A NOVEL INTRUSION DETECTION SYSTEM USING WIRELESS SENSOR NETWORKS

Durgadevi G
Department of Electronics and Communication Engineering, New Prince Shri Bhavani College of Engineering and Technology, Chennai, India.
Durgadevi.karthik@gmail.com

ABSTRACT: T **In this paper an novel intrusion detection using wireless sensor network is developed. A wireless network system for detecting the intrusions which may be caused in highly protected zones. This paper provides security for military storage room for weapons, confidential question papers and electronic voting machines. And this is done using a wireless network based security and monitoring system that includes WPAN, RF signal strength, MEMS motion sensors and GSM technology. By using star topology one coordinator node and 'n' slave nodes are connected to form a network. The coordinator node broadcasts a beacon that enquires the status of all slave units. Any disturbance to a slave unit in all three dimensions can be sensed via MEMS sensors and this information will be transmitted to the coordinator unit which will transfer the details via SMS to respective higher authority. When an intrusion occurs, there will be variation in propagation environment. Thus the received RF signals strength changes. The coordinator node is able to recognize this RSSI change and alert through SMS. This type of security offers complete protection for an entire storage room even if it contains hundreds of slave units. All data packets adhere to IEEE 802.15.4 frame format and each node has a transceiver circuitry to handle the packet transmission and reception. All slave units have a low power microcontroller which runs the security algorithm operating via battery power and the coordinator node runs from the main power.**

KEYWORDS: **MEMS, GSM, Intrusion detection, WSN, Military.**

I. INTRODUCTION

GSM is a wireless communication technology; most popular today for transmitting data anywhere in the world through SMS with the help of mobile phones [13]. SMS is a globally accepted wireless service that enables the transmission of alphanumeric messages between mobile subscribers and external systems such as electronic mail, paging, and voice-mail systems. It is a store and forward way of transmitting messages to and from mobiles [14]. A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Formed by hundreds or thousands of motes that communicate with each other and pass data along from one to another. They are decentralized and distributed in nature where communication takes place via multihop intermediate nodes. The main objective of a sensor node is to collect information from its surrounding environment and transmit it to the sink. WSNs have many applications and are used in scenarios such as detecting climate changed, monitoring environments and habitats, and various other surveillance and military applications.

Mostly sensor nodes are used in such areas where wired networks are impossible to be deployed. WSNs are deployed in physical harsh and hostile environments where nodes are always exposed to physical security risks damages. Furthermore, self-organizing nature, low battery power supply, limited bandwidth support, distributed operations using open wireless medium, multihop traffic forwarding, and dependency on other nodes are such characteristics of sensor networks that expose it to many security attacks at all layers of the OSI model. In recent days, the number of theft attempt has been increased drastically in various confidential environments such as Military weapons storage room, Bank lockers, Jewellery shops, E-voting machine and also in Question paper storage room. There is the need for enhanced and reliable security. Previously manual scheduling, surveillance cameras [1][2] and PIR sensors [5] are used to provide a security but there is high probability of malpractice and false triggering. MEMS (Micro Electro Mechanical Systems) are key components in many automotive, industrial, medical, aerospace and consumer applications. MEMS sensors are used in anything from gaming, smartphones, medical testing to satellites. The applications seem unlimited. MEMS [6] are everywhere. The MEMS are already proven that they have very high efficiency and sensitivity [7][8][9].

II. RELATED WORK

Hariprakash R, Ananthi S, Padmanabhan K initiated an economical wireless monitored system using surveillance camera in [1]. Literature [2] gave solution for localizing and tracking by using the surveillance camera. A number of papers which has intrusion detection system designed using surveillance cameras [2][3] and [4]. The coverage problem is a crucial issue of wireless sensor networks, requiring specific solutions when video-based sensors are employed. Daniel G. Costa and Luiz Affonso Guedes [11] illustrated the issues caused by the usage of surveillance camera. Lutz K [6] stated the need for the less power consumption of sensor nodes. Shaby S.M. ; Juliet, A.V. literature about the performance analysis of MEMS sensors and also they validated it. The rest of the paper consists of methodology in section III, results and discussion in section IV and conclusion in section V.

III. METHODOLOGY

A. OVERVIEW

A typical wireless sensor network is shown in the figure 1 which shows the connection between sensor nodes and the network.

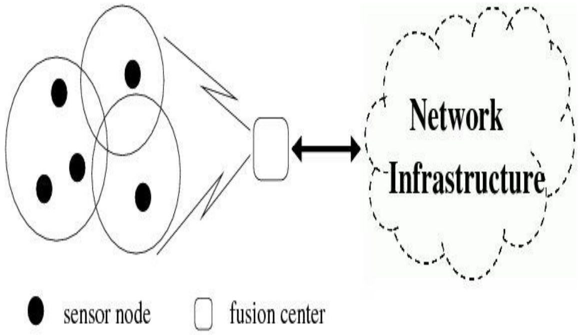
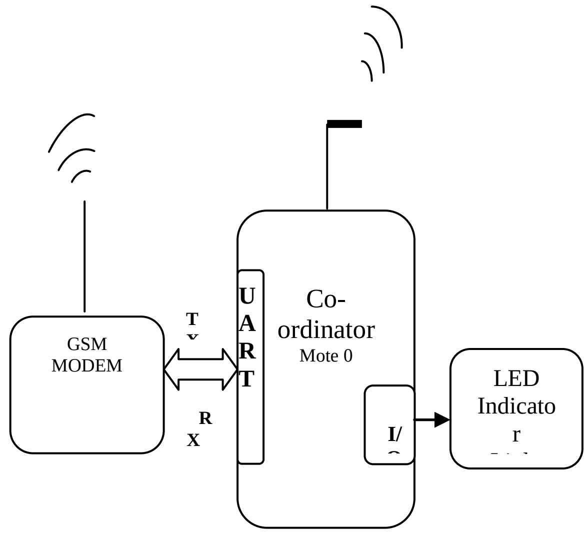
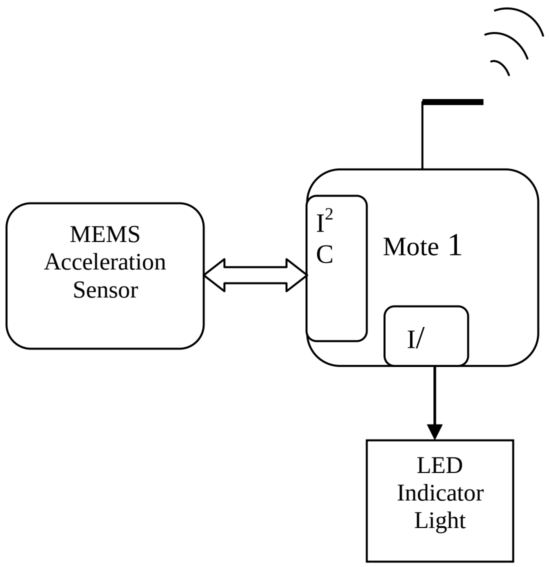


Fig. 1: A TYPICAL DIAGRAM OF A WSN

B. DESIGN AND DEVELOPMENT

The figure 2 shows the security system of the wireless sensor network. In Figure 2 block diagram consists of one Coordinator unit and two Slave units. Mote is defined as a sensor node in wireless sensor networks. The Coordinator mote broadcasts a beacon signal that enquires the status of all slave units. If any disturbance to a Slave units can be sensed in all three dimensions via MEMS sensors and this information will be transmitted to the coordinator unit which will send the details via SMS to respective higher authority.The wireless network based security and monitoring system consist of WPAN, RF signal strength, MEMS motion sensors and GSM technology. Mote consist of serial interface such as SPI, I2C, UART protocols. PIC microcontroller is interfaced with MEMS Acceleration sensor unit via I2C protocol and also interfaced with RF Transceiver IEEE802.15.4 via SPI protocol. Co-coordinator and GSM MODEM is interfaced with the help of general standard UART Protocol using MAX232 interface.





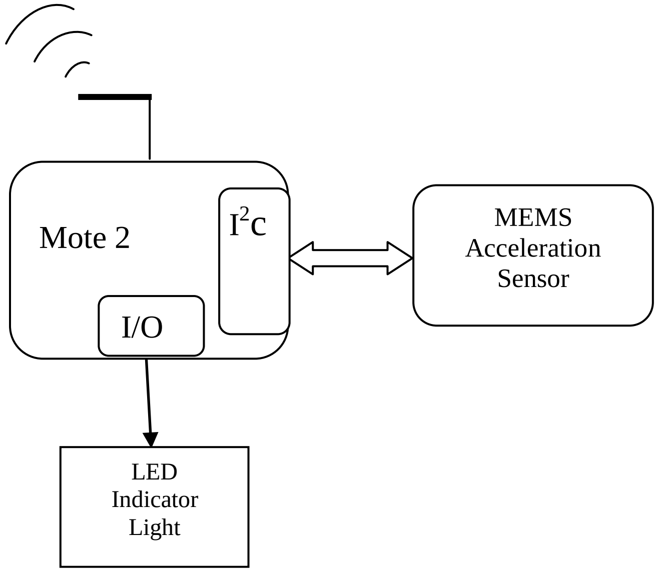


Fig. 2**: SECURITY SYSTEM**

LED indicates active state of slave and coordinator unit. The mote module is shown in fig.3. Mote is defined as sensor node in wireless sensor networks. It is a combination of Microcontroller and Transceiver. PIC18F45J11 microcontroller and MRF24J40MA Transceiver are used. Mote provides serial connection between PIC microcontroller and transceiver using SPI protocol. The I2C protocol is used to communicate between MEMS sensor and PIC microcontroller. IEEE 802.15.4 Transceiver has low Rate WPAN which is used to transmit and receive information from one mote to other mote with the help of on-chip omnidirectional antenna.

Frequency band used in transceiver is the ISM band 2.4GHz. This mote is a small device that consumes less power of 3.3v and can be fixed in multiple slave units across the entire room. A WSN-SCADA for the above said system SCADA system consists of a sensor which senses the information or the data and then that data is conditioned and sent to the analog to digital converter.

The converted data is given to the microcontroller for further processing. That data which is processed in the SCADA system will be finally given to the higher authority. In our paper we are using MEMS sensor in which the accuracy and the sensitivity is high when compared to the surveillance camera which is used earlier. The MEMS sensor checks whether there is any intrusion or not. If there is an intrusion sensor senses that intrusion and sends to the coordinator mote and that is information is given to the higher authority via SMS using GSM technique.

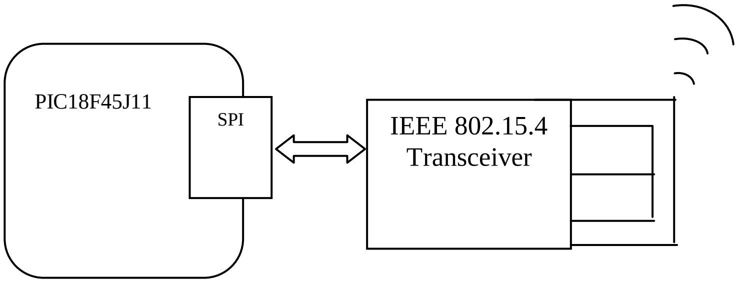


Fig. 3: MOTE MODULE

Transceiver

The Microchip MiWi P2P Wireless Protocol is a variation of IEEE 802.15.4, using Microchip's MRF24J40MA 2.4 GHz transceiver and any Microchip 8, 16 or 32-bit microcontroller with I2C. The protocol provides reliable direct wireless communication via an easy-to-use programming interface. It has a rich feature set that can be compiled in and out of the stack to meet a wide range of customer needs while minimizing the stack footprint.

Protocol Overview

The MiWi P2P protocol modifies the IEEE 802.15.4 specification's MAC layer by adding commands that simplify the handshaking process. It simplifies link disconnection and channel hopping by providing supplementary MAC commands. However, application-specific decisions, such as when to perform energy detect scan or when to jump channels, are not defined in the protocol. Those issues are left to the application developer.

Physical Layers

The MiWi P2P stack uses only a portion of the IEEE 802.15.4 specifications in PHYSICAL and MAC layers definitions. The specification defines three PHYSICAL layers, operating on a spectrum of 868 MHz, 915 MHz and 2.4 GHz. The MRF24J40MA radio operates on the 2.4 GHz, ISM band which is freely available. That spectrum has 16 available channels and a maximum packet length of 127 bytes, including a two-byte CRC value. The total bandwidth for the IEEE 802.15.4, 2.4 GHz ISM band is theoretically- 250 kbps. In reality for reliable communication, the bandwidth is 20-30 kbps.

Supported Topologies

IEEE 802.15.4 and the MiWi P2P Star and Peer-to-Peer topology. In both the topologies PAN coordinator initiates communication and accepts connections from other devices. PAN coordinator is a FFD with its radios on all the time and all the time and all other end devices are RFD with its radios off when it is idle.

Star Topology

A typical star topology is shown in Fig. 4 from a device role perspective, the topology has one PAN coordinator that initiates communications and accepts connections from other devices. It has several end devices that join the communication. End devices can establish connections only with the PAN coordinator. As to functionality type, the star topology's PAN coordinator is a

FFD. An end device can be an FFD with its radios on all the time, or a RFD with its radio off when it is Idle. Regardless of its functional type, end devices can only talk to the PAN coordinator. It is used to provide communication link between Master and Slave unit.

C. SYSTEM SPECIFICATION

1) Network Specification

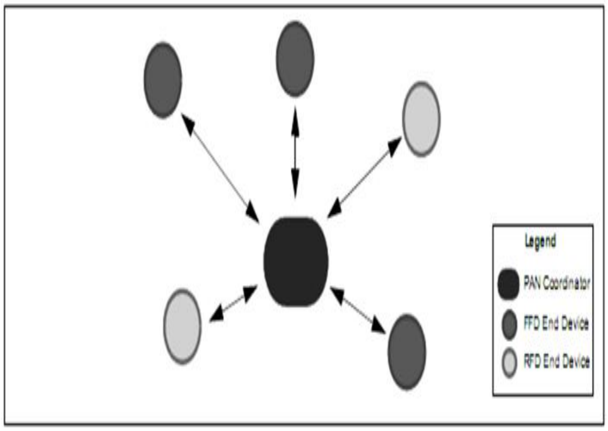


Fig. 4: STAR TOPOLOGY

Star Topology: Consists of a Coordinator as a centre processing unit functions. It gathers sensor readings from all End Devices.

2) Hardware Specification

Microcontroller

Here we use PIC18F24420 microcontroller which offers ten different oscillator options, allowing users a wide range of choices in developing application hardware. It has 5 I/O ports which can interface with the other devices such as I2C, SPI, digital and analog.

Sensor

The LIS302DL is an ultra-compact, low-power, digital output 3-axis linear accelerometer packaged in a LGA package. The complete device includes a sensing element and an IC interface able to take the information from the sensing element and to provide a signal to the external world through an I2C/SPI serial interface. It senses disturbance in three coordinate axes and the disturbance signal is transmitted to the master unit with the help of I2C interface.

Communication

GSM module is present in the coordinator node .when any disturbances occur to digital MEMS sensor or when the RSS reduces, transceiver sends the alert message to higher authority via SMS. The GSM makes use of narrowband TDMA technique for transmitting signals. It has an ability to carry 64 kbps to 120 Mbps of data rates. GSM digitizes and compresses data, then sends it down through a channel with two other streams of user data, each in its own time slot.

IV. RESULT AND DISCUSSION

Security has to be increase drastically in various confidential environments such as Military weapons storage room, Bank lockers, Jewellery shops, E-voting machine and also in Question paper storage rooms. Manual scheduling has been avoided and instead of using other sensors like

PIR, we used MEMS sensors which increased the level of security, malpractice and false alarms. In this project we used two slave units and one co-ordinator mote in which the slave units senses the information through the MEMS and transfer to the main mote. The intrusion is identified and this information is given to the higher authority through the SMS.

V. CONCLUSIONS

This paper highlights an efficient security system using wireless sensor network. Here we use the PIC18F24420 microcontroller and MEMS sensor. The theft in confidential places would be reduced to great extent on the implementation of this project. We would also like to suggest that the security system can be implemented in many places like military arm storage room, bank lockers, and jewellery shop and also in the room where the electronic voting machines will be kept before the counting is started. In future instead of using star topology peer to peer topology can be used and also the data collection capacity can be increased to some extent. And instead of using MEMS other kind of sensors can used and tested for their accuracy, sensitivity and efficiency. Even analog sensors can be added. Extensions of our current work include an extension from a star network to a mesh network which will be useful for deploying sensor networks in large areas like in buildings with multiple rooms and multiple floors.

VI. REFERENCES

[1] Hariprakash, R. ; Ananthi, S. ; Padmanabhan, K. “An economical wireless network monitored scheme for camera based intrusion detection at unattended sites” Computer Applications and Industrial Electronics (ICCAIE), 2011, IEEE International Conference Page(s): 150 - 155

[2] Sanchez-Matamoros, J.M. ; Dios, J.R.M.-d. ; Ollero, A. “Cooperative localization and tracking with a camera-based WSN“, Mechatronics, 2009. ICM 2009. IEEE International Conference, Page(s): 1 – 6

[3] Clinton Administration (ed.): The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. Washington D.C., 1998.

[4] Denning, Dorothy E.: Information Warfare and Security. Addison Wesley Longman,

[5] Absar-ul Hasan, Ghalib A Shaw Ather Ali “Intrusion detection systems using wireless sensor networks”, EJSE special issue, Wireless sensor networks and practical applications (2010).

[6] Lutz, K. ; Inst. of Integrated Sensor Syst., Tech. Univ. Kaiserslautern, Kaiserslautern, Germany ; Konig, A. “Minimizing power consumption in wireless sensor networks by duty-cycled reconfigurable sensor electronics” Intelligent Solutions in Embedded Systems (WISES), 2010, Page(s):97 – 102

[7] Zhen Fang ; Zhan Zhao ; Xunxue Cui ; Du, Lidong ; Geng, Daoqu ; Yundong Xuan ; Jing Xu ; Wu, Shaohua ,” Micro sensor network node design for meteorological parameter monitoring “, 2010, IET-WSN, International conference Publications, Year: 2010 , Page(s): 123 - 128

[8] Braghin, F. ; Leo, E. ; Resta, F., “ Modelling of Air Damping in MEMS Inertial Sensors: Comparison Between Numerical and Experimental Results", Thermal and Multiphysics Simulation and Experiments in Micro – Economics and Micro Systems, 2006, EuroSime 2006, 7th International Conference, 2006,

[9] Shaby, S.M. ; Juliet, A.V. "Performance analysis and validation of sensitivity of piezoresistive MEMS pressure sensor” Recent Advances Recent Advances in Intelligent Computational Systems (RAICS),2011, IEEE Publication Year: 2011 , Page(s): 692 - 695

[10] Mohamed Al-Ibrahim and Jasem Al-Ostad, " The Usability, creditability and Security of E-voting System in Education Sector", 2012 3rd International Conference on e-Education, e-Business, e- Management and e-Learning IPEDR vol.27, 2012, IACSIT Press, Singapore
[11] Daniel G. Costa and Luiz Affonso Guedes, " The Coverage Problem in Video-Based Wireless Sensor ", Networks: A Survey, Sensors 2010, 10, 8215-8247; doi:10.3390
[12] Surve, V, 2006, "A wireless Communication Device for Short Messages", Masters Thesis, Available: www.certec.lth.se/doc/awireless.pdf.
[13] Taylor, K; "Mobile Monitoring and Control Infrastructure", CSIRO Available online at http://mobile.act.cmis.csiro.au. International Journal of Engineering (IJE), Volume (3):Issue (1)