Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.417 – 424

RESEARCH ARTICLE

Arduino Based Wireless Intrusion Detection Using IR Sensor and GSM

Prakash Kumar[1], Pradeep Kumar[2]
[1]Final Year, M.Tech (CSE), NIET, MTU, Noida, India
[2]Assistant Professor, Dept. of CSE, NIET, Greater Noida, India

Abstract— Intrusion detection systems (IDS) strive to catch computer system intrusion & utilize by any garnering and analyzing data. Wireless IDS$_s$ garner all local wireless transmissions and generate alerts based either on predefined signatures or on anomalies in the traffic. These wireless IDS can monitor and analyze user and system activities of known attacks, identity abnormal network activity and detect policy violations. Intrusion detection systems (IDSs) should be designed to facilitate the detection of attempted and actual unauthorized entry into designated areas and should complement the security response by providing the security force with prompt notification of the detected activity from which an assessment can be made and a response initiated. We intended to avoid the access and keep track of the intruder's attempts and intensions. A clear and emerging new channel in the space of banking and payments is mobile. A key challenge with gaming user adopting of mobile banking and payment is the customer's lack of confidence in security of the services. The economic growth in wireless network faults, vulnerabilities and attacks make the wireless local area network (WLAN) security management a challenging research area. Deficiencies of security methods like cryptography (WEP) and firewalls, causes the uses of more complex security systems.

Key Terms: - Wireless Intrusion Detection System (WIDS); Global system for mobile communication (GSM); Radio Frequency (RF); Success point; sensor; Arduino; WEP; C2DM

I. INTRODUCTION

Wireless local area networks (WLAN's) have proliferated around the globe and are used in industry, in government, and at home. The benefits of mobility that are provided by wireless local area networks are well known. However, there is also some risk involved. There are many security threats that are unique to the wireless networking environment since it uses an open, uncontrolled transmission medium. A wireless intrusion detection system can help to mitigate the risks involved with wireless networking and provide a more secure operating environment for a WLAN.

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. The biggest concern with wireless, however, has been security. Along with improved encryption schemes, a new solution to help combat this problem is the Wireless Intrusion Detection System (WIDS). In the security and wireless world this has fast become a major part of securing a network. [1]

The GSM was initially designed for voice; it can be used to serve other purposes than talking. This idea is reinforced by the fact that the GSM infrastructure has been deployed in many countries. GSM can be used as the communication via to receive signals captured by machines in remote places, and also to send control signals to remote machines. The installation of long wires to reach remote places (i.e. bridges, vending machines, etc.) is more expensive than the use of a mobile network that can perform the same task. Of course suitable sensors and actuators are needed for the mentioned examples and others. Some automatic GSM module is also needed, but long wired installation is not necessary.[3]

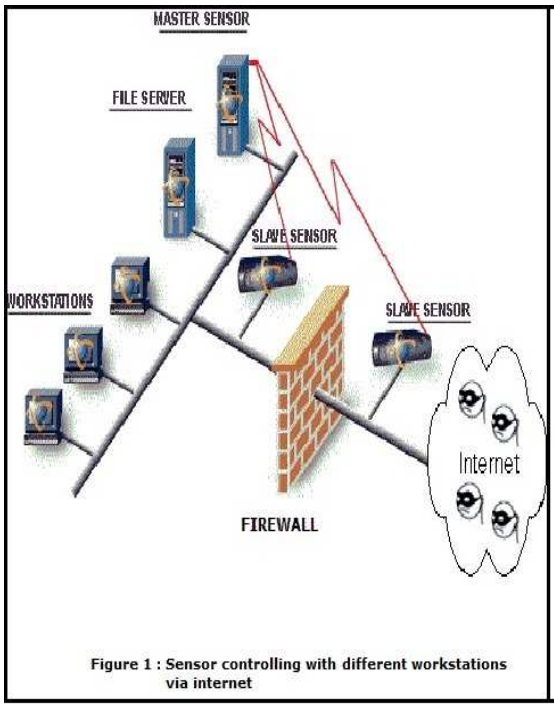


Figure 1 : Sensor controlling with different workstations via internet

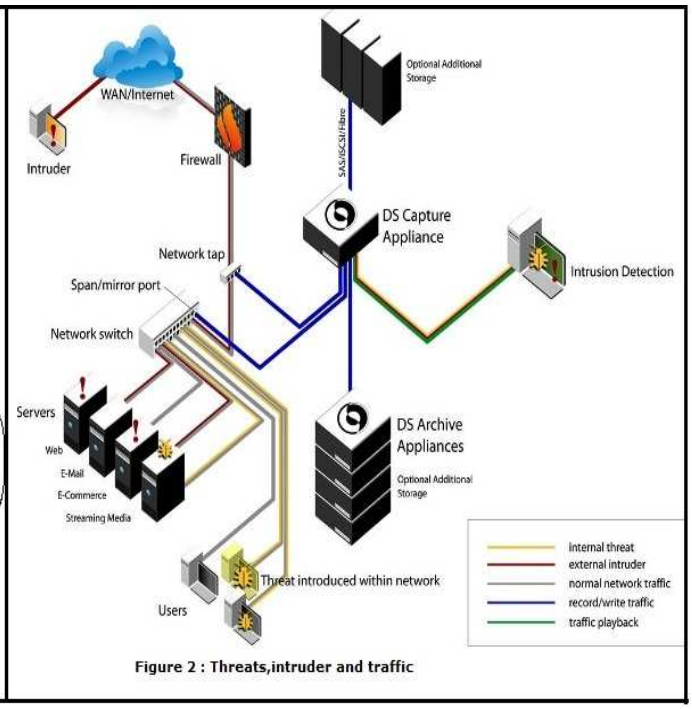


Figure 2 : Threats,intruder and traffic

What is an Intrusion Detection System?

An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network. A wireless IDS performs this task exclusively for the wireless network through sensor controlling with different workstations via internet (shown in Figure 1). These systems monitor traffic on your network looking for and logging threats and alerting personnel to respond (shown in Figure 2).[1]

A wireless IDS performs this task exclusively for the wireless network. These systems monitor traffic on your network looking for and logging threats and alerting personnel to respond. An IDS usually performs this task in one of two ways, with either signature-based or anomaly based detection. Almost every IDS today is at least in part signature-based. Attacks and their tools usually have a unique signature that can be detected and/or found. This means that known attacks can be detected by looking for these signatures. The downside to these is that they are easy to fool and can only detect attacks for which it has a signature. These are not often implemented, mostly because of the high amount of false alarms. An anomaly-based system develops a baseline of what it considers normal traffic. Any time it detects traffic which deviates from what it considers normal an alert is generated. The advantage is that it can catch many attacks that are new or unknown and that would never be seen by signature-based IDS. The drawbacks consist mainly of large amounts of time being spent to train and retrain the IDS system, as well as the large amount of false alerts that have to be examined. **[2]**

Why use a Wireless Intrusion Detection System?

The traditional wired IDS is a great system, but unfortunately it does little for the wireless world. The problem with wireless is that in addition to attacks that may be performed on a wired network, the medium itself has to be protected. To do this there are many measures which can be taken, however there are even more tools designed to break them. Due to the nature of wireless LANs (WLAN), it can be difficult to control the areas of access. Often the range of a wireless network reaches outside the physical boundaries of an organization. This creates limited control because it means an attacker can now sit in a car a mile away while he attempts to penetrate your network. With such a problem with wireless security, developing and implementing WIDS systems is definitely a step in the right direction. If you have wireless and are concerned about attacks and intruders, a WIDS may be a great idea. A large number of possible attacks can be detected by a WIDS. The following will list major attacks and events that can be detected with the help of a WIDS.

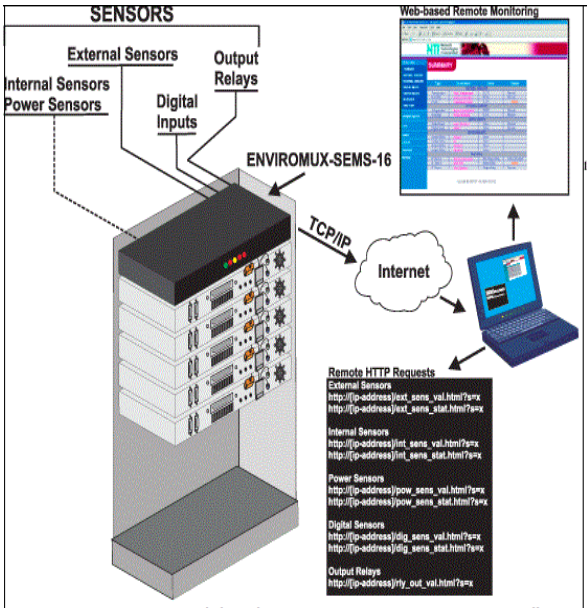


Figure 3 : Web-based remote monitoring using sensor controlling

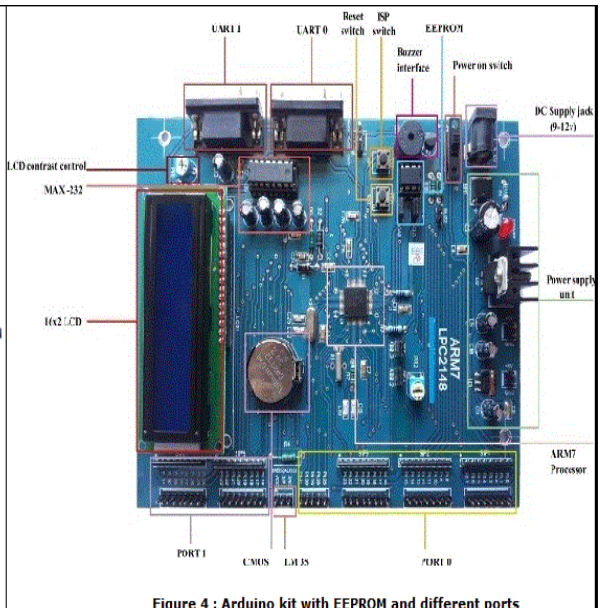


Figure 4 : Arduino kit with EEPROM and different ports

WIRELESS SENSOR NETWORK (WSN):

WSN is a kind of network, which includes many smart devices, called sensor nodes plus one or several sinks, randomly deployed in a wide area. These nodes are spatially distributed in order to perform an application-oriented global task. The basic component of the network is the sensor. It is necessary for measuring real world physical conditions or variables such as humidity, pressure, temperature, vibration, pollutants, sound, motion, and intensity. These tiny devices within the network are smart and inexpensive and responsible for web-based remote monitoring using sensor controlling (shown in Figure 3). Such properties make them to cover large areas of any geometry and one of the most important design and implementation requirements of a typical sensor network is energy efficiency. [7].

II. HARDWARE DESIGN AND INTERFACING

Arduino is an open-source physical computing platform based on a simple I/O board, and a development environment for writing Arduino software. Arduino can be used to develop interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other outputs. Arduino projects can be stand-alone, or they can communicate with software running on your computer (e.g. Flash, Processing, MaxMSP).

Why using Arduino?

It is flexible, offers a variety of digital and analog inputs, SPI and serial interface and digital and PWM outputs. It is easy to use, connects to computer via USB and communicates using standard serial protocol, runs in standalone mode and as interface connected to PC/Macintosh computers

It is inexpensive, around $30 per board and comes with free authoring software. It is an open-source project, software/hardware is extremely accessible and very flexible to be customized and extended. Arduino is backed up by a growing online community; lots of sources are already available.

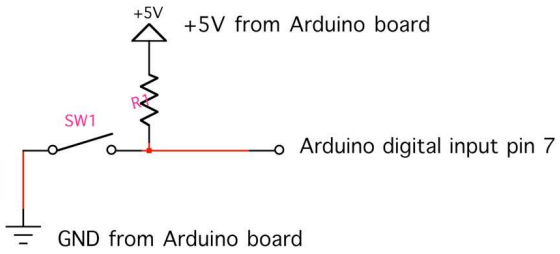
Arduino interfacing with Softwares:

The Arduino can "talk", (transmit or receive data) via a serial channel, so any other device with serial capabilities can communicate with an Arduino. It doesn't matter what program/programming language is driving the other device. You can either use the Arduino's "main" serial port, the one it uses when you "talk" to it to program it, or you can leave that channel dedicated to programming (and the development environment's serial monitor), and use two other pins for an extra serial link dedicated to the external device. Some programs (like Flash) don't have native serial capabilities. They can still communicate with Arduino through an intermediary which, like a "translator", enables them to talk to each other.

Connecting a Switch to the Arduino Board

This is probably the simplest possible example to get started with Arduino. It uses an external switch and the Arduino board to turn ON or OFF the on-board LED.

1. Connect a switch (you can replace the switch with a plain jumper wire) to the Arduino board in the following way:



R1 = 10kΩ
SW1 can be any type of push button switch or just a wire

Why do we need the resistor R1? R1 guarantees that the Arduino's digital input pin 7 is connected to a constant voltage of +5V whenever the push button is not pressed. If the push button is pressed, the signal on pin 7 drops to ground (GND), at the same time the Arduino's +5V power is connected to GND, we avoid a shorted circuit by limiting the current that can flow from +5V to GND with a resistor (1 - 10 KΩ). Also, if there was no connection from pin 7 to +5V at all, the input pin would be "floating" whenever the pushbutton is not pressed. This means that it is connected neither to GND nor to +5V, picking up electrostatic noise leading to a false triggering of the input. [5]

Sensor

Sensors are electronic devices that measure a physical quality such as light or temperature and convert it to a voltage. This process of changing one form of energy into another is called transduction. Often, sensors are also referred to as transducers. Sensors can be broadly classified in two categories: digital sensors and analog sensors. A digital sensor's output can only be in one of two possible states. It is either ON (1) often +5V, or OFF (0), 0V. Most digital sensors work with a threshold. Is the incoming measurement below the threshold, the sensor will output one state, is it above the threshold, the sensor will output the other state. In contrast to a digital sensor, an analog sensor's output can assume any possible value in a given range. Very often the output of an analog sensor is a variable resistance that can be used to control a voltage. Rather than only being able to toggle between two states and the analog sensor can output an almost infinite range of values. In the following examples we will take a look at a couple of digital and analog sensors. We will begin with the simplest digital sensor, the switch. When a switch is open, no current flows. In contrast, when a switch is closed, current flows (i.e. closed = ON). A switch that stays in the position it was put is called a latching switch. Switches can be spring loaded (e.g. micro switches/snap action switches), in this case they are called momentary. A simple switch can be Normally Open (NO) or Normally Closed (NC).

Microcontroller

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. [9].

III. PROPOSED METHODOLOGY

Human intrusion can be detected using many sensor modalities. Six types of sensors are included and all of these are passive in the sense that, unlike radar or ultrasonic sensors, they do not emit a signal and see how targets modify it. Passive sensors are preferred in sensor networks where there is limited energy. Magnetic sensors assume that the intruder, such as an armed person, has magnetically sensitive material. Ferromagnetic material creates a specific magnetic signature that can be detected using a magnetometer. Any metallic content worn by the intruder can be detected using electromagnetic techniques. Seismic and acoustic sensors are based on the vibrations caused by the intruder. Both come under the general category of vibration sensors which we describe next in some detail as a preamble to our prototyping effort. Vibration-based surveillance sensors can be

classified into two major groups, namely, acoustic sensors and motion sensors. Acoustic sensors measure the sound produced by the entity that is to be detected or monitored. In the case of vehicles, the main sources of sound are engine and power-train noise, track/tyre noise and exhaust noise. Footsteps of humans and animals, fluttering of wings by birds, etc., also generate sound in addition to the entity's vocal sound. Sensors that measure sound are essentially microphones and hydrophones. On the other hand, vibratory motion sensors sense displacement, velocity and acceleration using seismometers/ geophones, velometers and accelerometers, respectively. The physical construction of both classes of sensors is almost the same: they contain a spring-restrained mass which inevitably will have some damping. However, the frequency, range of operation and resolution of these sensors will be significantly different. Their cost also varies depending on their level of sophistication. [6]

Embedded system is not a new concept. Embedded systems has become a buzz word in the last fifteen years, but embedded systems and processors have been around for much longer than that. Some of the embedded systems are now commonly interfaced with Bluetooth and GSM (Global System for Mobile communication) modules to widen their scope and enhance the application areas to a greater extent. Although the GSM was initially designed for voice, it can be used to serve other purposes than talking. This idea is reinforced by the fact that the GSM infrastructure has been deployed in many countries. GSM can be used as the communication via to receive signals captured by machines in remote places, and also to send control signals to remote machines. The installation of long wires to reach remote places (i.e. bridges, vending machines, etc.) is more expensive than the use of a mobile network that can perform the same task. Of course suitable sensors and actuators are needed for the mentioned examples and others. Some automatic GSM module is also needed, but long wired installation is not necessary. Furthermore, mobile telephone can also be used in remote systems, but in moving systems as well, such as vehicles and people. Also Bluetooth is a popular mechanism for short distance point to point or point to multi-point communication. The features include low cost, low power and small size. Also the robustness for the interferences has made Bluetooth a highly versatile and attractive technology among other short range wireless technologies. The current sensor will send an analog signal to the microcontroller when the car is running. The microcontroller will send SMS directly to the owner. [11]

To further enhance this idea, I have planned to interface the mobile technology with electronics. That is, through this application, we target to control the secured zones by turning ON/OFF the human motion IR sensors along with knowing about any movement that happens in the periphery of the sensor. The application of this idea can be very well assumed in the situations that are highly secured and in which in addition to manual security, electronic and mobile security measures are also required. These places could be large banks, cash chests, criminal jails, nuclear installations, secret and highly confidential research areas etc. In order to develop this application, we also plan to make the use of Google C2DM service which will empower us to connect to the IR sensor device, at all times. The mobile application will connect to an electronic chip to which an IR sensor will be connected. The mode of connection will be GPRS which we have planned to use. This project will have two parts namely: Mobile Part and Electronic Part. The mobile part will have an interface through which we would be able to turn ON/OFF the infrared sensor (IR) remotely from any part of the world. In addition, the sensor will also communicate any human or infrared intrusion around it through GPRS and this indication will be displayed on the mobile handset through a flash message pop-up. If we use Java-enabled handsets, the J2ME application will have to be started for that message to be displayed but if we are using an Android Smartphone, the application can run in the background and the pop-up message will be displayed without explicitly starting the application. The electronics part will consist of a chip to which an IR sensor will be connected. We have planned to use GPRS as the medium of information exchange. Once the user presses ON button on the mobile handset, the IR sensor will turn ON or enable. Otherwise, if the user presses OFF, the sensor will go off and be disabled. This communication will occur through mounting a shield on the chip which will enable it to obtain an IP that would eventually help the connection between chip & mobile.

Planned to program the chip in C/C++ and it will communicate with the mobile application that will be developed in J2ME. This application would be a culmination of two very different technologies which will make it unique & strong as a whole. Objective behind developing this application is to control the security equipments remotely so that any unauthorized or illegal movement is immediately and effectively detected. This concept is also very prominently used in home security systems, surveillance systems etc. There would be four parts: Electronics Part, Web Part, Mobile Part, and Google C2DM Part.

1. Electronics Part: This module would consist of a small electronic board name *Arduino* that we would program in C. In addition to many other components, this board consists of a programmable microcontroller, EEPROM, Flash Memory etc. On the top of this (base) board, we would be mounting an Ethernet shield which would give us the freedom to connect it to a system which would act as the remote server in our project. We assume that the remote server would be in an ON state always and connected to internet. Once the electronic board is connected to the remote server, it will receive an IP which our mobile application would be using. We would also connect an IR sensor to this board which can be turned ON/OFF by the mobile application. This

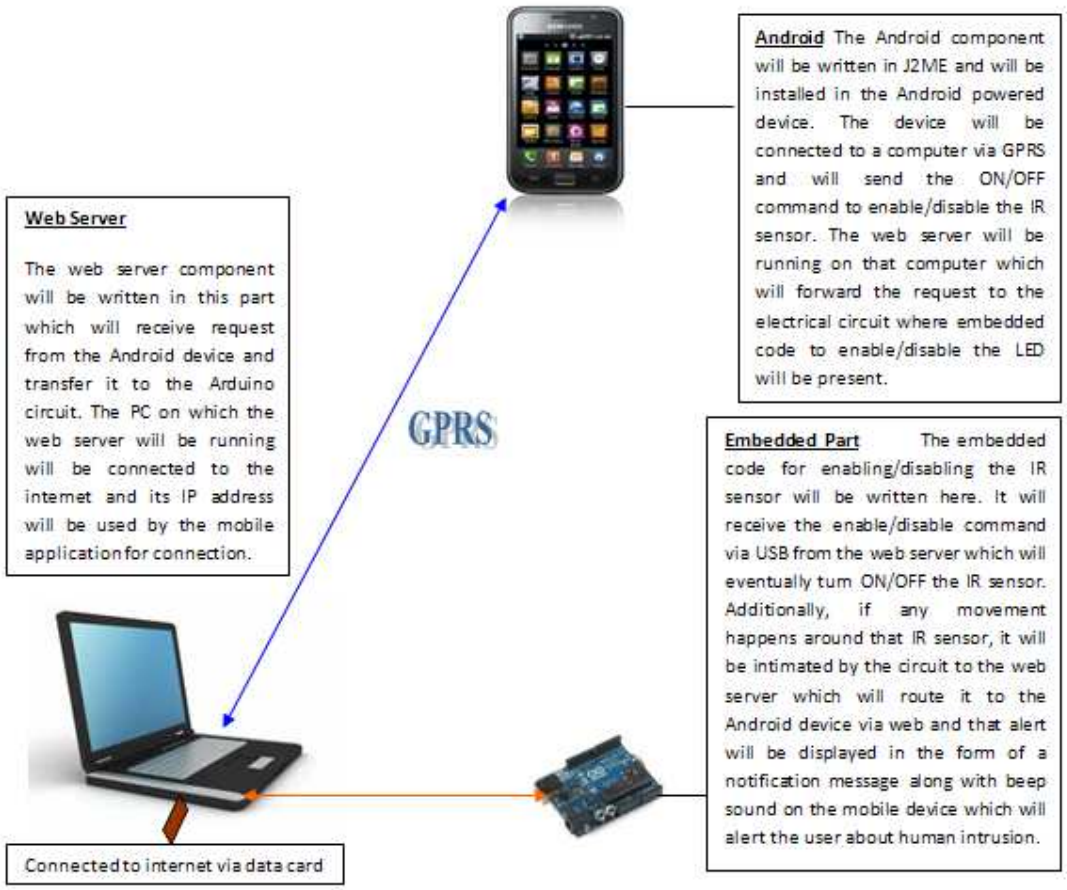
sensor will also sense the movement and signal about it via GPRS to the mobile part which will display a corresponding pop-up (flash) message.

2. Web Part: This module would be running at the remote web server end to which the electronic board would be connected via LAN/Ethernet cable. This module would be mainly responsible for processing operations from the electronic board and the commands being received from the remote mobile handset via GPRS. That is, when the remote mobile handset sends any signal via GPRS to the remote server which is connected to the internet, it will send appropriate instructions or signals to the electronic board\Arduino for switching ON/OFF the R sensor connected to the board. That is, whatever command the user will give through the mobile application will be appropriately converted to the signal and transmitted to the electronic board. The web module would be developed in J2EE involving JSP, Servlets etc. This module would not be accepting any user input but would mainly act as the processing stub.

3. Mobile Part: This part would be the actual application that will be developed on J2ME for Android or normal Java enabled platform. Once this application is developed, its corresponding .jar file would be transferred from the system to the Android mobile device for installation. Once the application is installed, its mobile user interface will give the user 2 basic options to control the IR sensor device i.e. ON & OFF. Once the user pushes the ON button on the mobile user interface, the command will travel via GPRS to the IP of the remote server where the web part is configured. Additionally, when there is any intrusion detected near or around the IR sensor, it will be communicated by the electronic chip via GPRS to the mobile application which will indicate same on the handset through a pop-up message like *Warning! An intrusion has been detected.*

4. Google C2DM Part: Under this module, we shall register our Google device / handset as well as the web server with the Google's C2DM service. C2DM service essentially means Cloud to Device Messaging through which Google keeps a track of the devices and initiates a server push when the device sends any signal. We need to register both the device as well as server with C2DM so that Google has the knowledge from where are the signal notifications coming and on which device does it need to perform the server push. We will program the mobile application in such a manner that it points only to the IP of the remote server and when the command is send from the mobile application, only the remote web server should attend & process it. Furthermore, we also assume that the mobile device would be GPRS enabled so that it connects to the internet and use that medium to connect to the remote server from virtually any location, irrespective of the geographical coordinates. Once the mobile command is received by the remote server, it will convert it to the appropriate electrical signals and send it to the board. In the board, we already have a running, embedded C program which will understand those signals and will switch ON/OFF the sensor as desired and selected by the user from his/her mobile application.

IV. DIAGRAMMATIC REPRESENTATION



V. ALGORITHM COMPARISON

1. Classification: Due to the large number of nodes in sensor network, flat protocols employ data centric method that helps in omitting a large amount of redundant data transmissions. Hierarchical protocols try to save energy through clustering the sensors. In this way, data gathering and reduction will be done by cluster heads.

2. QoS algorithms: Should guarantee some network metrics such as lifetime and latency. Geographic protocols use the location information to forward the data to the desired regions rather than the whole sensor field.

3. Multi-path: By using multiple paths from the source to the destination, traffic load could be distributed through the network uniformly. It can prevent network partitioning and prolong network lifetime. Moreover, at the time of link failure another route will be used by the source node. In this manner, the end-to-end delay could be reduced for each packet.

4. Route Disjointness: An important property for multi-path mechanisms is disjointness. Link or node disjoint algorithms try avoiding interference between multiple routes and prevent packet retransmission caused by collision. Node-disjoint strategies have much better performance than link-disjoint multi-path schemes. The reason is that they are congestion avoided. Meshed protocols cannot guarantee the Link or node disjointness among the multiple paths [7].

VI. RELATED WORK

Automobile industry and automobile market is in a high speed development state for several years. Automobile's appearance impacts and changes people's life, it's becoming the progressive symbol of modern society. At present, in the leading market of the automobile anti-theft production is CMOS chip production. GPS positioning system is also used, or combine the CMOS chip and GPS positioning system. However, chip anti-theft production is with a low security and small alarm scope, which can't be found after lost yet. Although GPS can used to retrieve automobile, what make user flinch is the high cost. Use GSM network can work out an

anti-theft system with low cost, large alarm scope, strong Anti-jamming capability, which even be able to verify approximate positioning in a certain scope. The automobile theft-proof system based on GSM communication network designed in this paper be able to accomplish short message services(SMS) like homogeneous anti-theft system, moreover, speed sensor and vibrating sensor are combined to realize dual theft-proof of automobile. The fortified vehicular security is advanced greatly, and the cost of the automobile's orient is reduced [8].

VII. FUTURE SCOPE

In the paper low cost, secure, ubiquitously accessible, auto-configurable, remotely controlled solution for automation of homes has been introduced. The approach discussed in the paper is novel and has achieved the target to control home appliances remotely using the notification-based system satisfying user needs and requirements. In future the system will be small box combining the PC and GSM modem including the GCM feature for both mobile device and the hardware device.

VIII. CONCLUSION

Prevent any unauthorized human intrusion in the data centre, the organization is of the opinion that during working hours, the authorized employees will access the centre through their employee id card whereas, during the off-office hours, the motion sensors which will be installed in the data centre will be turned ON and activated. . While the organization plans to install the motion sensors, it also requires an effective way through which the response time or action times during the event of an illegal access could be improved, when the motion sensor detects and informs about the intrusion. Giving the power to control the sensors to more than one person would again have been a breach of security guidelines. Hence, in order to suppress the disadvantages and dangers associated with the manual controlling of the human motion detection sensors like, the person did not reach the place, when the person was controlling the sensors, he damaged them etc. the company decided to control them automatically via GPRS wherein a designated authorized personnel could turn ON/OFF the sensors easily from any place, wirelessly, using GPRS thereby securing the security aspects related to dealing and controlling with the motion sensors manually. As Intrusion detection and assessment systems are an integral part of any physical protection system. Detection and assessment provide a basis for the initiation of an effective security response. Intrusion detection systems (IDSs) should be designed to facilitate the detection of attempted and actual unauthorized entry into designated areas and provide the related intrusion notification to the particular owner's smart device. The method(s) of detection and assessment selected for implementation should be robust and be capable of providing the highest level of protection for the specific application.

REFERENCES

[1] Snehal Boob,Priyanka Jadhav,"Wireless Intrusion Detection System", International Journal of Computer Applications(0975-8887),Vol. 5,no. 8,August 2010,pp. 1-5.
[2] Jeff Dixon, "Wireless Intrusion Detection Systems", http://www.infosecwriters.com/text-resources/pdf/wireless_IDS_JDixon.pdf.
[3] Vini Madan,S.R.N. Reddy, "GSM-Bluetooth based Remote Monitoring and Control System with automatic Light Controller", International Journal of Computer applications(0975-8887),Vol. 46,no. 1,May 2012.
[4] P.M. Lange, K.L.G. Nielsen, "Phase recognition in an operating room using sensor technology", IT-university of Copenhagen, Feb 2010.
[5] Fabian Winkler,"Arduino workshop", spring 2007,http://www.arduino.cc.
[6] The Smart Detect Project Team, "Wireless Sensor networks for Human Intruder Detection", Indian institute of Science,Bangalore,India,May 2010.
[7] M.R. Eslaminejad, M. Sookhak, S.A. Razak,"A Review of Routing Mechanisms in Wireless Sensor Networks", International Journal of Computer Science and Telecommunication, Vol. 2, no. 7, October 2011.
[8] Lili Wan, Tiejun Chen,"Automobile Antitheft System Design based on GSM", International Conference on Advanced Computer Control, Jan 2009, pp 551-554.
[9] Jayanta Kumar Pandey, R.N. Das choudhary,"Embedded Automobile Engine locking System, using GSM technology", ITER, SOA University Odisha, India.
[10] Indian Institute of Science, "Wireless Sensor Networks for Human Intruder Detection", Journal of the Indian Institute of Science,Vol. 90,no. 3,Jul-Sep 2010.
[11] M.N. Ramadan, MD. Al-Khedhar,"Intelligent Anti-theft and Tracking System for Automobiles", International Journal of Machine Learning and Computing, Vol. 2, no. 1, Feb. 2012.

