IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 51-58
www.iosrjournals.org

Wireless Sensor Network Security in Military Application using Unmanned Vehicle

Arun Madhu[1], A. Sreekumar[2]
[1](Department of Computer Application, Cochin University of Science and Technology, India)
[2](Department of Computer Application, Cochin University of Science and Technology, India)

Abstract: *Wireless Sensor Network is widely used in Military Applications like Tracking the enemy movements and force protection. Security is the major concern and very difficult to achieve due to the unattended nature, limited memory, and limited power of network. This paper is mainly intended to describe the implementation of the secure unmanned Vehicle Navigation system controlled by wireless sensor network. We used a cluster based approach to prevent the various types of attacks in military field. We propose armed and sealed mote to prevent the physical attacks. In order to avoid a single key compromise lead to the entire network compromise we have proposed a modified version of LEAP for key management. The vehicle navigation was implemented using a toy car controlled by a micaz mote inside it. The GPS unit is connected with the vehicle to determine the position and in the absence of GPS range we can use the relative position. The vehicle can directly send the messages to the nearest sink node. The vehicle is used for making the application more secure and all the costly devices needed for the application can be incorporated with the vehicle. This paper shows how we can use the unmanned vehicle navigation system in Military applications and how it is used to detect the intruders and prevents various kinds of security attacks in the military field.*

Keywords: *vehicle; wireless sensor network security; gps; leap; cluster based routing; vehicle navigation.*

I. Introduction

This paper is mainly intended to implement a secure unmanned Vehicle Navigation system for military application using wireless sensor network. Wireless sensor networks are networks consisting of numerous small computers equipped with sensors [1, 2]. Various types of sensors are used to detect the different events. For example infrared sensors are used to detect events like human motion and thermistor sensor is used to determine the temperature [13]. These sensor nodes are equipped with a radio to communicate with each other and to send data to a central computer where this data can be parsed and viewed. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges [1,2]. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. The unreliable communication channel and unattended operation make the security defenses even harder.

Wireless sensor networks helps in military operations by delivering critical information rapidly and dependably to the right individual or organization at the right time, thereby significantly improving the efficiency of combat operations. Here we are using the wireless sensor network for monitoring and tracking application in military field. The security is a major concern in this application. First we list the set of applications in military field and what are the different types of attacks in this network. We will give the solutions for common types of attacks in military application. Various techniques are used to mislead the attacker from getting the information. The unmanned vehicle is incorporated in the military application to make the system more secure and improve the life time and connectivity of the network. The vehicle will be equipped with a mote controlling the vehicle based on base station commands and surrounding nodes data. The vehicles mote is like a driver of the vehicle. The driver mote has three different inputs at each stage. First the data from the sensors are connected to the mote and the second is the data from surrounding motes and the third is the data from base station. The mote will consider the three different inputs and will take an appropriate decision at each stage. The system can be used for monitoring application and protecting our military forces from intruders. We have proposed solutions for the major types of attacks in the military field. The unmanned vehicle can be used to check the reliability and integrity of the network.

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 51-58
www.iosrjournals.org

II. Military applications

Military security is a major application area of wireless sensor network. The major functions of the wireless sensor network is to monitor the enemy movements and coordinating the activities of the army. The motes will be deployed in the area we want to monitor as shown in fig.1 and a base station will be there to control the motes and to collect and process the information from various motes. The motes are connected with sensors to sense the environment for enemy movement detection and to coordinate the military activity at our side. The motes connected with sensors will look for particular events and give periodical messages to the base station. In case of suspicious activities the motes will immediately send messages to the base station. The base station will receive the information from various motes and will take the necessary action like informing the command in charge for that region or give messages to motes surrounding that area. The base station will be placed in a safe area and we can deploy the motes in the area we want to monitor without deploying army.

There are some limitations like power and low computation make us to make the network secure in the conventional ways like cryptography. So we have consider the case of an unmanned vehicle to make the system more secure. The costly sensors and other devices like camera can be attached with the vehicle. The vehicle will sense the data and sends it to the Base station directly. The Base station will receive the information from other sensor nodes and can control the vehicle movement inside the network. The vehicles contains a driver mote to receive the messages from surrounding motes and from the base station. It can be used to monitor movements on both sides. The military movements from our side can be very well coordinated by obtaining the information from driver mote. The enemy's movement information will help us to plan our next step. If the sensors send some important data about intrusion, then vehicle can be moved to that location for a detailed analysis.

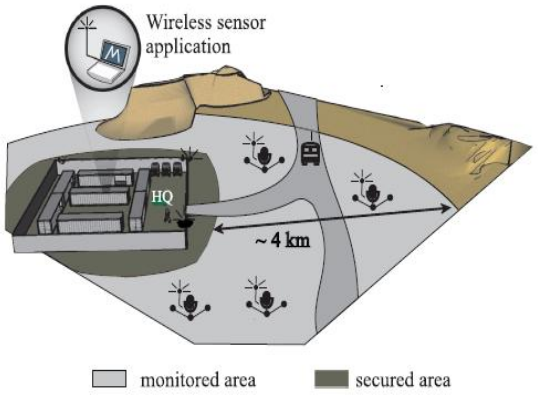

Figure 1. Wireless Sensor network based military monitoring [10].

III. Security Issues In Military Field

Security is a major concern in the military applications because if the intruder or compromised node gets the secret information it may be a passed to the opponent. The various types of attacks against the military application are listed below. The security cannot be assured by the conventional concepts in networking due to the limitations in wireless sensor network.

3.1 Denial of Service Attacks

A very common attack on wireless sensor networks is simply to jam a node or set of nodes by the intruder node. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network [13]. Another form of attack is a malicious node continuously transmit messages in an attempt to generate collisions. The intruder node can also drop some messages. The above attack will lead to retransmission of packets.

3.2 Sybil Attack

The Sybil attack done by an intruder mote or device taking on multiple identities"[13]. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks [13]. In military application a single malicious node can send data about a imaginary event multiple times as different entities. This will form a trust that the event has actually occurred. This node can confuse the whole network traffic and it is very difficult to identify.

3.3 Traffic Analysis Attacks

Wireless sensor networks in military application are typically composed of many low-power sensors communicating with a few relatively robust and powerful base stations [13]. If the enemies got information about the base station they can simply disable it and the whole network is useless. A rate monitoring attack simply makes use of the idea that nodes closest to the base station tend to forward more packets than those farther away from the base station. An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets. In a time correlation attack, an adversary simply generates events and monitors to whom a node sends its packets.

3.4 Node Replication Attacks

An attacker seeks to add a node to an existing sensor network by replicating the node ID of an existing sensor node [13]. This node can get the cryptographic keys and secret messages passing through the network. It can drop the packet and disconnect a section of the network from the whole network. If the enemy can introduce more number of this type of nodes they can control the whole network.

3.5 Attacks Against Privacy

Monitor and Eavesdropping is the most obvious attack to privacy. By listening to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which may contains location information's of the nodes in the network. If an adversary node gets this information it will use this information to estimate the position of critical areas. Through the analysis on the traffic, some sensors with special roles or activities can be effectively identified. Adversaries can insert their node or compromise the nodes to hide in the sensor network to get the secret information like a spy in military application.

3.6 Physical Attacks

Military sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions [13]. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker [13].

IV. Unmanned Vehicle to Protect Network

We are introducing the concept of unmanned vehicle controlled by wireless sensor network in Military application. This vehicle can navigate through the network and monitor the network security. The vehicle will be small and it will not get the enemy attention. The vehicle will be controlled by a mote inside it and if a particular event is reported from a area the vehicle can go and check whether the event is occurred. The vehicle node having unlimited power and we can do the maintenance of the vehicle. We can add other facilities like camera and other costly sensors in the vehicle. The importance of localization is to relate the vehicle location with local map or global map. If we are using GPS, we will get the global position with these position information and we can decide the next movement of the vehicle. The driver mote inside the vehicle will send the sensor information to the other motes. They will reply to the mote at the next movement.

The next part is to navigate the vehicle by using Location information and Neighbor mote communication. If we know the local map, we can give the full controls to the mote inside the vehicle i.e. mote can decide the movements and load the program based on the path. The next type of control is by neighbor mote communication in which the vehicle will know the path. The mote inside the vehicle will send the location information and the nearest neighbor will take the control of the vehicle. The implementation is done by using a toy car having five functions. The movement of the vehicle is based on the coordinate system. First the X direction gap will be moved and next the Y direction gap will be moved. The navigation can be controlled by base station also. The GPS is used to find the location of the vehicle. Based on the location, node will determine the next action.

The vehicle navigation system consists of a Vehicle, Driver mote, Base station mote, and Surrounding motes. The vehicle is the main part of the system. The selection of the vehicle will depend up on the application in which it is using. For military application a vehicle like a small tank can be used. For monitoring and maintenance application in a safe area small car can be used. The vehicle motion will be controlled by mote

placed inside the vehicle. The vehicle and mote will be connected through an interface card. The vehicle design in military field should be in such a way that it should be able to reach the entire battle field and should not be small enough to hide the presence. We need to place a driver mote within the vehicle and the driver mote will consider the messages from both surrounding motes and base station and will take appropriate actions. It also controls the devices and sensors connected with the vehicle and will send the valuable information's to the base station. The driver mote is having unlimited battery power and computational power like base station. It will collect the sensitive data and checks the credibility of data and if the data is very important it will encrypt the message using modern encryption technique and directly sends to the base station. The driver node will get the exact location of the vehicle from GPS connected with the mote. It moves to the next destination based on the program running in the driver mote. The mote is controlling the vehicle navigation. Apart from navigation, driver mote has other controls like deploying the motes and maintenance of the WSN network.

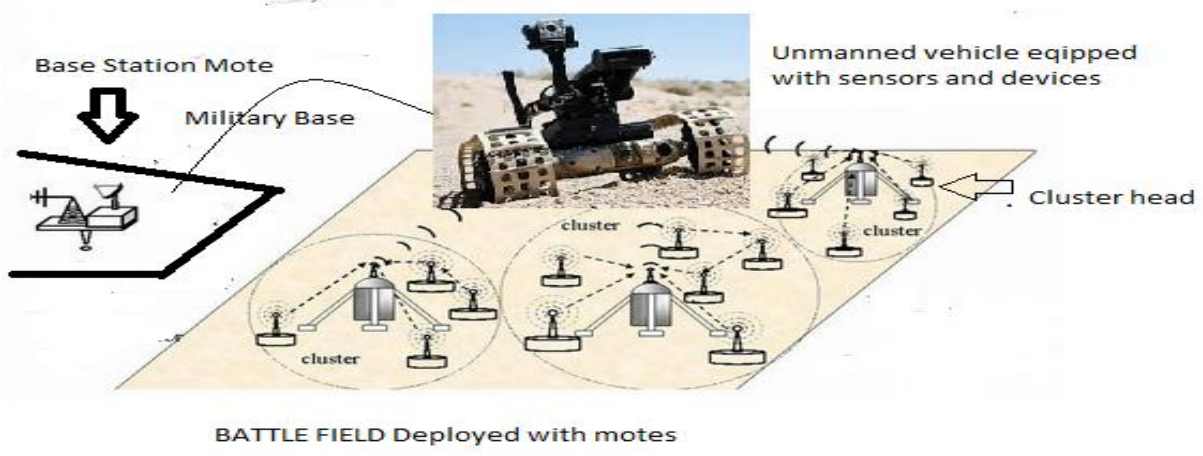

Figure 2. Unmanned vehicle to protect the battle field

V. Security Architecture

The security architecture proposed in this paper is to secure the wireless sensor network in military applications. The wireless sensor network is divided into clusters. Each cluster contains a set of motes in a particular area. The group will elect a cluster head. The cluster head will aggregate the messages from cluster members and the cluster head selection is based on remaining energy in the mote. The key management adopted in our paper is LEAP [25]. The Leap is having four sets of keys and we have taken two set of keys only from this Individual key and Cluster Key [26, 27]. The individual keys will be distributed to all the nodes before deploying by using that they can send encrypted messages to base station and the Vehicle driver mote. Only base station and Vehicle mote can only decrypt and read those messages. The cluster nodes in a cluster share a cluster key with in that cluster. The nodes will sense the environment and sensor readings will be encrypted by cluster key and send to the cluster head. The cluster Head will aggregate the messages and will encrypt with individual key will send to the base station through the network and will reach the base station. The base station will decrypt the messages from cluster head and will take appropriate actions. This is based on a threshold value and if the readings from the sensor is greater than that threshold the base station will judge it as an intrusion or attack has happened. In some cases if the base station take decision only on the basis of a cluster head information can lead to more problems. Sometimes a compromised node will send the false readings as a cluster head and can mislead the base station from the actual event. This is a serious issue and the unmanned vehicle in the network can solve this problem.

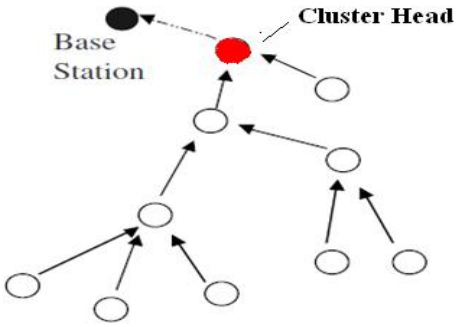

Figure 3. Data aggragation by Cluster head

The vehicle connected with sensors and powerful devices like camera and GPS can help the base station to take critical decisions. Consider the case that infrared sensor is attached with all the motes to detect the movements of enemies in our area. These nodes will send the messages to cluster head and cluster head will report this to the base station. Suppose the base station need to cross check whether the event is actually happened. It will move the unmanned vehicle to the region it is being reported and the vehicle will move to that area using gps or surrounding sensor location. The motes in that region will be connected with sensors and the sensors will collect data and sensitive information's will be passed to the driver mote. The driver mote will collect the data from the surrounding and it will immediately send the exact values to the base station immediately. The base station can then compare the values and if it is same it can take the appropriate actions like informing the military commander or activate the mines etc. The vehicle can be used to further examining the situation by using advanced devices like camera or other sensing devices. The base station and vehicle driver mote communication is direct and we can use conventional encryption techniques between them since both the nodes are powerful and unlimited battery life. We can use the vehicle movement to recharge the battery in the vehicle.

VI. Implementation Details

The entire application was implemented by using a remote controlled toy car which was connected to a micaz mote and the movements were controlled by mote using a interface card MDA 320 CA. The driver mote controlled by surrounding motes and base station was placed inside the vehicle. The coding is mainly in Nesc and it is implemented in Tiny Os operating system.

6.1 Hardware Implementation

The main parts are the vehicle, mote and interface part. In vehicle part, we used a car having four movements. The car was controlled by mote through interface card. The interface card and the mote are placed inside the car. There is a sensor board inside the vehicle in order to sense the changes in the vehicle surroundings. The car is having five functions. They are Forward, Reverse, Left, Right, and Stop. The main part of this circuit is the CAR transmitter circuit. In this circuit we will connect our mote. The mote interface is done through the MDA320CA board. The mote will generate the output based on the mote's program. Through MDA320CA interface board the signals will be passed to transmitter circuit. The main use of this transmitter circuit is to convert the signals from the mote to control signals for the car. For this purpose we are using an IC called TX-2B [22]. TX-2B is designed with five functions. The TX-2B/RX-2B is a pair of CMOS LSIs designed for remote controlled car applications. The TX-2B/RX-2B has five control keys for controlling the motions (i.e. forward, backward, rightward, leftward and the turbo function) of the remote controlled car. The TX2B is connected with the sensor and the sensor will control the switches. Based on the function, the corresponding switch will be enabled and transmitter will generate signals corresponding to each function. These signals are converted as radio signals and are send to the receiving part. Receiver circuit : In the receiver unit, first the signals are received and are given to the receiver. The receiver will do the corresponding actions. In the receiver part we will use RX2B IC as the receiver IC. The received signals are given to the IC. Corresponding to each signal there will be a function associated with RX2B. This IC is connected with the two motors.

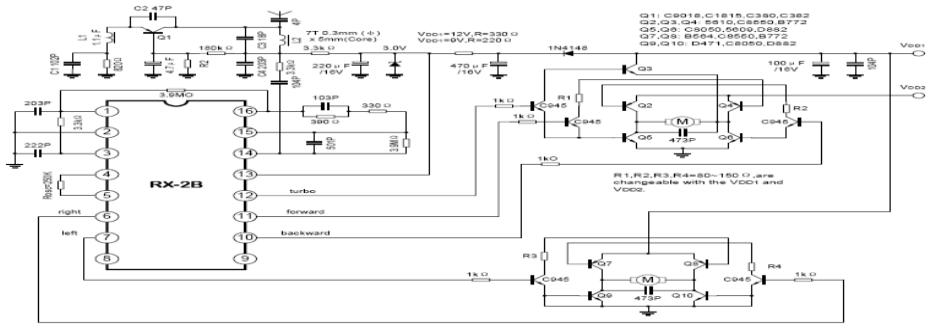

Figure 4. Transmitter circuit diagram of vehicle [22]

As shown in the figure 3 circuit diagram the forward and reverse pins are connected to the CD motor. The forward and backward functions will be based on the signal from the transmitter. The stepper motor will be connected to the right and left pin. The motes used in this implementation is MPR2400 (MICAz).

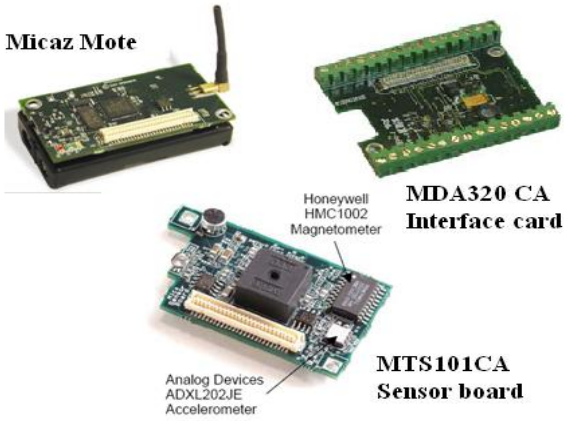

Figure 5. The Mote, Interface card and Sensorboard [User Manual].

The data acquisition board is used for the interface card between Mote and the vehicle transmitter unit. The MDA320CA is used as the interface card. Crossbow's MoteView software is designed to be the primary interface between a user and a deployed network of wireless sensors. The MTS101CA series sensor boards have a precision thermistor, a light sensor/ photocell, and general prototyping area. The sensing capabilities include light, temperature, microphone, buzzer, accelerometer and magnetometer.

6.2 Software Implementation

The Operating system used is TinyOS is an open-source event-driven "real-time" operating system designed by U.C. Berkeley. TinyOS is designed for use in low-power/limited resource applications which utilize wireless embedded sensor networks [23]. The programming of mote is done in a C-based language, known as nesC [21]. NesC program in driver mote is taking care of the messages from base station and surrounding motes and will decide the next movement or action. The driver mote is programmed to navigate the vehicle to a particular location. The surrounding motes are programmed to report the incidents in its premises. The base station is programmed to analyze the sensor data and give commands to driver mote. We have used the temperature as a parameter and programmed the motes. If the temperature value from a cluster head or node is more than a threshold the car will be moved to that region and sense the temperature and will give the report back to base station.

VII. Results

The vehicle controlled by wireless sensor network was implemented. The vehicle moved under the control of driver node attached with the vehicle. The driver node was controlled by the sensor readings from the sensors attached to it, surrounding nodes' reading and by the control of Base station nodes. The system shows 90 percentage accuracy on the location where the vehicle was planned to move. The vehicle was able to

crosscheck the fire detected by a node using temperature sensor and it was reported to the base station. The wireless sensor network worked as a unit for the successful navigation of the vehicle. The overall performance of the vehicle navigation system was satisfactory.

The Vehicle navigation system controlled by driver node can be implemented using GPS or GPS free localization algorithms. The comparison between these techniques are given in Table 1. The decision of which algorithm to use is taken based on the application in which the vehicle navigation algorithm is using. The comparative study based on accuracy of localization is done based on different algorithms. The GPS based algorithms are more accurate. We are using anchor free localization in our experimental study.

Table 1. Comparison of Vehicle Navigation Techniques

Vehicle Navigation		
Parameters	Using GPS	Not Using GPS
GPS Connectivity	Not usable in the absence of GPS	in Can be used in all locations
Cost	Costlier	Less Costlier
Accuracy	More Accurate	Less Accurate
Sensor Reading	No Reading from Sensors	Readings used in applications
Node Density	No influence	Directly proportional to accuracy

The graph shown in fig 6 is the Accuracy comparison based on connectivity of the nodes. As the connectivity of the nodes increases the Percentage location error decreases. So since the connectivity increases the location will be more accurate. It is very difficult to find whether a mote is compromised. We need to find the compromised nodes by cross checking the readings sent by the node with actual readings from the vehicle mote. If a node found compromised, the vehicle can destroy that mote. The Vehicle will be exploded if it is taken by an opposite military person. More the number of vehicles, the safer is our side. If more than one vehicle is there, we can divide the total area to regions and assign regions to vehicles. These vehicles can be used to detect mines and bombs. These vehicles can be used in battle field surveillance and detection of nuclear, Biological and chemical attack detection.

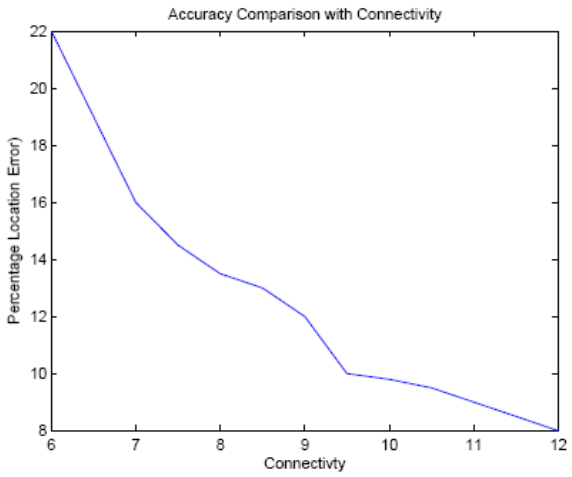

Figure 6. Wireless Sensor network based military monitoring.

VIII. Conclusion

The wireless sensor network is an emerging technology. The work we have done resulted in a Vehicle navigation system controlled by wireless sensor network to make the network more secure and useful. The system can be used in various applications such as monitoring and maintenance and fire detection. If the vehicle

is equipped with GPS, the exact location can be determined. The implementation was done on a small car with five functions. We can enhance this system to add more features to the vehicle.

Acknowledgment

I would like to express my sincere thanks to professor Dr. Sreekumar, Department of Computer Application, Cochin University for his continued support and guidance towards the concept. I would also like to express my sincere thanks to professor Dr. K P Soman, HOD, CEN, Amrita University for giving the initial thoughts and experimental setup in his lab.

References

[1]. Tufan Coskun Karalar. Implementation of a Localization System for Sensor Networks, University of California, Berkeley 2002.
[2]. Guoqiang Mao, Barýs¸ Fidan and Brian D.O. Anderson. Wireless Sensor Network Localization Techniques. In 2003.
[3]. N. B. Priyantha, H. Balakrishnan, E. Demaine, and S. Teller, "Anchorfree distributed localization in sensor networks," in ACM 2003.
[4]. S. Capkun, M. Hamdi, and J.-P. Hubauz, "Gps-free positioning in mobile ad hoc networks," in Hawai International Conference on System Sciences, 2001.
[5]. Connelly, R. Rigidity. In Handbook of Convex Geometry, vol. A. North-Holland, Amsterdam, 1993, pp. 223–271.
[6]. Crippen, G., And Havel, T. Distance Geometry and Molecular Conformation. John Wiley & Sons, 1988.
[7]. Doherty, L., Pister, K., And Ghaoui, L. Convex position estimation in wireless sensor networks. In Proc. IEEE INFOCOM (April 2001).
[8]. Fruchterman, T., And Reingold, E. Graph Drawing by Force-directed Placement. Software - Practice and Experience (SPE) 21, 11 (November 1991), 1129–1164.
[9]. Graver, J., Servatius, B., And Servatius, H. Combinatorial Rigidity. American Mathematical Society, 1993. University of California, Berkeley, 2002.
[10]. Guoqiang Mao, Bars Fidan and Brian Anderson.Wireless Sensor Network Localization Techniques, 2003.
[11]. Jeonghoon Kang , Jongmin Hyun, Dongik Kim, Kooklae, Pil Mhan Jeong, Taejoon Choi and Sukun Kim. Tracking Vehicles in a Container Terminal, In SenSys'11, November 2011.
[12]. P Santi. Topology Control inWireless Ad Hoc and Sensor Networks, In Wiley, 2005.
[13]. Lynch J P. Overview of Wireless Sensors for Real-time Health Monitoring of Civil Structures, In Proceedings of the 4th International Workshop on Structural Control, 2004.
[14]. Javed Aslam, Zack Butler, Florin Constantin, Valentino Crespi, George Cybenko, and Daniela Rus. Tracking a moving object with a binary sensor network, In ACM Confer ence on Embedded Networked Sensor Systems, November 2003.
[15]. Adrian Perrig, John Stankovic and David Wagner. Security in wireless sensor networks, In ACM Communication, 2004.
[16]. B Sinopoli, C Sharp, L Schenato, S Shaffert, Sh S Sastry. Distributed control applications within sensor networks, In Proceedings of the IEEE, August 2003.
[17]. A Mainwaring, J Polastre, R Szewczyk, D Culler and J Anderson. Wireless Sensor Networks for Habitat Monitoring, In Proceedings of WSNA, 2002.
[18]. Joo Valente, David Sanz, Antonio Barrientos, Jaime del Cerro, ngela Ribeiro and Claudio Rossi. An Air-Ground Wireless Sensor Network for Crop Monitoring, In Sensors, 2011.
[19]. M Healy, T Newe, E Lewis. Wireless sensor node hardware: A review, In 7th IEEE Con- ference on Sensors, 2008.
[20]. Michael Johnson, Michael Healy, Pepijn van de Ven, Martin J Hayes, John Nelson, Thomas Newe and Elfed Lewis. A Comparative Review of Wireless Sensor Network Mote Technologies, In IEEE SENSORS Conference, 2009.
[21]. David Gay, Philip Levis, Robert von Behren, Matt Welsh, Eric Brewer and David Culler. The nesC Language: A Holistic Approach to Networked Embedded Systems, 2007.
[22]. TX2B/RX2B, Toy Car Remote Controller With Five Functions, Hangzhou Silan Microelectronics, 2005.
[23]. TinyOS 2007, http://www.tinyos.net.
[24]. HPI Racing High Performance R/C Car Products, http://hpiracing.com/products/en/10001.html.
[25]. R. Blom. An optimal class of symmetric key generation systems. In Advances in Cryptology, Proceedings of EUROCRYPT'84. LNCS 209. 335–338. 1995
[26]. D. Carman, P. Kruus and B. Matt, Constraints and approaches for distributed sensor network security, NAI Labs Technical Report No. 00010 (2000).
[27]. L. Eschenauer and V. Gligor. A Key-Management Scheme for Distributed Sensor Networks. In Proc. of ACM CCS 2002