimeter acoustic sensor should be installed also with another interior intrusion detector.
Magnetic contact detectors:
1- Magnetic contact detectors should be hidden as much as possible, and using embedded magnetic switches.
2- The magnet must be attached always to the moving part of a door or window.
3- The distance between the magnet and the detector must be within the manufacturer limits (usually less than 10mm).

4- In magnetic contact detectors only two-conductor alarm cables should be used.
5- Where possible, mount the body of a magnetic detector close to the top of the non-moving frame of a door or window.
6- Always align correctly the magnet with the existing marc on the detector.
7- Magnetic contact detectors must not be fixed near metallic, magnetic structures, or high voltage cables, and nor near the floor.
Vibration/Chock detectors:
1- Should be used models that bring also magnetic contacts, for extra double protection on opening doors and windows.
Wireless detectors:
1- Do not install wireless magnetic detectors near electrical engines and other electronic equipment that could generate radiofrequency interferences, like automatic curtains or garage doors.
For the intruder alarm control panel:
1- First it is necessary to study in detail the location of the areas to protect, and to choose the right detectors and the alarm system to be installed. 2- The chosen intruder alarm control panel has to achieve the best cost/liability/time relation, considering also the esthetic outcome of the hardwired, wireless or hybrid solution. 3- The right protected zones must guarantee a minimal number of loops and the total number of sensors needed, assuming a PIR/PET/Dual Technology interior motion detector solution per protected zone, along with the use of additional perimeter detectors for the outside, and for windows and doors. 4- Install the alarm control panel in hidden places (inside a closet for example), to avoid and prevent burglar vandal acts. 5- If only one keypad is used, it should be placed near the frequently used door. 6- Only keypads should be visible, preferentially in frequent passage areas. 7- An additional Panic distress code should always be programmed into the intruder alarm control panel, for letting know (silently) that someone might be in a dangerous situation.

Table 1. Basic intruder alarm project rules

A perimeter arming mode feature will allow for a homeowner to freely circulate at night, inside his home, yet still being the intruder alarm system ready and armed, and continuously monitoring all house perimeter sensors (such as doors and windows detectors), only disregarding the interior motion detectors.

A remote control panel arming/disarming operation can be made in many intruder alarm models, using a single specific current loop (or zone) previously programmed for that purpose. This will allow to remotely arm and disarm an intruder alarm system with a PDA or a mobile phone.

Automatic arming/disarming uses the alarm control panel internal real-time-clock (and calendar). This programmable mode could be very useful for protecting places where predefined working timetables exist (at stores, or at industry for example). Door chime mode (Antunes, 2007b) is also often used in stores, allowing a quick audible sound, for example, each time a client enters inside a store.

3. Web-Based Intruder Alarm Systems

3.1 Monitoring and Control

IP modules allow the communication between an intruder alarm system and a remote monitoring station. Some connect directly to the existing control panel main telephone lines, transmitting in ContactID or SIA protocols to an IP receiver station.

A very low cost IP module can be made by using an embedded standard micro web-server, with built-in IP connectivity, that is able to send and receive digital commands via TCP/IP (Adão et al., 2008a). This could be a nice low cost solution for the existing alarm and notification home automation models, and without the need to have a main server PC running, or special software (like other expensive available solutions). Although care should be taken to assure a full SSL (Secure Sockets Layer) communication.

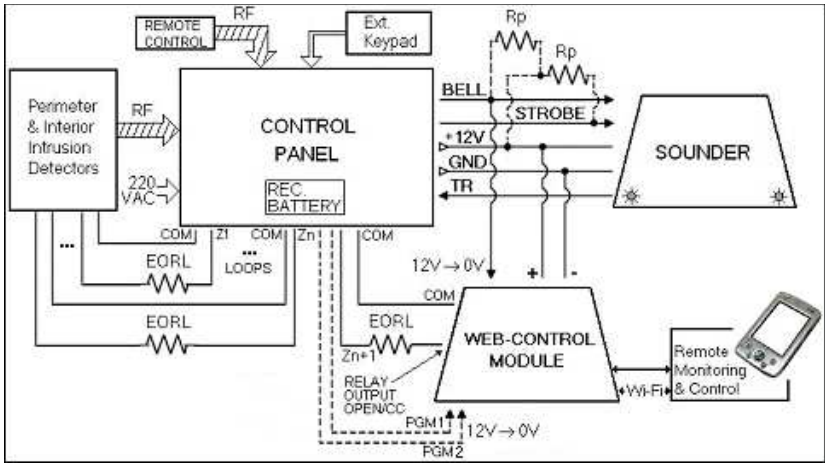

Fig. 5. Alarm circuit for low cost web-control and monitoring

The BELL and STROBE outputs may usually need an external pull-up resistor to work, depending on the control panel and the sounder model.

Zones may also be programmed to be used as key switch arming/disarming. This will allow to remotely arm or disarm an intruder alarm control panel. Note that a key switch web-control module needs to be connected to the additional loop zone (n+1) that is programmed as maintained key switch arm, as shown below:

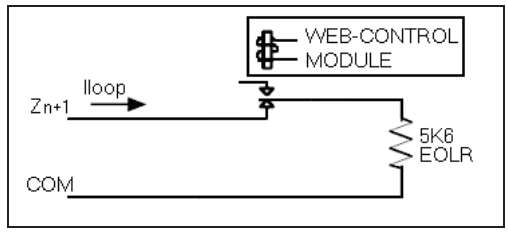

Fig. 6. Dedicated EOLR n+1th maintained key switch arm zone, with the web-control module

So, in the restored state the alarm control panel is usually disarmed. The switching of this n+1th zone to the alarm state may turn a control panel to arm. Nevertheless this operation has to be confirmed, because IP communications sometimes might go down. That is why an available output line (PGM1) may also be programmed, when possible, to be able to confirm an armed condition.
A second control panel output line (PGM2), usually provided, can be very useful to monitor a ready-to-arm status. This could provide, for example, to remotely check a detector malfunction or a false trigger condition, thus preventing a remote arming command.
A low cost micro web-server (Adão et al., 2008b) usually allows interaction with .CGI web pages, making possible the user to call pre-programmed functions within the web-server from an internet browser, for reading inputs and set or reset output values.
A CGI html and JavaScript versatile web page can be easily build, even by an homeowner, to upgrade an intruder alarm system with a web page interface, that is directly downloaded into a non-volatile chip, inside the micro web-server.

3.2 New Developments for Distributed Web-Based Intruder Alarm Systems

New intruder alarm systems based on web monitoring and control are now starting to grow into complete distributed nets, not only with traditional signaling functions but also with new "smart" decision functions.
Midllware computational systems rely, with more than a decade, on a grid computing scalable distributed nets approach (Grilo & Figueiredo, 2008), with dynamic capacity, and can be a starting reference on the development of new distributed web-based intruder alarm systems.
Web based intruder alarm systems can exist in distributed nodes ("Grid topology", as shown in next figure), having each node the ability to dynamically change its functions:

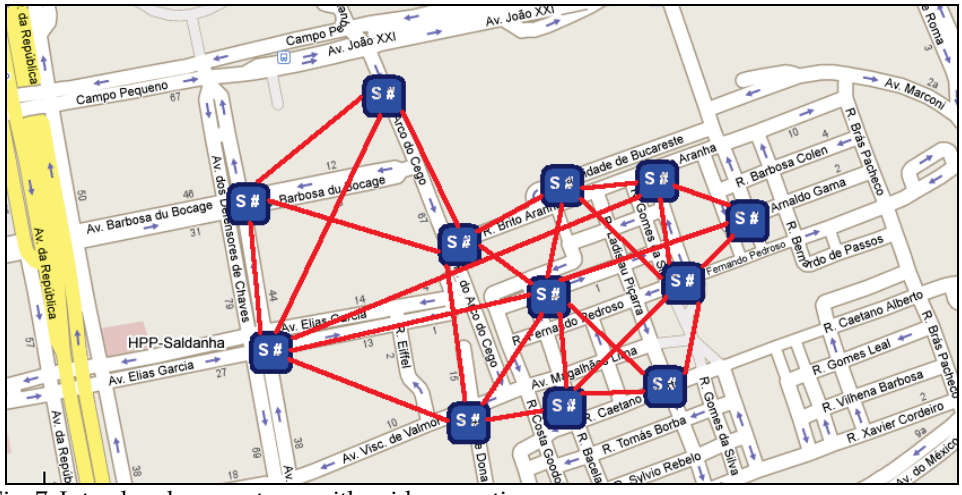

Fig. 7. Intruder alarm systems with grid computing

From this approach the "intelligence" capability of all the distributed net will be applied to react in a much more efficient way to the different alarm situations that can occur, being the

alarm systems able to distinguish more accurately real security violations from, for example, unadvertedly operations, increasing security levels and also the immunity to technical failures.
The development of web-based systems from the evolution of the new APIs, and from the new languages based on the web 2.0 generation are also bringing improvements for intruder alarm systems.

3.2.1 Integration

Using the IP protocol for the net support and Html as the language for the web-servers, it is created the possibility to support several hardware technologies on the same physical net implementation, and also, no less important, created the capability to use and connect to the network systems from different suppliers and technologies, which will give an huge flexibility, not only with the net topology but also at the built grids (individual alarm systems), improving the adaptation capabilities.

3.2.2 Systems Redundancy

Being necessary to certain applications and environments to have a redundancy systems strategy, the topology of the distributed network ("grid") can implement this functionality with efficiency, because with all intruder alarm systems connected we can simply choose those for the same security and surveillance area. The systems given for the same area can have then a privileged communication.
We might considerer use redundancy in different ways, as for example:

- One of the systems is active for security violations and the other is active, in backup function, in case of failure of the first, turning all system more robust.
- The two systems are active and ready. In case of a security violation detected, a mutual approach giving the response of each system is made, as shown below:

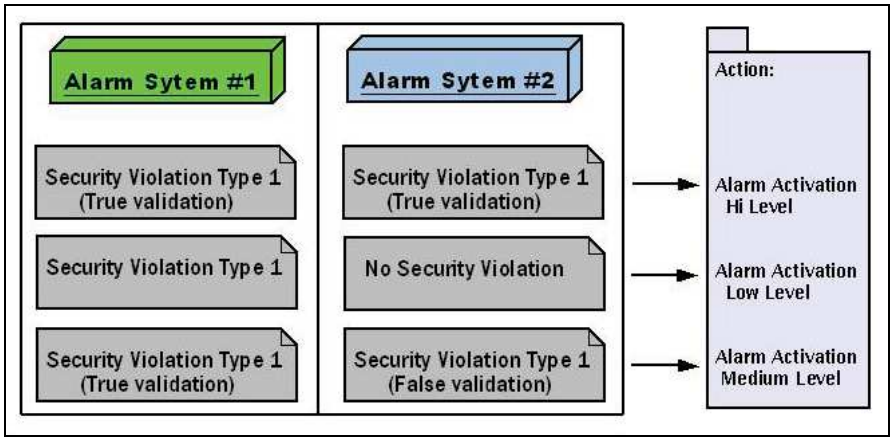

Fig. 8. Redundancy example

Theses capabilities could be programmed in a static, or if necessary, in a more dynamic way, reacting to pre-defined situations comprising all security strategy.

3.2.3 Connectivity Redundancy

IP protocol can be supported by different hardware technologies. These add an important advantage because it will allow several levels of redundancy between the intruder alarm systems that made the "grid".

In the lowest redundancy level each system can have two different types of connections. So, there are always two different ways for the system to communicate through the net. Redundancy gives in practice, to the system, two valuable functions:

1. In case of a connection failure due to a technical problem, the system stays connected to the net through another connection(s) according with the redundancy level used, and then it can monitor the failure;
2. In case of a failure due to a security violation produced on purpose, the system stays connected to the net as explained already, but it loses its security capabilities, monitoring the security violation.

The first example (in next figure), shows the intruder alarm systems connected through the network. Each system has a first level of redundancy, with two different available connections:

1. A connection by a dedicated cable structure;
2. A wireless GPRS connection.

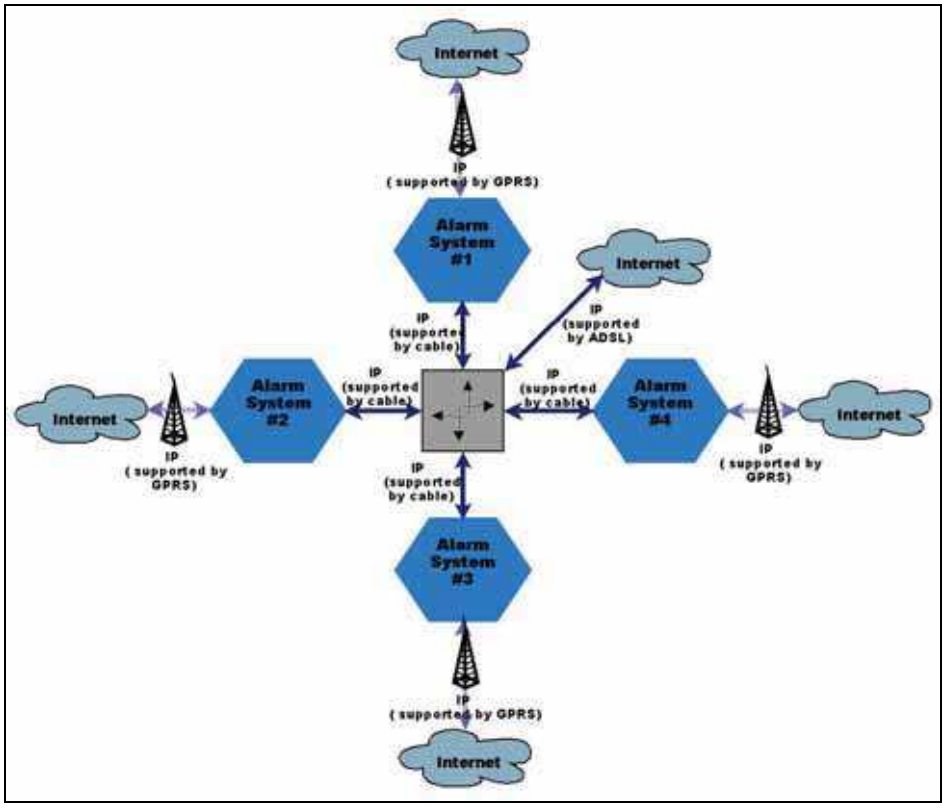

Fig. 9. Intruder alarm systems connected through the network (first configuration)

In this case, the alarm systems have fixed positions, and so the second wireless connection do not serve for mobility but rather for the ability that the system could maintain all its functions working, even when isolated by a security violation.
In the second example (figure 10) is also implemented a first redundancy level, with two connections to the net available:

1. A connection through ADSL supported on a conventional phone line cable, and without using a dedicated infrastructure;
2. Other connection (wireless) supported by GPRS.

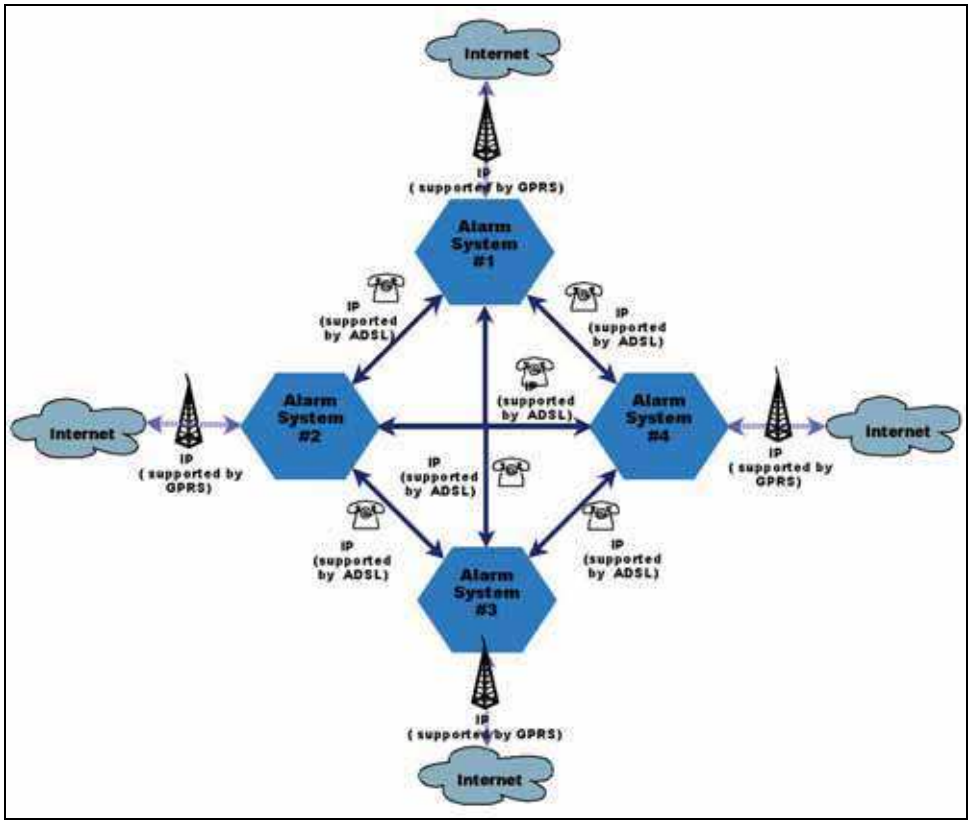

Fig. 10. Intruder alarm systems connected through the network (second configuration)

For this second configuration, using non dedicated structures, the implementation costs can be reduced, giving also more flexibility to the net topology:

- In the number of network nodes;
- Also concerning systems localization.

because the two used structures (ADSL with phone cable, and GPRS) are usually available at the urban (and other) environments.

3.2.4 Distributed Control

Intruder alarm distributed decentralized networks are indeed a new paradigm for the supervision and control of the security systems.

Each system (working as an individual node) has its own control, but also has the ability to monitor the state of the other alarm systems on the complete network. This way one can implement a global security alarm strategy, allowing the network to detect a certain failure, either by a technical failure or a security violation of one of the individual intruder alarm systems. On the other hand, it will be also possible, if necessary, to develop an high level network control, which can be done by any of the intruder alarm systems (node) of the network.

All these capabilities make alarm systems more robust, not only in terms of security but also in terms of supervision flexibility.

Security definitions can be adapted to each intruder alarm control system, for an individual security policy. These definitions can also be dynamically changed, following programming, or in reaction to possible contingence scenarios.

Being the network supported by a structure with Internet access, all monitoring and control, and programmer settings are reachable form any part of the globe (by using several internet access equipments, with different access privileges).

3.2.5 Web 2.0 Integration

Intruder alarm network systems work on a web-server basis, and new developments can now be achieved using web 2.0 integrated technologies.

An interesting intruder alarm systems application can de made by adopting integrated geo-localization (GPS). Figure 11 shows a geo-localization scenario. It is presented a possible application using a web 2.0 with Google Maps API., allowing the use of internet support maps:

Fig. 11. A geo-localization scenario with two different security levels

Fig. 12. Geo-localization scenario after a change of security levels

Two distinct security areas are defined (internal and external rectangle). Each intruder alarm system is one of the vertices (red marks) of the correspondent rectangle which is associated to one of the security areas.
Each type an intruder violation occurs, a special contingency state is automatically implemented, whereas specific actions are taken, with security levels dynamically changed for each protected area, as shown in figure 12.
A developed html code with JavaScript is presented in figure 13. In this sample code a security strategy was simplified for three different possible scenarios, in which, depending on the origin of the security violation, are signalized the edges of the two security areas, from a green level to the red level (the most severe), passing through a yellow level condition.
Without any intruder violation occurrence, the interior zone is at green alert and the exterior zone is at the yellow level (as shown in figure 11). If a violation is detected by any intruder alarm system located at the exterior area, the interior area will change to a yellow condition, and the exterior area to the red condition, as shown in figure 12.
In case of an intruder violation detected in the interior security area, both areas will immediately change to the red level condition.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="content-type" content="text/html; charset=utf-8" />
    <title>Google Maps JavaScript API Example</title>
    <script src="http://maps.google.com/maps?file=api&amp;v=2&amp;key=ABQIAAAAWurjbYaDZ-
    -</script>
    <script type="text/javascript">

    function load() {
      if (GBrowserIsCompatible()) {
        var map = new GMap2(document.getElementById("map"));
  map.addControl(new GSmallMapControl());
  map.addControl(new GMapTypeControl());

  var bounds = map.getBounds();
  var southWest = bounds.getSouthWest();
  var northEast = bounds.getNorthEast();
  var lngSpan = northEast.lng() - southWest.lng();
  var latSpan = northEast.lat() - southWest.lat();

  //get the 8 Alarm System position
  for (var ind = 0; ind < 8; ind++) {
        var point[ind] = new GLatLng(GPS_Lat[ind], GPS_Lng[ind])
      }

  // center the map
    map.setCenter(new GLatLng(GPS_Lat[2], GPS_Lng[3]), 17);

//  marker the 8 Alarm System
for (var ind = 0; ind < 8; ind++) {
    map.addOverlay(new GMarker(point[ind]);
    }
//get security status
S_level1=GetSLevel(point[0].point[1],ponit[2],point[3]); //internal rectangle.
S_level2=GetSLevel(point[4].point[5],ponit[6],point[7]);          // external rectangle

//security strategic

If (S_level1==0 && S_level2==0)
   {
  var polyline1 = new GPolyline([
    point[0],point[1],point[2],point[3],point[0], "#fff000", 6); //yellow level
  map.addOverlay(polyline1);

  var polyline2 = new GPolyline([
    point[4],point[5],point[6],point[7],point[4], "#00ff00", 6);  //green level
  map.addOverlay(polyline2);
    }

If (S_level1==0 && S_level2==1)
   {
  var polyline1 = new GPolyline([
   point[0],point[1],point[2],point[3],point[0], "#ff0000", 6); //red level
  map.addOverlay(polyline1);

  var polyline2 = new GPolyline([
    point[4],point[5],point[6],point[7],point[4], "#fff000", 6); //yellow level
  map.addOverlay(polyline2);
    }

If (S_level1==1 && S_level2==1)
   {
  var polyline1 = new GPolyline([
    point[0],point[1],point[2],point[3],point[0], "#ff0000", 6); //red level
  map.addOverlay(polyline1);

  var polyline2 = new GPolyline([
    point[4],point[5],point[6],point[7],point[4], "#ff0000", 6); //red level
  map.addOverlay(polyline2);
    }


  }
    }
    //]]>
    </script>
  </head>
  <body onload="load()" onunload="GUnload()">
    <div id="map" style="width: 500px; height: 300px"></div>
  </body>
</html>
```

Fig. 13. Sample code for web 2.0

4. Conclusion

Intruder Security is a billion dollar Industry, and a growing world wide market. The mobile and IP communications have developed and completely changed the way we now use, monitor and control intruder security systems.
The development of web-based intruder alarm systems from the evolution of the new APIs, and from the new languages based on the web 2.0 philosophy are now giving better ways and tools to design intruder alarm systems and to increase security - the road ahead to follow.

5. References

Antunes, R. (2007). Intruder Alarm Systems: The State of the Art, Proceedings of the 2nd International Conference on Electrical Engineering (CEE'07), pp. 252-261, ISBN:978-972-99064-4-2, Portugal, November 2007, Coimbra

Antunes, R. (2007). Manual do Curso de Formação de Projecto e Instalação de Sistemas de Alarme, ESTSetúbal

Adão, H.; Antunes, R.; Grilo, F. (2008). Web-Based Control & Notification for Home Automation Alarm Systems, Proceedings of the XXVII World Academy of Science, Engineering and Technology Conference (ICAR'08), International Conference on Automation and Robotics, pp. 152-156, ISSN:1307-6884, Egypt, February 2008, WASET, Cairo

Adão, H.; Antunes, R.; Grilo, F. (2008). Web-Based Control & Notification for Home Automation Alarm Systems, International Journal of Electronics, Circuits and Systems, Vol.2, No.1, 2008, pp. 20-24, ISSN:2070-3988

Grilo, F.; Figueiredo, J. (2008). An Industrial Vision System for Quality Control Based on a Distributed Strategy, Proceedings of the 8th Portuguese Conference on Automatic Control CONTROLO2008, pp. 426-431, ISBN: 978-972-669-877-7, Portugal, July 2008, Vila Real

Google Maps API Developer's Guide in
http://code.google.com/intl/pt-PT/apis/maps/documentation/index.html

Google Maps API Reference in
http://code.google.com/intl/pt-PT/apis/maps/documentation/reference.html

Advanced Technologies

Edited by Kankesu Jayanthakumaran

ISBN 978-953-307-009-4
Hard cover, 698 pages
Publisher InTech
Published online 01, October, 2009
Published in print edition October, 2009

This book, edited by the Intech committee, combines several hotly debated topics in science, engineering, medicine, information technology, environment, economics and management, and provides a scholarly contribution to its further development. In view of the topical importance of, and the great emphasis placed by the emerging needs of the changing world, it was decided to have this special book publication comprise thirty six chapters which focus on multi-disciplinary and inter-disciplinary topics. The inter-disciplinary works were limited in their capacity so a more coherent and constructive alternative was needed. Our expectation is that this book will help fill this gap because it has crossed the disciplinary divide to incorporate contributions from scientists and other specialists. The Intech committee hopes that its book chapters, journal articles, and other activities will help increase knowledge across disciplines and around the world. To that end the committee invites readers to contribute ideas on how best this objective could be accomplished.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Rui Manuel Antunes and Frederico Lapa Grilo (2009). Intruder Alarm Systems - The Road Ahead, Advanced Technologies, Kankesu Jayanthakumaran (Ed.), ISBN: 978-953-307-009-4, InTech, Available from: http://www.intechopen.com/books/advanced-technologies/intruder-alarm-systems-the-road-ahead

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821