# Design of a Fence Surveillance System based on Wireless Sensor Networks


Youngsoo Kim
Information & Communications University (ICU)
119 Munjiro Yuseong-gu
Daejeon, 305-732, Korea
+82-42-866-6811
pineland@icu.ac.kr

Daeyoung Kim
Information & Communications University (ICU)
119 Munjiro Yuseong-gu
Daejeon, 305-732, Korea
+82-42-866-6811
kimd@icu.ac.kr

Poh Kit Chong
Information & Communications University (ICU)
119 Munjiro Yuseong-gu
Daejeon, 305-732, Korea
+82-42-866-6811
chongpohkit@icu.ac.kr

Jonggu Kang
Information & Communications University (ICU)
119 Munjiro Yuseong-gu
Daejeon, 305-732, Korea
+82-42-866-6811
jjang9dr@icu.ac.kr

Eunjo Kim
Information & Communications University (ICU)
119 Munjiro Yuseong-gu
Daejeon, 305-732, Korea
+82-42-866-6811
imikej33@icu.ac.kr

Suckbin Seo
Information & Communications University (ICU)
119 Munjiro Yuseong-gu
Daejeon, 305-732, Korea
+82-42-866-6811
pastrol@icu.ac.kr



## ABSTRACT

In this paper, we present a real application system based on wireless sensor network (WSN) for fence surveillance which is implemented on our development platform for WSN, called ANTS (An evolvable Network of Tiny Sensors). Our system, called the WFS system, is expanded to connect and control a robot (UGV/UAV) and a camera sensor network for the purpose of fence surveillance. Two kinds of sensor nodes, ground nodes and fence nodes, are deployed and collaborative detection is performed and the result is reported to the base station (BS). The BS does not only give a control message to the camera to show the place where an event has occurred, but it also issue orders to the robots to extend the communication distance of the system, to approach and sense the object more precisely, or even to attack an enemy autonomously. This paper describes various techniques and know-how to fulfill a WSN-based integrated surveillance system. A new adaptive threshold algorithm to detect intruders is proposed and some sensing results in the real field of our system are shown. In conclusion, we show the high accuracy of the WFS system.



## Categories and Subject Descriptors

C.3 [**Special-purpose and Application-based Systems**]: *Microprocessor/microcomputer applications, Process control systems, Real-time and embedded systems*




*Autonomics 2008*, September 23–25, 2008, Turin, Italy




## General Terms

Design, Experimentation

## Keywords

Sensor network, distributed system, autonomous system


## 1. INTRODUCTION

Wireless sensor networks (WSNs) have great promise as an enabling technology for a variety of applications from merely for data collection to getting significant information on an interested area. With the rapid development of WSN technology, it is now feasible to make more complex WSN applications. Military, Environment, Habitat, Industry & Business, Health, and Smart Home are the main categories of the WSN applications. As the surveillance system is one of the typical applications of WSN, many existing researches have been performed and some systems have already been built for the purpose. [2][3][4]

The capabilities of WSNs, such as event detection, are appropriate for automating fence surveillance. G. Wittenburg, et. al already explored the fence monitoring system using previous WSN technologies [2]. However, most existing systems including the above system merely obtain some information from their sensor field without associating any equipment or other systems such as robots, etc to extend the sensing accuracy. The validity of WSN can be extended through combination with those systems, and their technology can also play a central role to perform the mission of the system. The WSN system is expected to play an increasingly important role for various application spaces in the future.

We implemented a fence surveillance system which is a WSN system combined with a network (N/W) camera, a UGV

(Unmanned Ground Vehicle), and a UAV (Unmanned Air Vehicle). The connected peripheral systems are also controlled based on the results from the sensor field, so they are called subsystems. The camera is used to visually identify what a detected object is and the robots are used to extend the communication distance of the system, to approach and sense the object more precisely, or to attack an enemy. The details are described in Sec. 2. In summary, the primary goals of our system are:

- To make a fence surveillance system feasible with current WSN technology, in this case our ANTS (An evolvable Network of Tiny Sensors) platform [1], by setting up a working system.
- To combine the WSN technology with other systems to upgrade the capability of the system.
- To develop and describe a systematic approach to build a robust event detection and reporting algorithm based on the capabilities of WSN.

The rest of this paper is organized as follows. Section 2 contains a discussion of the architecture of our WSN-based Fence Surveillance (WFS) system, and section 3 describes our S/W algorithms implemented in the system. Our deployment and experimental results are illustrated, and the performance of our proposed algorithm is empirically compared in section 4. Finally, Section 5 concludes our experiments and discusses future works.

# 2. WSN-BASED FENCE SURVEILLANCE SYSTEM

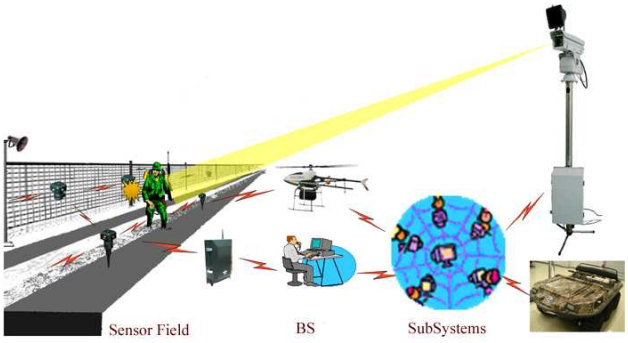


**Figure 1. The overall architecture of the WFS system**

The WFS system is largely divided into 3 parts, sensor field, base station (BS) and subsystems as shown in Figure 1. The first part consists of two types of sensor nodes, ground sensor node and fence sensor node, and the BS part is composed of a gateway (G/W) and a control center (CC). Lastly, the part of subsystems comprises a N/W camera, a UAV and a UGV. The detection targets are human beings and vehicles. The scenario is as follows:

- An object enters in the detection scope of the WFS system and a sensor node senses it and then transfers the information to the BS through the sensor network.
- The BS displays the transferred information in the screen and remotely controls the N/W camera to show the location where the event had occurred.
- The BS instructs the UGV or the UAV to perform a mission if necessary.
- An operator can identify what the sensed object is through the image transferred by the camera. If falsely alarmed, a control message for modifying the detection threshold is sent to each false alarming node.

## 2.1 Sensor Field

All nodes are installed with acoustic, magnetic and passive infrared (PIR) sensors to detect intruders while a seismic sensor is only equipped on a ground node and a piezoelectric sensor only on a fence node. Three PIR sensors are built into a fence node and four PIR sensors are found in a ground node. Figure 2 shows the outdoor appearances of the nodes and their circuit board.

(a) (b) (c)

**Figure 2. The circuit board of nodes (a), a ground node (b) and a fence node (c). The circuit board has a 1.97”x1.97” footprint and the dimensions of the enclosure are 3.03”x3.03”x9.84” for a ground node and 3.03”x3.03”x 3.94” for a fence node respectively.**

### *2.1.1 Ground sensor node*

The ground sensor node operates using a low-power 16-bit 8 MHz CPU. All sensors are controlled by the CPU, which means it can drive noise levels lower as well as increase the strength of weak signals through the amount of amplification we require. For the RF module, a Chipcon CC1100 operating at 433MHz is used.

The NaPiOn Passive Infrared Sensors [5] are equipped with the Fresnel lens and an OP-AMP is used for signal amplification between the PIR sensors to and the ADC. An acoustic sensor with high sensitivity, WM-61A [6], is used and a geophone, GS-20DX [7], is employed as the seismic sensor. Its signal is amplified to increase the sensitivity and a bridge circuit is applied to minimize the power consumption of the amplifier. Our magnetometer is from Honeywell [8]. It senses along 3 magneto-axes and its advantage is in the near-perfectly orthogonal dual sensor on a single chip. The sensor is designed to be controlled by the CPU as well to be calibrated regardless of magnetic intensity of surroundings. The magnetometers are very sensitive, low field, solid-state magnetic sensors designed to measure direction and magnitude of Earth’s magnetic fields, from 120 micro-gauss to 6 gauss.

### *2.1.2 Fence sensor node*

We hung fence sensor nodes on the fence. The sensor node for the fence is designed based on the same board and built with a piezoelectric cable sensor, Piezocable [9], which can sense the movement of the fence while hanging on the fence, instead of a seismic sensor in the above ground node. The piezoelectric cable is a sensor which reacts to any compression in the fence by transforming kinetic energy caused by those movements to

electronic signals which are then captured by the CPU. Since the piezoelectric sensor is directly connected to the ADC of the CPU, their measurements can be monitored in real-time and an interrupt is signaled by a comparator when their values are over a threshold.

## 2.2 Base Station

Our Base Station (BS) comprises a gateway (G/W) node and a control center (CC). The G/W has a high performance 32-bit CPU running embedded Linux kernel 2.4.x and a communication module, which supports Ethernet and CDMA. The communication distance is between 50 and 500 meters. It supports a multi-threaded based full-duplex communication and real-time signal processing. Filtering, buffering and retransmission are performed for a stable communication. The CC was implemented using Microsoft Visual Basic. Four functional parts, showing sensing data (including TTS (Text-to-Speech) for alarming), controlling the thresholds of sensor nodes, controlling and displaying the N/W camera, and interacting with UGV/UAV, are contained within the CC. The state of each sensor is shown with three color modes (red: positive detection, yellow: probable detection, gray: no detection)

The type of communication messages between the G/W and CC are divided into N/W management message, control message and notification message as shown in Figure 3. The control message is to control thresholds of sensor nodes and the notification message is to transfer sensing data from a sensor node to the CC. All messages are encoded and transported according to RFC1662 binary format. A checksum is included in the datagram of all sensing data to be transferred to the BS for ensuring the integrity of the data and the G/W filters any erroneous data prior to sending it to the CC.

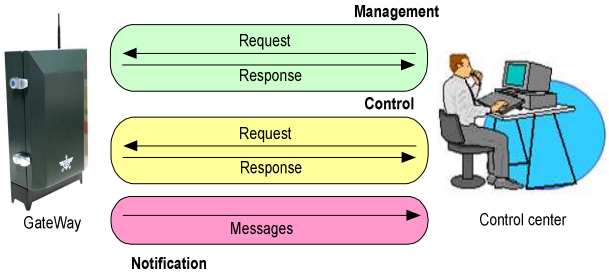


**Figure 3. Communication messages between the G/W and the CC**

## 2.3 Subsystems

### *2.3.1 Unmanned Ground Vehicle*

A 6-wheeled Argo manned vehicle, remodeled for autonomous unmanned control, is used as a UGV to provide active and prompt countermeasure for the WFS system. Our UGV is equipped with a control box which contains TI TMS320F2812 processors as a low-level controller to conduct defined autonomous operations by commands, 3 motor controllers, and relays to interface with operational functions of the vehicle. The processor on board adjusts 3 linear actuators to drive it. One actuator controls throttle for acceleration. The other two actuators control 3 wheels on each side for steering and braking. A PC-104 type computer system based on a Pentium 660 MHz CPU is used as a high-level controller. By utilizing several sensors like a laser range finder, SICK LMS291, for obstacle avoidance and a DGPS, developed by Dusitech [10], for global positioning, the high-level controller can plan routes and decide motions to be processed. The decision is transmitted to the low-level controller via RS232 communication. In addition, the UGV has two wireless communication channels for external control. One is the same channel as the sensor nodes used. Therefore, the UGV is regarded as a part of the sensor network which has mobility. The other channel is to communicate with the BS. Currently, wireless LAN is utilized for this purpose.

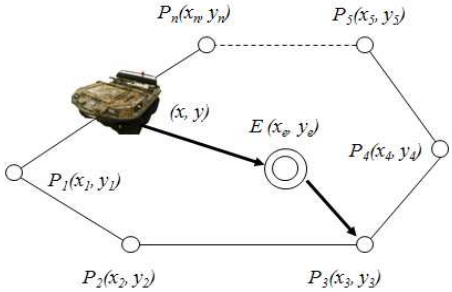


**Figure 4. Operations of an Unmanned Ground Vehicle (UGV)**

The UGV can provide high level of security by removing and compensating blind spots in WFS system with only static sensor nodes and cameras. In ordinary conditions, it patrols predefined routines, defined as a polygon whose vertices are waypoints $P_1$ to $P_n$ in Figure 4, watching for extraordinary situations via day and night cameras. If such situations are detected, it sends notification messages with the position to the BS in order to meet the emergency. Alternatively, in case sensor nodes on the fence or the ground detect invaders or unconfirmed events, it sends a control message for arbitration by BS, and immediately moves to the spot (depicted as E in Figure 4), out of the ordinary routine to check the situation. Finally, after the situation is handled, the UGV continues to conduct normal patrol operation by rejoining the nearest defined waypoint.

### *2.3.2 Unmanned Air Vehicle*

As shown in Figure 5, A RC-type helicopter, a Hirobo 90 EX model [11], is used as the UAV to extend the communication distance between nodes and the BS. The UAV has the characteristics of being speedy, and having well-controlled and stable movements. Our UAV is equipped with a wireless LAN module, a GPS, a battery, and it can fly at a maximum speed of 90 km/h with the full payload of 5 kg. A PC-104 type board based on an Intel Pentium 400 MHz CPU is used as its computer system since it should work well even in a harsh environment with frequent oscillation or electronic noise signals. Embedded Linux is used as its operating system (OS). To prevent being influenced by exhaust fumes from its engine, an outer aluminum shield case and a specially manufactured muffler are used.

**Figure 5. The Hirobo Freya EX 90 RC helicopter and its computer system (PC-104)**

### *2.3.3 Network Camera*

Our network camera consists of a CCD camera, headlights, a pan tilter, a pan tilter controller, and an embedded image server. Normally, the camera is connected to the BS through an Ethernet link and keeps rotating using the pan tilter in angles of between -90 degree and 90 degrees to the forward position, and acts as a server to send the observed images to the BS. Once an event is detected by a sensor node, the BS immediately transmits a request to monitor the position. Once the camera receives the request, it changes from the normal mode, and focuses on the position where the sensor node detected the event. Since our camera possesses GPS, the camera can estimate the positions for the pan tilter with the known locations of sensor nodes.

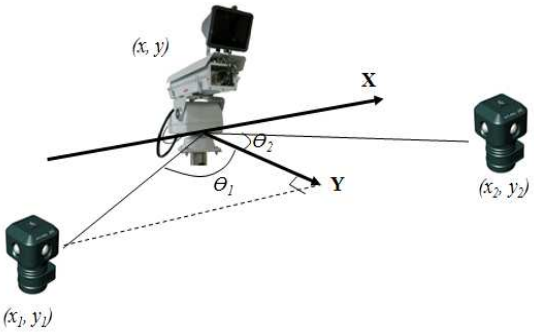


**Figure 6. Automatic Pan Tilter Control of a N/W camera**

Figure 6 illustrates the method of automatic pan tilter control. The position of the camera is $(x,y)$ and a sensor node $n$ is located in $(x_n,y_n)$. Y-axis is neutral position of the pan tilter and X-axis is orthogonal to Y axis. Finally, the angle $\Theta$ of pan tilter is computed as the Eq. 1

$$\theta = tan^{-1}\left(\frac{y_n - y}{x_n - x}\right) - \frac{\pi}{2} \quad (1)$$

## 3. SOFTWARE ARCHITECTURE

We implemented the software architecture of the WFS system based on the ANTS platform which includes OS, Medium Access Control (MAC) and N/W stack for WSNs. For this project, we used the TI MSP430FG4618 microcontroller which has 116KB Flash memory, 8KB RAM and a frequency of 8MHz. To avoid unexpected errors, we primarily allocated the memory as follows: 1.5 Kbytes for the OS, 1.5 Kbytes for the MAC, 2Kbytes for the N/W, and 3 Kbytes for signal processing.

### 3.1 Operating System

The design criteria of the evolvable operating system (EOS) we developed are low power consumption, small code and data size, and evolvability. The EOS's task management module includes a priority round robin scheduler and task synchronization. The problem of stack usage when an application has a large number of concurrent tasks in the system is solved using the Hybrid Task scheduler. The EOS also provides a Message Handling module which includes Inter-Thread Communication (ITC) and Remote Thread Communication (RTC). The basic idea of ITC is using a circular message queue to exchange data among threads and RTC has three communication models: Base station Centered Communication, Publish/Subscribe Communication, and Collaboration/Group Communication. The EOS supports memory space efficient thread management, collaborative thread communication model and a network stack. In addition, power management of the microcontroller and radio transceiver is provided as well.

### 3.2 Medium Access Control

There are 2 types of MAC that is available in the military sensor node. The first is a carrier sense multiple access with collision avoidance (CSMA/CA) that is similar to the one used in the IEEE802.15.4 standard. The second one is based on the CC1100's wake on radio (WOR) capability. In the WOR mode, every sensor node sleeps and wakes up at fixed intervals to sample the channel for packets. The receiver on-time (t_RX_time) is equivalent to the maximum packet length in addition to the sleep interval between each packet transmission and a small amount of guard time. This is to ensure that packets are not inadvertently missed due to slight timing problems. Nodes which want to transmit a packet, transmit the same packets repeatedly at fixed intervals slightly smaller than the t_RX_time and for a total duration longer than the sleep interval. This allows the node to conserve energy through duty cycling at the cost of a slightly longer delay.

### 3.3 Network

Our routing protocol is based on hierarchical routing and supports multi-hop routing to cover a large area of sensor networks. The critical issue in the WFS system is to ensure reliable communication between sensor nodes even when there are unexpected disturbances. Therefore, we try to reduce network failures and support dynamic network functions. The main characteristic of our protocol is as follows:

*1) Self-forming function*: Once sensor nodes are distributed, each sensor node's address is allocated by its parent using the Hi-Low address scheme. So, each node has a dynamic 16-bit address depending on its environment, so that the sensor network becomes more flexible. Assume that the number of children, *MC*, is 4, Each child's address is assigned based on the address of the parent as in Eq. 2 where $AC_n$ is the address of $n^{th}$ child and $A_p$ is the address of its parent.

$$AC_n = MC \times A_p + n \quad (2)$$

Therefore, when a node loses its parent, it can get another address by searching for a new parent's address. The main characteristic of this scheme is that there is no limitation to extend the children's depth compared to the Zigbee addressing scheme and a parent's address can be easily calculated through Eq. 3 where $A_c$ is a child's address.

$$A_p = (A_c - 1) / MC \quad (3)$$

2) *Low power consumption*: When sensor nodes are deployed in a field, they search their neighbors and then construct a neighbor table. If sensor nodes use a routing table as well as a hierarchical routing scheme, they can forward data over a shorter distance by sending packets directly to the destination. This can not only solve the shortest distance problem in hierarchical routing, but also reduce energy consumption caused by detour paths.

3) *Supporting various network topologies*: sensor networks request diverse topologies according to its deployed environments, so our routing protocol is designed to support string, star, and tree

topologies. It means that sensor networks can be easily adapted to different circumstances.

4) *Fault-tolerance function*: sensor nodes can die due to energy drainage, interference, shock and etc, and a dead node can affect the whole network performance. Therefore, we design our network routing protocol with a network-reconfiguration function. For example, if a sensor node is disconnected from its initial network, it will search for another network or find its original parent to connect to.

## 3.4 Event Detection Processing

To use less than 3Kbytes memory for various sensor applications, the sampling rate of the acoustic sensor is 300 Hz and the other sensors are sampled at 100 Hz, and a decision is made every 0.5 seconds. Since a magnetic sensor has 3 axis and four PIR sensors are equipped, nine channels of ADC are required in a sensor node. Each ADC converts an analog voltage to a 12 bit digital value, which is in the range of 0 to 4,095, and each sample is stored as a 2 byte integer. Furthermore, the data is double buffered to allow continuous sampling. Therefore, the total amount of memory required for raw data is 2.2 Kbytes whenever a decision is performed.

$$(50\times8+150)\times2\times2=2{,}200\ bytes$$

It is the most important thing in our system to detect intruders without false alarms, thus we proposed a novel algorithm of adaptive threshold appropriate to the system. Figure 7 describes the sequential process of sensed signals for event detection. Once a node turns on, it first measures the information, average and variance, of its surrounding environment for all sensors for 5 minutes so that it is not affected by the installer of the node and then begins to start sensing for event detection. We then apply a median filter for sensed signals to decrease the influence of outliers or noises and each energy value is computed and compared with the threshold of the corresponding sensor for decision making. Since all nodes are surrounded by different environments, an adaptive threshold scheme should be applied to decrease the rate of false alarm.

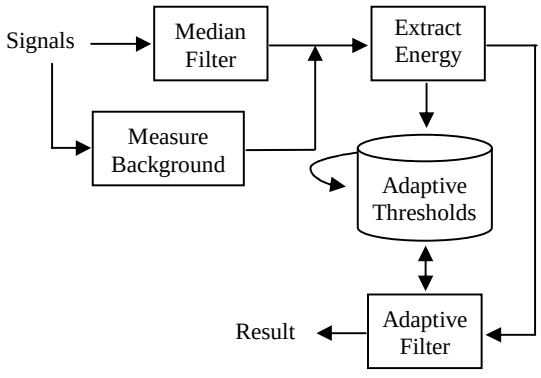


**Figure 7. Diagram of signal processing**

Our adaptive threshold algorithm is derived as follow: The initial average $m_{i,0}$ and the initial standard deviation $\sigma_{i,0}$ for a sensor $i$ are obtained from measuring the background signals and the initial base threshold $BT_{i,0}$ of the sensor is set to $\sigma_{i,0}$ as in the Eq. 4.

$$BT_{i,0} = \sigma_{i,0} \tag{4}$$

To reduce the complexity of the computation, the energy value of signal is computed using Eq. 5 as follows

$$E_{i,t} = | b_{i,t} - m_{i,0} | \tag{5}$$

Assuming that $s$ is the size of buffer for moving average filter, a moving average for energies is computed through Eq. 6 for comparison with the adaptive threshold.

$$m_{i,t} = \begin{cases} mean(E_{i,1} \sim E_{i,t}), & if\ \ t < s \\ mean(E_{i,t-s} \sim E_{i,t}), & otherwise \end{cases} \tag{6}$$

An auto-adapting base threshold, $BT_{i,t}$, that detects an event is computed considering the current energy value as the Eq. 7. The coefficients $\alpha_{1,i}$ and $\alpha_{2,i}$ are settled between 0 and 1 through experiments. Normally, $\alpha_{2,i}$ is greater than $\alpha_{1,i}$ so that the threshold could be more sensitive. However, a real applied threshold, $RT_{i,t}$, is computed as the Eq. 8 to decrease the number of false alarms.

$$BT_{i,t} = \begin{cases} (1-\alpha_{1,i})BT_{i,t-1} + \alpha_{1,i}E_{i,t}, & if\ E_{i,t} > BT_{i,t-1} \\ (1-\alpha_{2,i})BT_{i,t-1} + \alpha_{2,i}E_{i,t}, & otherwise \end{cases} \tag{7}$$

$$RT_{i,t} = BT_{i,t} + 2 * \sigma_{i,t} \tag{8}$$

Finally, The decision of sensor $i$, $\delta_i$, is determined through comparing the average of sensor $i$'s energy with the corresponding real applied threshold, $RT_{i,t}$ as in Eq. 9. If the number of continuous detection is greater than 5, it is regarded that an intruder is detected and the application in the BS gives the red signal for the sensor as well as sounding its alarm through the TTS service. Otherwise, a yellow signal is given to an operator.

$$\delta_i = \begin{cases} DETECTED, & if\ \ m_{i,t} > RT_{i,t} \\ NOT\ DETECTED, & otherwise \end{cases} \tag{9}$$

After a node detects objects, it sends all sensing data to the BS and the N/W camera is used to identify them.

## 3.5 Energy Consumption

The MSP430 processor that we deploy consumes 3.2 mA during active mode and 10.4 μA during sleep mode. The RF module also offers low power consumption i.e., rx: 15.6 mA and tx: 28.8 mA (+10 dBm) at 433 MHz. The battery consumption of RF when it is idle is 15.6 mA in active mode and 1.6 mA in sleep mode. In our application, since the main goal is to monitor the surrounding of a fence and identify intruders, a 30 seconds duty cycle period of 10 seconds for sensing and 20 seconds for sleep, a duty cycle of 33.33%, was used. It is thought that all intruders could be sensed in the situation of our system by using the sensing cycle. So, we applied a sleep and wake up mechanism for the CPU, RF module, and sensor modules so that when sensor nodes are not sensing, they change their status to the sleep state. Later, when they wake up, they sense once and then go back into the sleep mode. The required power for each sensor is shown in Table 1.

The total amount of power required is the sum of power consumed by the microcontroller, radio module and sensor modules. Therefore, the average power consumption for a second is given as follows:

- Active mode

▪ Ground node : 3.20 + 15.60 + (4 * 0.30 + 0.50 + 0.10 + 10.00) = 30.60 mA

▪ Fence node : 3.20 + 15.60 + (4 * 0.30 + 0.50 + 0.01 + 10.00) = 30.51 mA

- Sleep mode : 0.01 + 1.60 + 0.00 = 1.61 mA

If an event to transmit is occurred, 28.8 mA is additionally needed during the active mode. Assuming that no event occurs, our ground node and fence node with a 19,000 mAh capacity batteries can stay alive for 70.22.39 days and 70.41 days respectively as follows:

- Ground node : 19,000 / {(120 * 1.61 + 60 * 30.60) / 180} = 1,685.39 hours (70.22 days)
- Fence node : 19,000 / {(120 * 1.61 + 60 * 30.51) / 180} = 1,689.89 hours (70.41 days)

Since our nodes are not only manually installed and periodically managed but are also monitored all the time, the batteries of all nodes are normally scheduled to be exchanged once every two months in the case of no events being detected. However, when some events occur, the batteries need to be changed faster based on the increased energy consumption.

**Table 1. Characteristics of each sensor used**

| Sensor | Detection Range | Maximum Consumption current | Detection Type | Sensitivity |
|---|---|---|---|---|
| PIR | 10m | 0.3mA | Infrared radiation | -na- |
| Acoustic | variable | 0.5mA | Voice | -35dB |
| Seismic | variable | 0.1mA | Vibration | -na- |
| Magnetic | variable | 10mA | Magnetic field | 1.0 mV/ V/gauss |
| Piezoelectric | 1Km | <10uA | Intrusion | -na- |

## 4. DEPLOYMENT & EXPERIMENTAL RESULTS

We deployed 15 fence nodes on and 20 ground nodes around the fence which is 78.74 inches in height and 2,409.45 inches in length in the campus of Information & Communications University (ICU) and conducted over 50 runs including natural occurring events. The Figure 8~12 shows energies, moving averages, base thresholds and real applied thresholds of real signals by a human or a car passing by a sensor node. We fix the adaptive thresholds as $\alpha_1$ is 0.02 and $\alpha_2$ 0.1 through empirical observation, giving a performance of within 5% false alarm rate. Considering the ratio of signal-to-noise, the sequence of the capacity of detection for sensors is as follows:

*PIR > seismic > acoustic > magnetic > piezoelectric*

First, the PIR sensor can not only sense an object very well but it is also affected less by noises compared to the other sensors. The capacities of acoustic signals and seismic signals seem to be similar with each other for target detection. When a human produces a normal voice or a step sound, he or she can generally be detected within 5 meters by an acoustic sensor. Although magnetic signals are less affected by noise, they have a tendency of being insensitive for detecting smaller metal objects. So, they were unable to detect a human riding a bicycle over a range of 2 meters from a node in our experiment. The variance of piezoelectric signals is relatively big, as Figure 12 shows, that it gives us the most unstable performance among the sensors.

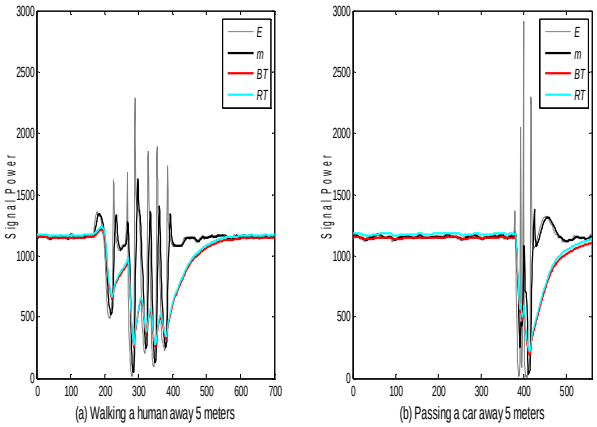


**Figure 8. PIR energy and threshold for each object**

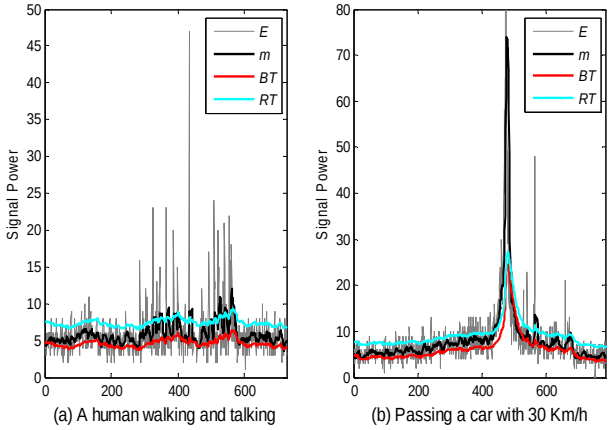


**Figure 9. Acoustic energy and threshold for each object**

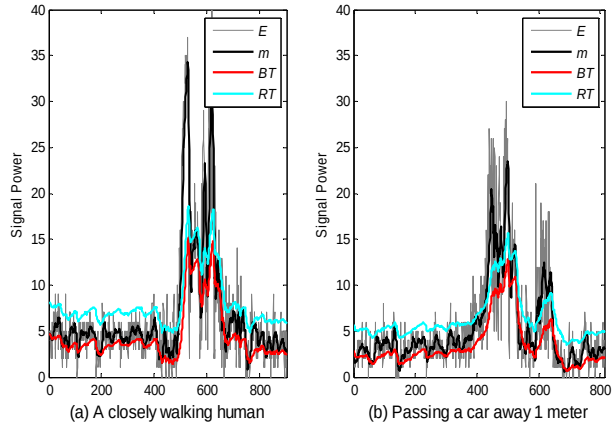


**Figure 10. Seismic energy and threshold for each object**

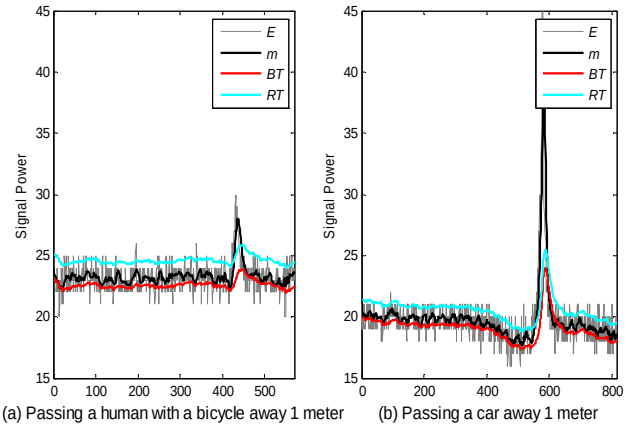


**Figure 11. Magnetic energy and threshold for each object**

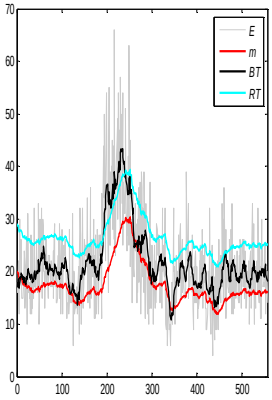


**Figure 12. Piezoelectric energy and threshold in a case of shaking the fence**

In the beginning of the system, the adaptive threshold scheme caused some false alarms prior to stabilizing those thresholds. Except for those initial errors, all intruders were perfectly detected for normal cases in our system. However, some false alarms also occurred, i.e., a piezoelectric sensor made a false alarm in strong wind, and some tiny wild animals such as a cat infrequently gave us some false alarms. However, we could identify them immediately through the camera. In conclusion, we have a satisfactory result from the WFS system.

## 5. CONCLUSION & FUTURE WORKS

We present a real application system based on wireless sensor network (WSN) for fence surveillance combined with a UGV/UAV system and a camera system. It is implemented based on our ANTS development platform of WSN. The technologies of WSNs are very promising in changing human lifestyle in the near future, and they will also perform a major role in various distributed autonomous systems.

We proposed and implemented many realistic techniques to improve the accuracy and robustness in our system. Since the sensor nodes are very cheap, we focused on event detection through refining the sensor signatures and reducing the number of false alarms significantly. It is shown that all intruders are detected for the normal cases and few false alarms occurred using our proposed adaptive threshold algorithm in the system. Additionally, we found that other autonomous systems like UGV/UAV can not only upgrade the capability but they also enhance the benefits of WSNs.

As future works, we will implement an advanced classification scheme in a sensor node and experiment with a much larger testbed.

## 6. ACKNOWLEDGEMENT

This work was supported by the Daedeok Innopolis Project performed by the Korea Ministry of Knowledge Economy and the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MOST) (No. R0A-2007-000-10038-0)

## 7. REFERENCES

[1] D. Kim, T. S. Lopez, S. Yoo, J. Sung, J. Kim, Y. Kim, Y. Doh, "ANTS: An evolvable Network of Tiny Sensors",2005 IFIP International Conference on Embedded And Ubiquitous Computing (EUC-05), Nagasaki, Japan, December 2005

[2] Georg Wittenburg, Kirsten Terfloth, Freddy López Villafuerte, Tomasz Naumowicz, Hartmut Ritter, and Jochen Schiller. Fence Monitoring - Experimental Evaluation of a Use Case for Wireless Sensor Networks. In Proceedings of the 4th European Conference on Wireless Sensor Networks (EWSN'07), Delft, The Netherlands, January 2007

[3] Prabal Dutta, Mike Grimmer, Anish Arora, Steven Bibyk, and David Culler, “Design of a Wireless Sensor Network Platform for Detecting Rare, Random, and Ephemeral Events”, In The Fourth International Conference on Information Processing in Sensor Networks (IPSN'05), USA, 2005

[4] Lin Gu, Dong Jia, Pascal Vicaire, Ting Yan, Liqian Luo, Aajay Tirumala, Qing Cao, Tian He, John A. Stankovic, Tarek Abdelzaher, and Bruce Krogh, “Lightweight Detection and Classification for Wireless Sensor Networks in Realistic Environments”, In 3rd ACM Conference on Embedded Networked Sensor Systems (SenSys 2005), November 2005

[5] Panasonic Electric Works Corporation, http://pewa.panasonic.com/pcsd/product/sens/

[6] Panasonic Electrets Condenser Microphones, http://panasonic.com/industrial/components/pdf/em06_wm61_a_b_dne.pdf

[7] Geo Space Geophysical Instrumentation GS-20DX & DM Geophones, http://www.geospacelp.com/gs20dx.shtml

[8] Honeywell magnetic sensors HMC105X, http://www.ssec.honeywell.com/magnetic/datasheets/HMC105X.pdf

[9] Piezocable sensor, Piezolab Corp., http://piezolab.koreasme.com/

[10] Dusitech smart GPS, http://www.dusi.co.kr/

[11] Freya 90 EX helicopter Hirobo Corp., http://model.hirobo.co.jp/products/0404-988/0404-988-e.htm