Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 7 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks (WSN)

By Srinivasaraju Dantuluri & P. Poturaju

Grandhi Varalakshmi Venkatarao Institute of Technology, Tundurru

Abstract - Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a combat zone. The intrusion detection is defined as machinery for a WSN to detect the subsistence of unfortunate, incorrect, or anomalous moving attackers. For this purpose, it is a fundamental issue to differentiate the WSN parameters such as node density and sensing range in terms of a desirable detection probability. In this paper, we consider this issue according to two WSN models: homogeneous and heterogeneous WSN. Furthermore, we derive the detection possibility by considering two sensing models: single-singing detection and multiple-sensing detection. In addition, we converse the network connectivity and broadcast reach ability, which are necessary conditions to make certain the corresponding detection probability in a WSN. Our simulation results validate the analytical values for both homogeneous and heterogeneous WSNs.

Keywords : intrusion detection, node density, node heterogeneity, sensing range, wireless sensor network (WSN).

GJCST-E Classification : C.2.1

Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks (WSN)

Srinivasaraju Dantuluri [α] & P. Poturaju [σ]

Abstract - Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a combat zone. The intrusion detection is defined as machinery for a WSN to detect the subsistence of unfortunate, incorrect, or anomalous moving attackers. For this purpose, it is a fundamental issue to differentiate the WSN parameters such as node density and sensing range in terms of a desirable detection probability. In this paper, we consider this issue according to two WSN models: homogeneous and heterogeneous WSN. Furthermore, we derive the detection possibility by considering two sensing models: single-singing detection and multiple-sensing detection. In addition, we converse the network connectivity and broadcast reach ability, which are necessary conditions to make certain the corresponding detection probability in a WSN. Our simulation results validate the analytical values for both homogeneous and heterogeneous WSNs.

Keywords : intrusion detection, node density, node heterogeneity, sensing range, wireless sensor network (WSN).

I. Introduction

An Intrusion detection system (IDS) is designed to detect unwanted attempts at accessing, disabling of computer mainly through a network, such as the Internet. Intrusion detection plays a key role in the vicinity of network security, so an attempt to apply the idea in WSNs makes a lot of sense. Intrusion, i.e. unconstitutional access or login (to the system, or the network or other resources); intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability and authenticity) of a network's resource.

There are two approaches: misuse detection and anomaly detection. Misuse detection identifies an unauthorized use from signatures while anomaly detection identifies from analysis of an event. When both Techniques detect violation; they raise an alarm signal to warn the system. Wang divides intrusion detection techniques into single - sensing detection and Multi - sensing detection. In single-sensing detection, the intruder can be successfully detected by one sensor. While in multi-sensing detection, multiple collaborating sensors are used to detect the intrusion.

A wireless sensor network (WSN) is a type of wireless network consist of small nodes with capabilities of sensing physical or environmental conditions, processing related data and send information wirelessly. 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. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control. The sensor nodes are tiny and limited in power. Sensor types vary according to the application of WSN. Whatever be the application, the resources such as power, memory and bandwidth are limited. Moreover, most of the sensors nodes are throw away in nature.

Early study on wireless sensor networks mainly focused on technologies based on the homogeneous wireless sensor network in which all nodes have same system resource. However, heterogeneous wireless sensor network is becoming more and more popular recently. And the results of researches show that heterogeneous nodes can prolong network lifetime and improve network reliability without significantly increasing the cost. A typical heterogeneous wireless sensor networks consists of a large number of normal nodes and a few heterogeneous nodes. The normal node, whose main tasks are to sense and issue data report, is inexpensive and source-constrained.

II. Related Work

With respect to security, there are many tools that are used to ensure security in ID systems. The IDSs are very important tools since they can detect intrusions in networks. Many techniques that are result of research

Author α : M.Tech (CSE), Department of CSE, Grandhi Varalakshmi Venkatarao Institute of Technology, Tundurru, Bhimavaram, Affiliated to JNTUK. E-mail : srinivasarajud@gmail.com

Author σ : Assistant Professor, Department of CSE, Grandhi Varalakshmi Venkatarao Institute of Technology, Tundurru, Bhimavaram, Affiliated to JNTUK. E-mail : poturaju.gvit@gmail.com

are pertaining to network security in general. They are developed for the nodes that have lot of resources in place. For this reason they can't be directly applied to WSN. That led to further research in the area of WSN for modifying techniques or inventing new ones that are best suited for WSN where nodes are energy constrained. Among the researchers on WSN Zhang and Lee [1] are first in researching on security issues of Ad hoc networks. Their IDS which is distributed in nature works based on the detection techniques of statistical anomaly. This technique assumes much traffic and the time taken for detection of intrusion is high and thus not efficient. The cost of this model can't be afforded by any WSN.

At times intruders might be moving and detecting such intruder is also important in WSN. This has attracted research in this domain. When nodes are in transit, the mechanisms and techniques are to be altered. The moving objects, their direction and probability of intrusion, detection etc. are to be considered. The intrusion detection in this environment also has to be considering energy efficient approaches. Most of the research that has been done in this area focuses on detection of intrusions under assumptions and criteria. The sensor coverage and sensing capabilities for detection of intrusions has effect are impacted by mobility according to Liu et al. [9]. His work demonstrated with the mobility of sensor increases the coverage of network and provides fast detection of intrusions and targeted events. Sensing models are of two types. They are single sensing model and multi sensing model. Intrusion detection process in these two models is explored by Wang et al. [13].

In his work, the combination of detection probability and network Parameters such as transmission range, sensing range, and node density are considered for experiments under single sensing models. A security management model is proposed by [15] where intrusion detection in WSN assumes that the nodes in the network are self organizing and the model is based on the layers in network. The cryptography used by WSN can only prevent external attacks while it can't do it with already compromised nodes.

Heterogeneous WSN

A heterogeneous wireless sensor network (WSN) consists of several different types of sensor nodes (SNs). Various applications supporting different tasks, e.g., event detection, localization, and monitoring may run on these specialized sensor nodes. In addition, new applications have to be deployed as well as new configurations and bug fixes have to be applied during the lifetime. In a network with thousands of nodes, this is a very complex task. A heterogeneous node has more complex processor and memory so that they can perform sophisticated tasks compared to a normal node. A heterogeneous node possesses high bandwidth and long distant transceiver than a normal node proving reliable transmission.

a) Types of Heterogeneous Resources

There are three common types of resource heterogeneity in sensor node:

i. *Computational Heterogeneity*

Computational heterogeneity means that the heterogeneous node has a more powerful micro-processor and more memory than the normal node. With the powerful computational resources, the heterogeneous nodes can provide complex data processing and longer term storage.

ii. *Heterogeneity*

Link heterogeneity means that the heterogeneous node has high bandwidth and long-distance network transceiver than the normal node. It can provide more reliable data transmission.

iii. *Energy Heterogeneity*

Energy heterogeneity means that the heterogeneous node is line powered, or its battery is replaceable.

Among above three types of resource heterogeneity, the most important heterogeneity is the energy heterogeneity because both computational heterogeneity and link heterogeneity will consume more energy resource. If there is no energy heterogeneity, computational heterogeneity and link heterogeneity will bring negative impact to the whole sensor network, i.e., decreasing the network lifetime.

A heterogeneous node is line powered (its battery is replaceable).The heterogeneous WSN consists of different types of sensors with different sensing and transmission range. So while selecting the sensor nodes for intrusion detection, we need to consider these inequality of sensing and transmission range. For example, if two nodes have different transmission range it is better to select the one whose transmission range is higher. In this paper, we are considering N types of sensors. Here the sensing range and transmission range is high for Type 1 compared to Type2 and so on. The sensors are uniformly and independently deployed in an area A = LxL.

III. Contribution

Here we have developed an algorithm which helps the WSN in detecting the intruder with energy efficiency and thereby increasing the life time of the network .Moreover, we have carried out the probability analysis for intrusion detection. Two things are considered in this work.

- Energy consumed for the intrusion detection process.
- Whether this technique can be used for both external and internal intrusion detection.

The algorithm is developed by keeping these two things in our mind. We cannot separate internal and external intrusion detection as separate fields because most of the applications need both in the network. The internal intrusion detection includes the analysis of data send by each node. The algorithm proposed by us can be used for internal data analysis. This algorithm selects a set of nodes among the entire nodes and activates its IDS module.

IV. Problem Definition

The life span of wireless sensor network directly depends on the power. The power required to transfer a data from sensor is more compared to its internal processing. All sensors are performing the intrusion detection and passing this information to base station may cause unnecessary usage of power. It is better to activate only few sensors within a region of WSN at a time for intrusion detection. So in the case of intrusion detection, if we are able to save battery power of each sensor, then it is very easy to increase the WSN life span. In this paper, we are proposing a new technique of energy efficient Intrusion detection, which will maximize the network life time, and its probability analysis.

V. Assumptions

The sensors we are considering here are static sensors. The intruder is considered as a moving object. Each node has Omni antenna properties for sensing. The sink node knows each nodes location and its neighbour list. The algorithm is executed at the sink node and it sends packet to the selected nodes to activate its IDS module. Such a random deployment results in a 2D Poisson point distribution of sensors. A sensor can only sense the intruder within its sensing coverage area that is a disk with radius as centred at the sensor.

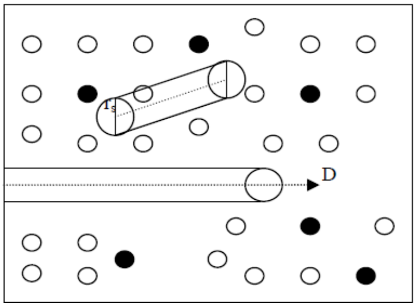

Figure 1 : Area moved by intruder

Consider figure 1, here the intruder is coming from the boundary and the distance moved by the intruder is D, the intruder is detected only when there is any sensor in the area moved by the intruder. In this paper we are considering only straight path. Figure 1 show the case when the intruder enters from the boundary. Here the area moved by the intruder

$$S=2*D*r_s+ \Pi r_s^2/2 \tag{1}$$

If the intruder is entering the WSN area from a random point, i.e. , the intruder is dropped from the air, then the area moved by the intruder is also shown in figure 1. This area is given by

$$S=2*D*rs+\Pi r_s^2 \tag{2}$$

a) Algorithm

The algorithm for node selection trying to select the high capacity nodes compared to other one. High capacity means large sensing range and transmission range.

```
Si- set of type i sensors in the WSN area.
S- Set of all sensors
N (a) - Set of neighbours of node a
Repeat
For i=1 to N
        Select node a with min N (a) in set Si
        If N (a) $\neq\emptyset$
        Select a
        SN = {j/ the distance between a and
N (a) < ($r_{si}$ /2)}
        If |SN|>1
                        S=S-(SN U a)
Else
        S=S-a
Until S is null se
```

The algorithm select a certain set of nodes that cover the entire area based on type of node, its transmission range and sensing range.

b) Single sensing detection model

As we explained before, the intruder is detected only when it enters the sensing range of any one sensor nodes. When the intruder enters the area through the boundary and the boundary is covered by the sensors, then the intruder will be detected as soon as it enters the WSN area. Otherwise it has to move a certain distance D before detected by any of the sensors.

Theorem 1

The probability P (D) that an intruder can be immediately detected once it enters a heterogeneous WSN can be given by

$$p(D=0)=1-\prod_{i=1}^{N} e^{-n_i}$$

Where n_i is the number of type i nodes activated in the area $\Pi r_{si}^2/2$.

Proof:

Here the area we need to consider when the intruder enters from the boundary is $A_1= (\pi\ r_{s1}^2)/2$, $A_2= (\pi r_{s2}^2)/2$, $AN=\pi r_s N^2/2$ as shown in figure 2. So P (0, A1), P (0, A_2)….P (0, AN) gives the probability that there is no Type 1, Type 2 type N sensors in that area. The probability that neither type 1 nor type 2….nor type N are given P (0, A1) P (0, A2)…..P (0.A_N) =1-$e^{-n1}e^{-n2}$…e^{-nN} where n1, n2, nun are the number of selected nodes from each type. So the probability of detecting the intruder when it enters the boundary is given by complement of P (0, A1) P (0, A_2)….P (0, AN) =1-$e^{-n1}e^{-n2}$….e^{-nN}.

Theorem 2

Suppose η is the maximal intrusion distance allowable for a given application, the probability P(D) that the intruder can be detected within η in the given heterogeneous WSN can be derived as

$$p(D <= \eta) = 1 - \prod_{i=0}^{N} e^{-n_i} ,$$

Where n_i is the number of sensors participating in intrusion detection area A_i= 2**η**$r_{si + (1/2)}$ πrsi2.

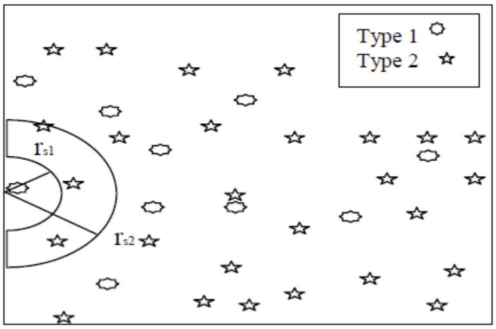

Figure 2 : The area covered by sensors at the boundary

Proof: This can be proved just like above theorem

(c) Multi sensing detection model

Multi sensing in a heterogeneous WSN is explained in figure 3. Here multiple sensors have to detect a intruder at the same time. Three sensors are considered. The intruder is within sensing range of three sensors. In the k-sensing detection model of a heterogeneous WSN with types of sensors, at least k sensors are required to detect an intruder. These k sensors can be any combination of any type of sensors.

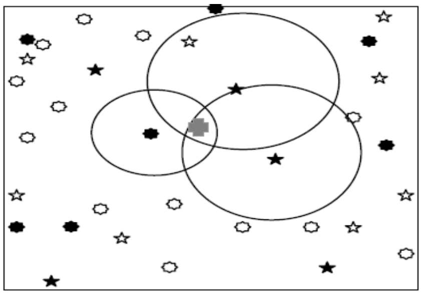

Figure 3 : Multi Sensing

Let P_m (D=0) be the probability that an intruder is detected immediately once it enters a WSN in multi sensing detection model.

$$Pm\ (D=0) = 1 - \prod_{j=1}^{N} \sum_{i=0}^{m-1} P(i, Aj)$$

Where A_j is the area covered by type j sensor and we are assuming that n_j of type j sensors are activated in the area A_j.

Proof:

This theorem can be proved just like above theorems. Here the area is only one half circles with radius r_s...P (i,A) gives the probability of detecting the intruder with i sensors.

$\sum_{i=0}^{m-1} P(i, A)$ gives the sum of the probabilities of detecting the intruder with less than m sensors. So the complement will give the multi sensing probability.

VI. Simulation and Verification

The simulation considers two types of nodes. Here in order to get the result we are varying the parameters such as sensing range, transmission range, number of sensors etc. The sensors are uniformly distributed in a two dimensional space of 1000*1000 meters. The sensing range is varied from 0 to 50 meters and maximal allowable intrusion distance is 50 meters. The graph shows the detection probability. It is found that the detection probability remains same as in the case of analytical results, thus proving the correctness of the analytical model. The fig 4 shows Single-Sensing detection. It is evident that the single sensing detection probability is higher than that of multi sensing detection probability.

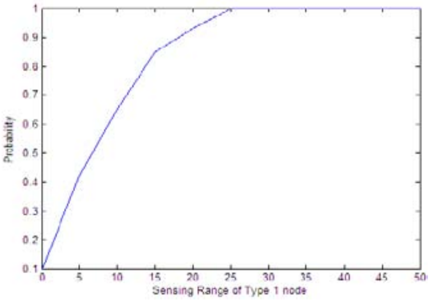

Figure 4 : Probability Analysis

This is because the multi-sensing detection imposes a stricter requirement on detecting the intruder (e.g., at least 3 sensors are required).

Type 1 node: Here the graph is obtained by changing the sensing range from 0 to 40. The each point in the graph is a result of 100 simulations. That is to get each point we need to execute our simulation and find out the probability from the result of this 100 executions. Here we can see that single sensing is possible at lower ranges also. But for multi sensing it will take a little time to get the result. Because needs the more than one sensor (here, in this simulation 3 sensor information) information to detect the intruder. Fig. 5 demonstrates the average number of nodes selected by using this algorithm specified above. The density of type 1 nodes is varied to check how many nodes are activating its IDS module. Here the simulation is done by fixing the number of Type 2 sensors to 300. The sensing range and transmission range are set to 30. The sensing and transmission range of Type 1 is set to 45. The numbers of type 1 nodes are varied in each execution and find out how it will affect the selection process.

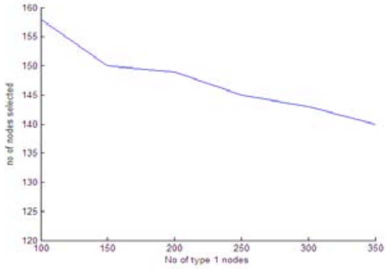

Figure 5 : Number of Nodes Selected

The energy used by this algorithm is analyzed in the figure 6 given below. Here we compared our paper with the base paper. We assumed that the energy used by one node for a unit time is one unit. The graph clearly shows the energy efficiency.

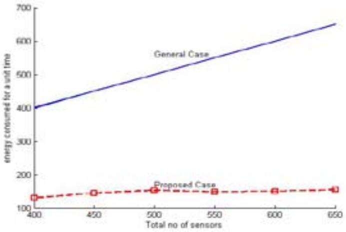

Figure 6 : Energy Used

a) Verification for Network Connectivity and Broadcast Reach Ability

In this part, we verify our analysis on the network connectivity and broadcast Reach ability. The analytical results shown in Figs.7 and 8 are calculated by using Theorems1 &2.In the simulation, an adjacency matrix is constructed to represent the digraph of the network topology.

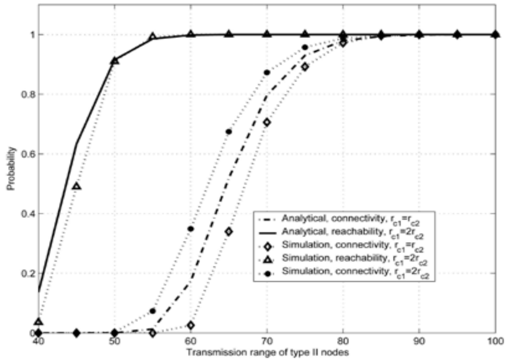

Figure 7 : Effects of transmission range on the broadcast reach ability in heterogeneous WSN

The depth-first-search algorithm is employed to check the network connectivity by selecting a random sensor as the starting node and the broadcast Reach ability by choosing a random Type I sensor as the broadcast initiator. The simulation considers 200 Type I sensors and 300 Type II sensors. In the homogeneous WSN, the transmission range of Type I sensors is set equally to that of Type II sensor (i.e., rx1 ¼ rx2). The transmission range of Type II sensor rx2 is varied from 40 meters to 100 meters in both homogeneous and heterogeneous case.

Broadcast reach ability is equivalent to the network connectivity since there are no asymmetric links. Next, the simulation is carried out to see the effect of Type I sensors on the network connectivity and broadcast reach ability. We fix the number of Type II sensors as n2¼300 and vary the number of Type I sensors from 10 to 300. The transmission ranges are set as rx1 ¼ 140 meters and rx2 ¼ 70 meters for Type I and Type II sensors, respectively.

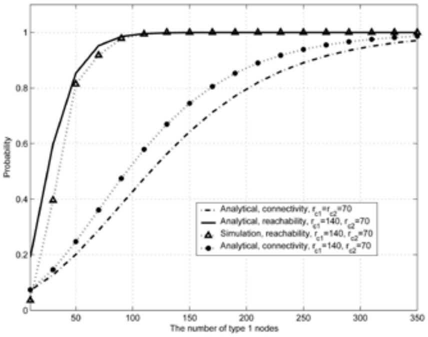

Figure 8 : Effects of Type I sensors on the broadcast Reach ability in heterogeneous WSN

We compare the results in homogeneous WSN with that in heterogeneous WSN by reducing Type I sensors to Type II sensors. Fig. 8 shows the analytical and simulation results, and they match with each other closely. From the figure, network connectivity and broadcast reach ability are improved while increasing Type I sensors. This is because some sensors that are originally isolated or unreachable from the rest of the network are now connected or reachable in the network after the introduction of Type I sensors. In addition, the results indicate that even a small increase of Type I sensor significantly improves the broadcast reach ability, while network connectivity only improves gradually. This also implies that the node heterogeneity does affect the broadcast reach ability much more dramatically than it does to the network connectivity.

VII. Conclusion

This paper analyzes the intrusion detection problem in both homogeneous and heterogeneous WSNs by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range). Two detection models are considered: single-sensing detection and multiple-sensing detection models. The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios. Moreover, we consider the network connectivity and the broadcast reach ability in a heterogeneous WSN.

Our simulation results verify the correctness of the proposed analytical model. This work provides insights in designing homogeneous and heterogeneous WSNs and helps in selecting critical network parameters so as to meet the application requirements.

Acknowledgement

I would like to express my sincere thanks to my guide and my authors for their consistence support and valuable suggestions.

References Références Referencias

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, vol. 40, no. 8, pp. 102-14, Aug. 2002.
2. Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2004)
3. Hu, W., Chou, C.T., Jha, S. and Bulusu, N.: Deploying Long-Lived and Cost-effective Hybrid Sensor Networks. Elsevier Ad- Hoc Networks, Vol. 4, Issue 6. (2006) 749-767.
4. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks.
5. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Commun-ications, vol. 3, Montreal, Canada, August 2005, pp. 253–259.
6. A. Perrig, et al., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, 8(5):521-534, Sep. 2002.
7. S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03), Oct. 2003.
8. J. Deng, R. Han and S. Mishra, "A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks", Proc. of the 2nd Int. IEEE Workshop on Information Processing in Sensor Networks (IPSN'03), Apr. 2003.
9. Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.
10. O. Dousse, C. Tavoularis and P. Thiran, "Delay of intrusion detection in wireless sensor networks," in Proceedings of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2006.
11. H. Kung and D. Vlah, "Efficient location tracking using sensor networks," in IEEE Wireless Communications and Networking Conference, ser. 3, vol. 3, March 2003, pp. 1954–1961.
12. C.-Y. Lin, W.-C. Pang and Y.-C. Tseng, "Efficient in-network moving object tracking in wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 5, no. 8, pp. 1044– 1056, 2006.
13. Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad-Hoc Networks. In Proc. ACM MobiCom, pages 275-283, 2000.
14. B. Liu, P. Brass, O. Dousse, P. Nain and D. Towsley, "Mobility improves coverage of sensor networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.
15. Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks" IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.
16. Yun Wang, Yoon Kah Leow, and Jun Yin, "Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks," in 15th International Conference on Parallel and Distributed Systems, 2009.
17. Xi Peng, Zheng Wu, Debao Xiao, Yang Yu, "Study on Security Management Architecture for Sensor Network based on Intrusion Detection," in 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing 2009.
18. P. Brutch and C. Ko. Challenges in intrusion detection for wireless ad-hoc networks. In 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), 2003.
19. Byunggil Lee, Seungjo Bae and Dong Won Han, "Design of network management platform and security frame work for WSN", IEEE International conference on signal image technology and internet based system, 2008.
20. Qi Wang, Shu Wang, "Applying an Intrusion detection algorithm to wireless sensor networks", Second international workshop on Knowledge Discovery and Data Mining, 2009.