ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

Wireless Sensor Network Based Surveillance System to Track Enemy Intrusion at Borders

K.Shanmugavalli, K.Fathima

Abstract*— *In today's geopolitical climate, ensuring the protection of secure facilities or key locations against resourceful and determined intruders is of paramount importance to the defense of a national border as well as industries of national importance. The greatest threat to national security is "Terrorism" and it cannot be defeated by conventional military force alone. In critical border areas , regular forces or even satellites cannot monitor these intruding terrorists as the area monitored is quite large and quite complex. To assist the army and security forces operating in these areas, smart dust like micro-sensors with wireless interfaces could be utilized to study and monitor these environments from a certain distance for military purposes. The paper aims to develop next generation wireless sensor networks for defense industry and homeland security applications. The smart dust wireless sensor mote detects and classifies into vehicles, individuals and groups.

***Index Terms*— Sensors, smart dust, Intrusion Detection Systems.**

I. INTRODUCTION

The transportation sensing wireless network is recognized as an important component of the intelligent transportation systems. More and academic researchers and people from Industry are engaged in developing them due to the good promise and potential with various application systems. Wireless sensor networks offer the potential to significantly improve the efficiency of existing transportation systems currently, collecting data for traffic planning and management is achieved mostly through wired sensors. The equipment and maintenance cost and time consuming installations of existing sensing systems prevent large-scale deployment of real-time traffic monitoring and control. Small wireless sensors with integrated sensing, computing, and wireless communication capabilities offer tremendous advantages in low cost and easy installation. Target classification is an important enabling technology for the monitoring task in transportation sensing networks. Some applications of sensor network technologies in intelligent transportation systems (ITS) include parking lot monitoring, traffic monitoring, and traffic control. Vehicle classification information is one of the important measurements that we need to obtain in practice, which is invaluable for various aspects of transportation including engineering and planning. If a mobile target on some key roads can be recognized, it would provide helpful traffic information.

II. PROBLEM BACKGROUND

In a transportation system mobile targets can be classified according to different classification standards. In the paper we divide them into six kinds, including free personnel, personnel with metal object, small vehicle, passenger car, heavy vehicle and track layer vehicle. This classification method can be used either in most of applications or in military field.

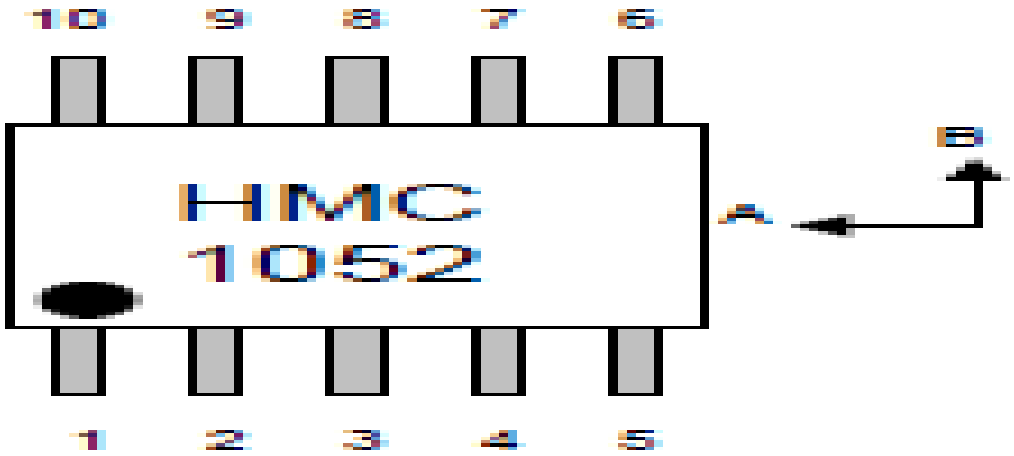

Fig 1. HMC1052 MAGNETORESISTIVE

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

The detailed recognition description is given as follows. Free personnel are the persons who walk without any metal object, while personnel with metal object can be detected by the sensing signals from magnetic Sensors nearby. They would create a tiny seismic signal heavy vehicle, small vehicle and passenger car. A heavy vehicle has a total mass exceeding 4500 kg, otherwise it should be belong to the type of small vehicle. The length of passenger car should exceed six meters taking no account of its weight. As this type of target has a high strength of seismic signal in the ground that is obviously different from other types of vehicle, thus we take it as a special type of target. The category of track layers exists in most of battlefields, e.g. armoured cars and tanks.

A) TYPE SELECTION OF SENSORS AND NODE SYSTEM

With the rapid development of technology is developed rapidly, the trend of sensor micromation becomes common in many applications. Usually a single sensor is used to provide the information of road targets. In the paper different kinds of tiny sensors are adopted to collect the target data. They are the magnetic Honeywell 1052 sensor and the seismic acceleration ADXL202E are used in figure 1. In order to improve recognition performance, we adopt the concept of peak and valley pattern which is used to deal with the hybrid detection signals from different sensors. In the paper, the magnetic signal and seismic acceleration signal from various sensors are collected, analyzed and transmitted to the system. We obtained experimental results of the performance of classification of sensors track the field. These results are shown that classification accuracy is high, and the algorithm is capable of identifying mobile targets on some roads in intelligent transportation of various data to the system. The paper develops as follows. The next section describes the basic problem background which includes the classification principle of WSN and type selection of the used sensors.

B) DEVICE OPERATION

The Honeywell HMC1052 magneto resistive sensors are Wheatstone bridge devices to measure magnetic fields. With power supply applied to a bridge, the sensor converts any incident magnetic field in the sensitive axis direction to a differential voltage output. In addition to the bridge circuit, the sensor has two on-chip magnetically coupled straps; the offset strap and the set/reset strap. The magneto resistive sensors are made of a nickel-iron (Perm alloy) thin-film deposited on a silicon wafer and patterned as a resistive strip element. In the presence of a magnetic field, a change in the bridge resistive elements causes a corresponding change in voltage across the bridge outputs. These resistive elements are aligned together to have a common sensitive axis that will provide positive voltage change with magnetic fields increasing in the sensitive direction. Because the output only is in proportion to the one-dimensional axis and its magnitude, additional sensor bridges placed at orthogonal directions permit accurate measurement of arbitrary field direction. The combination of sensor bridges in two and three orthogonal axis permit applications such as compassing and magnetometer. The offset strap allows for several modes of operation when a direct current is driven through it.

II. NETWORK INTRUSION DETECTION SYSTEM ON SMART SENSORS

Totally there are 3 dust Motes in this paper, out of them 2 motes are the tiny sensor dust motes and 1 Mote with display unit and an alert buzzer. The 2 dust motes have a variety of sensors i.e. vibration/seismic, magnetic, acoustic and thermal, a microcontroller for processing these sensor values and a radio transceiver for communication over a wireless network. A Network of this type can be deployed within an area as large as 4,000m² in a few minutes by one or two men. The central monitoring node acts as the parent node in a peer to peer wireless network model.

The dust motes communicate with central parent node using LR-WPAN. Microchip PIC microcontroller and MiWi P2P wireless protocol is used in all dust motes and they are typically battery powered. Microchip's MRF24J40MA, the RF transceiver used in this implementation, is a 2.4 GHz wireless transceiver module which offers low-data rate, low-power consumption and has an integrated PCB antenna with matching circuitry.

MiWi P2P protocol is selected for this paper since many developers trying to use WPAN technologies have observed that ZigBee seems undesirably complex and increases system cost. MiWi P2P protocol is lightweight WPAN stack, small foot-print alternatives (3K-17K) to ZigBee (40K-100K); they are useful for cost-sensitive applications with limited memory such as the dust mote in this paper.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

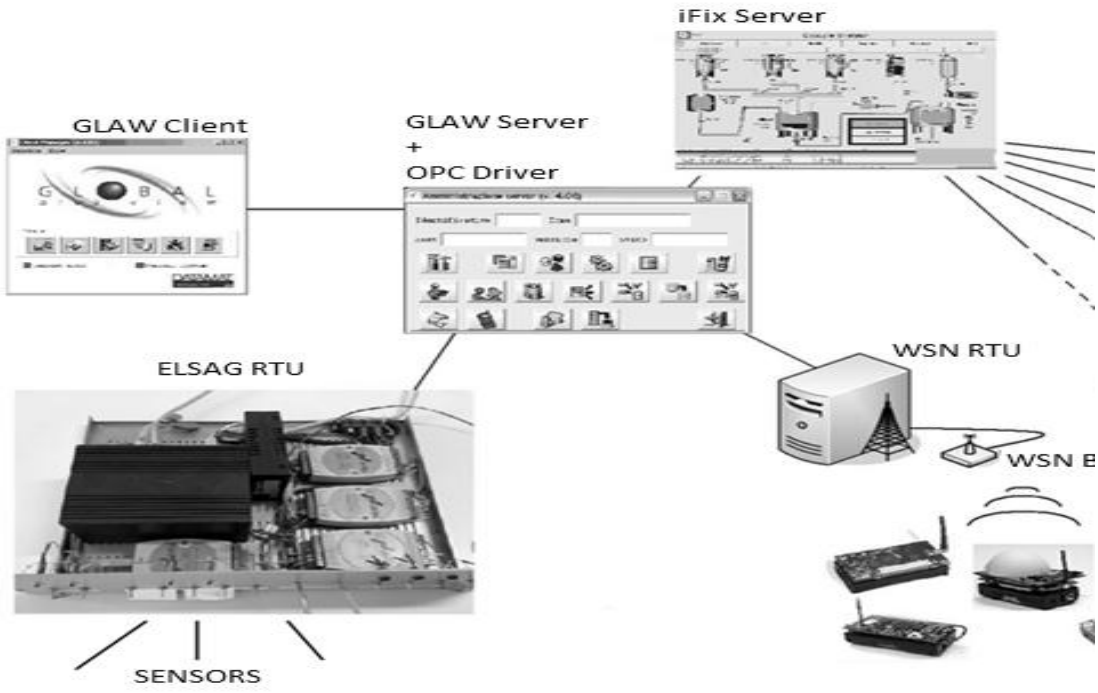

Fig 2. NETWORK INTRUSION DETECTION SYSTEM ON SMART SENSORS

IV. GLOBAL SCENARIO

Although the design of the smart sensors via the implantation of IDS in a device to make it behave as an intelligent sensor is the core idea of this paper, it is also true that most of this proposal advantages make that sense only, when one or more of these sensors act, forming a DIDS (Distributed intrusion detection system) as part of a much more sophisticated system. That is why we begin our proposal description by defining the general framework within smart sensors is used to integrate the system. In this scenario, our embedded are seen as smart sensors and play the role of service providers offering WSN. For this same reason, the scenario has been divided into the three classical scenario areas: 1) Service Provider Area; 2) Service Broker Area ; and 3) Service Consumer Area. The Service Provider Area may find different intelligent network sensors which act as embedded and which have been connected to the networks to be investigate. From a functional perspective, the scenario may also be described on the basis of different phases of the SOA model: 1) publication, 2) discovery, and 3) consumption.

1) Publication phase correspond with the first sensors state (when they are connected to the network). In this phase, the sensor should locate a publication server using the UDDI (universal description discovery integration) protocol to send all the documentation describing the service in the form of WSDL (web-service detection login format) pages.

2) During the discovery phase, any WSN client wishing to consume an intrusion detection service offered by a smart sensor should know it previously. For this purpose, first they will locate a registered service and will request sensor documentation to ascertain all its address details, how it should be approached, and the manner in which the requested service will be returned to them. Once again, the UDDI protocol will be used and the information will be based on WSDL pages.

3) Consumption is the most important phase of all as this is what grants real significance to the whole wireless system and then Networks are more effective. Clients in this phase, having discovered the available services, are in a position to consume them or to approach the smart sensors and request the services they offer directly. Communication between the services and consumers in this phase shall be made through requests and response.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

V. EMBEDDED IDS PROPOSAL

Once established the general scenario, this section will focus on the design of the IDS(intrusion detection system) embedded into a device inspired in smart sensors. Before starting up, it is important to clarify the existing relationship between our proposal and the traditional approach based on smart sensors networks (SSN). In the field of SSN, each sensor's autonomy is taken for granted.

To achieve that, it is been considered, generally speaking, that the smart sensors cannot be wired. Due to that, sensors should be efficient and collaborate to transmit the information to its final destination in the most sensible way consumption-wise. In our proposal, the smart-sensors-based device employed are twisted-pair network sensors, so any limitation to their power autonomy becomes meaningless by the fact that they could be energized by an array of different techniques like Power over Ethernet and external power supplies, for example. By similar reasons, there is no point in addressing the typical problems related to signal–retransmission collaboration and the like.

These are just a few SSN's characteristics, but there are others of similar importance. Among them, the way they were conceived, in which traditional sensors acting as mere transducers are bestowed with processor, memory, and a communications module that allow the inclusion of know-how, information storage, and the supply-on-demand of the often processed into knowledge information. These are the features that have guided our IDS design, embedding it into a smart sensor. The sensor should be continuously consulted via pooling techniques, but, on the contrary, that it will just notify any intrusion attempt asynchronously, on demand and under the conditions and restrictions (detection thresholds, bandwidth, etc.) indicated. Therefore, we can say that the fundamental basis of our proposal is the design of an IDS embedded in a miniaturized network device which will offer functionality as a WS.

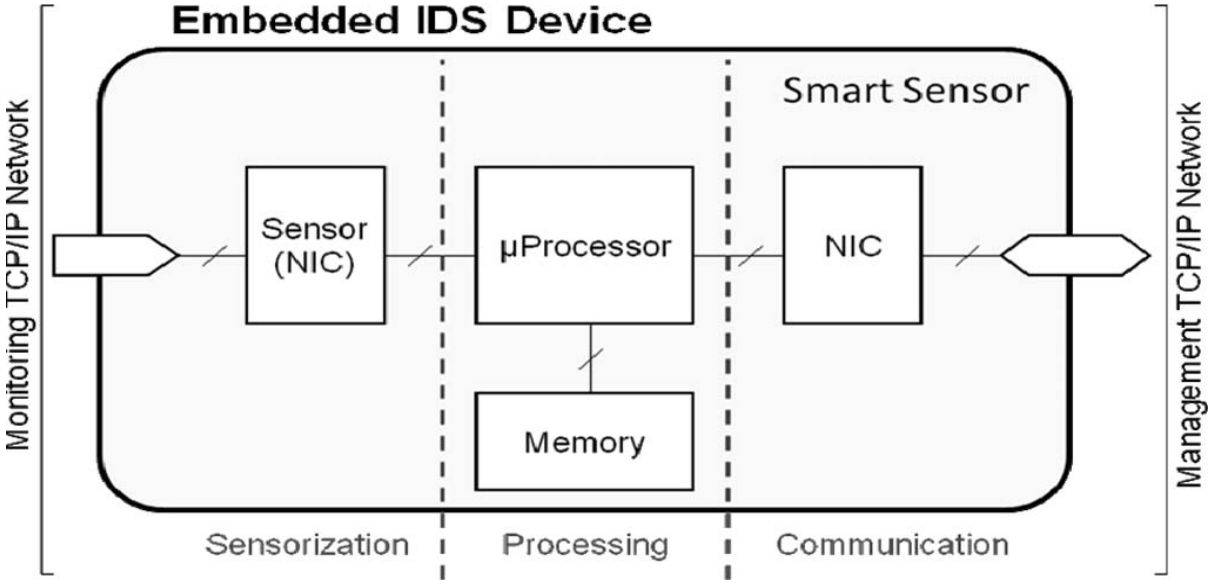

Fig 3.PHYSICAL STRUCTURE OF THE SMART SENSORS WHICH ACTS AS AN EMBEDDED DEVICE WHICH SERVES AS A SUPPORT FOR THE SENSORS

From a physical perspective, the system has been designed as a smart sensor. Fig. 3 shows the physical structure of the sensor indicating its main elements: The sensor itself which is formed by a network adapter for connection to the local area network (LAN) whose traffic is being analyzed. This adaptor should support promiscuous mode to capture all the network traffic. This element provides the system with sensitivity; a microprocessor with embedded additional functionality to analyze the captured traffic online, looking for behavior patterns which could be considered anomalous, such as intrusion attempts, which are to be converted into alerts; in addition to computing power, the sensor has been provided with a non volatile internal memory to store the alerts generated by the IDS, together with the involved traffic; and finally, the device has an additional communications model for its connection to the management network (generally the Internet) by means of which it will receive analysis requests on possible intrusion attempts from the system.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

In fact of having two independent networks interfaces for monitoring and for communication, in addition to generalizing the proposal, makes it more viable in terms of a hostile, resources-starving environment like the world of computer network management. Although from a physical perspective, the IDS network system could be considered smart sensors; from a functional viewpoint, it could be labeled as a service for network intrusion detection organized into different layers as in figure (4.)

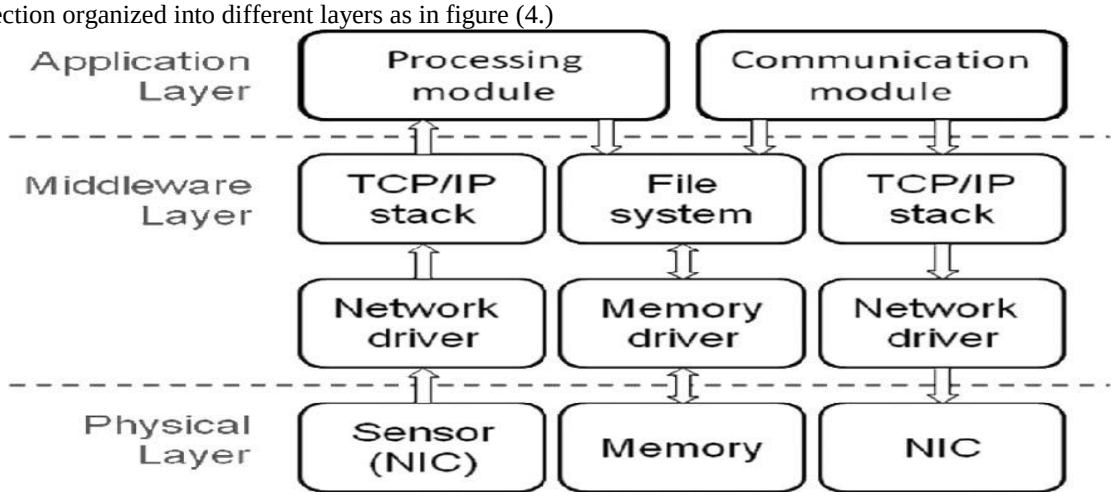

Fig 4. SOFTWARE ARCHITECTURE OF THE EMBEDDED IDS DEVICE

1)The physical layer considers the physical resources of the device from a functional point of view; to achieve its objectives, the following elements should be connected, i.e., the LAN from which information is to be obtained, the internal memory of the device in which the processed information will be stored (i.e.,IDMEF alerts generated), and the management network.

2) The middleware layer houses the modules which provide access to the basic resources of the physical layer (network adaptors, memories), encapsulating them, and providing the upper layer with a standardized vision, free from physical details. According to the foregoing, the main blocks proposed are those of network and disk input/output management, together with a simple file system to facilitate nonvolatile memory management and an implementation of a TCP/IP stack essential for all the processes of the application layer.

3) The application layer is the most important layer from a functional perspective. It contains the main functional components of the device. These components have been grouped into two large modules, a processing module and a communications module. These are analyzed in further detail above. The processing module has in turn a preprocessing filter which adapts the traffic from the network, normalizing and converting it into an information pattern. This pattern is the input source of the analysis module which detects intrusions and generates alerts in IDMEF format. This module compares the input patterns with a map of patterns previously stored in the nonvolatile memory of the device, and in the event of detecting an anomalous behavior, it will catalogue it as an intrusion attempt and will store an alert indicating this fact, together with the traffic from which it originated and other appropriate information (such as the date and time it occurred or the type of traffic affected). The analysis module is a key element of the system since it implements the IDS and its constitutes.

VI. EXPERIMENTAL RESULTS

We conducted our experiments on a simulated WSN. The simulation was performed by using TOSSIM .Each simulation run was conducted with a number between 100 and 250 and the following settings: only one attacker, nodes are stationary, and a number of each node between 5 and 10. The results of the simulation tests were confirmed by executing an experimental campaign on a real network consisting of a number of nodes ranging from eight to fifteen. At each run of the test on the real network we physically deployed the nodes accepted best practices for WSN deployment, in order to avoid common pitfalls. The workflow includes four phases. Sensor nodes periodically generate control messages whose content is processed by the IDS CA module (Phase 1) to detect possible ongoing attacks and identify the attacker. During Phase 2 the malicious behaviour of the attacker node is triggered. During Phase 3, the nodes under i) recognize an anomalous behaviour, ii) put the suspicision nodes in a block list, and iii) generate alert messages. In Phase 4, alerts are sent to the IDSCA, which in turn – base on the control messages which have been gathered and the received alert –makes its decision. It is worth noting that the

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

IDS CA continuously checks control packets also in absence of alerts. Hence it is able to detect possible attacks evading detection performed by the Local Agents.

Experiments were conducted focusing on the sinkhole attack. To compare our hybrid solution to purely centralized solution, we deployed two different scenarios. In scenario A we assume that the sensor data, but it does not modify the control messages which are used for detection purposes. In scenario B, we assume that the attacker is smarter, and it is able to modify all received messages (data and control packets). A first test session was executed with a simulated network made of a random number of sensors. In this session we tested 100 different topologies each in 10 different simulations. In each run a random node behaves as the attacker. The results of the simulation tests have been validated by comparing them to those attained in the real network environment Current permanent Wireless Sensor Networks (WSN) installations all employ static configurations. In this paper we are concerned with applications in which the relative positions of motes can change quickly, where there is a need to maintain a record of their positions, so that the data gathered can be correctly interpreted. Of course, the Global Positioning System (GPS) [4, 5] provides a practical solution to WSN localisation, however GPS has two main drawbacks; it requires a good 'view' of the sky which limits its use to the outdoor environment; secondly the size, cost, power requirement and general operational practicality are significant limitations. We use a computer model of a WSN of 'Smart Dust' (SD) motes envisioned as 'free-flying' in a 3-D Dimensional airspace. The motes automatically generate Relative Signal Strength Indicator (RSSI) [6] data as part of the data packet stream subsequently stored.

VII. CONCLUSION

In this paper we presented an Intrusion Detection System for protecting Critical Information Infrastructures using Wireless Sensor Network technology. The proposed system relies on a hybrid detection approach in the sense that any node runs a detection agent which is in charge of identifying suspicious nodes. In order to validate the an experimental campaign has been conducted, which demonstrated the effectiveness of the proposed approach against some emerging attacks to WSNs, namely sinkhole attacks and sleep deprivation attacks. Also importantly, results demonstrated that our solution satisfies the stringent requirements (in terms of limited availability of resources)which are typical of Wireless Sensor Networks.

REFERENCES

[1] Bradley C. Norman & Douglas G. Adams. 2007."Virtual Perimeter Security (VPS) in a Physical Protection System", IEEE A&E SYSTEMS MAGAZINE.

[2] CUI Xun-xue, QIU Guo-xin, ZENG Jian-qin, XING Li-jun, LIU Qi .2008."A Target Classification Algorithm Based on Transportation Sensing Network ", Workshop on Power Electronics and Intelligent Transportation System.

[3] Francisco Maciá-Pérez, Francisco J. Mora-Gimeno, Diego Marcos-Jorquera, Juan Antonio Gil-Martínez-Abarca, Héctor Ramos-Morillo, and Iren Lorenzo-Fonseca,2011. "Network Intrusion Detection System Embedded on a Smart Sensor", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 58, NO. 3.

[4] GRAHAM A. ROLLINGS and DAVID W. CORNE, 2008,"Intelligent Operators for Localization of Dynamic Smart Dust Networks", Eighth International Conference on Hybrid Intelligent Systems.

[5] Luigi Coppolino, Salvatore D'Antonio, Luigi Romano, and Gianluigi Spagnuolo.2010. "An Intrusion Detection System for Critical Information Infrastructures Using Wireless Sensor Network Technologies", IEEE.

[6] K. M. Tan and R. A. Maxion, "Defining the operational limits of stide, an anomaly-based intrusion detector," in Proc. IEEE Symp. Security Privacy, Oakland, CA, 2002, pp. 188–201.

[7] C. Kruegel and G. Vigna, "Anomaly detection of Web-based attacks," in Proc. ACM Conf. Compute. Common. Security, Washington, DC, 2003, pp. 251–261.

[8] K. Wang and S. Stolfo, "Anomalous payload-based network intrusion detection," in Proc. Int. Symp. Recent Adv. Intrusion Detection, French Riviera, France, 2004, pp. 203–222.

[9] Camp T, Boleng J, Davies V. A" Survey of Mobility Models for Ad Hoc Network Research". WCMC: Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, 2(5):483–502, 2002.

[10] Akyildiz I, Su W, Sankarasubramaniam Y, Cayirci E. "Wireless sensor networks: A survey," IEEE Computer, vol. 38(4):393–422, 2002.

[11] Niculescu and B. Nath." Ad Hoc Positioning System (APS) using AoA "INFOCOM 2003.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

[12] Mainwaring A, Polastre J, Szewczyk R, Culler D, Anderson J." Wireless Sensor Networks for Habitat Monitoring, in ACM International Workshop on Wireless Sensor Networks and Applications" (WSNA'02). 2002.

[13] Szewczyk R, Osterweil E, Polastre J, Hamilton M, Mainwaring A, Estrin D, "Habitat monitoring with sensor networks, "Communications of the ACM, 47(6):34–40.

[14] National Space-Based Positioning, Navigation, and Timing Coordination Office. http://www.gps.gov/

AUTHOR BIOGRAPHY

Asst.prof. K.Shanmugavalli obtained her Bachelor's degree (B.E) in Electrical and Electronics Engineering from Anna University, Chennai, India and master's Degree in Process control and instrumentation from Hindustan University, Chennai, India. .she has presented papers at conferences .At present; she is Associate Professor in the Department of Electrical and Electronics Engineering, vel tech engineering college, Tamil nadu, India. She has 1.1 years of teaching Experience.

Asst.prof. K.Fathima obtained her Bachelor's degree (B.E) in Electronics and communication engineering from Anna University, Chennai, India and Master's Degree (M.E) in embedded system technologies from Anna University, Chennai, India. .she has presented papers at conferences .At present; she is Associate Professor in the Department of Electrical and Electronics Engineering, vel tech engineering college, Tamil nadu, India. She has 1.2 years of teaching Experience.