Intrusion Detection: A Probability Model for 3D Heterogeneous WSN

Mohamed Mubarak.T
Royal College of Engineering,
Department of Computer Science,
Trichur,Kerala,India

Syed Abdul Sattar
RITS,
Hyderabad,
India

Appa Rao
GIT,
GITAM University,
India

Sajitha M
MES CE,
Kuttippuram,
India

ABSTRACT
WSN in three dimensional space is common in different application areas such as space monitoring, cave monitoring under water eco system and so on. Intrusion is a common type of attack in such types of networks. In this paper, we analyze the intrusion detection probability which helps in deploying the sensors in efficient manner. Even though the sensors are throw away in nature, still the cost matters. And the intelligent deployment helps in reducing the redundancy in communication. Therefore this model can be beneficial in case of three dimensional WSN.Here we deal with heterogeneous WSN as such types of WSN are common in different applications. For the case of simplicity, in our analysis, we consider only two types of sensors named as Type 1 and Type 2. This model can be extended to any number of types. This paper is an extension of our previous work where intrusion detection on homogeneous networks was discussed.

General Terms
Wireless sensor networks, security, internal and external intrusion detection.

Keywords
Intrusion detection, node density, sensing range, Wireless Sensor Network (WSN).

1. INTRODUCTION
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[1]. 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 in WSNs are usually static after deployment, and communicate mainly through broadcast instead of point-to-point communication. Sensors are deployed in a variety of domains and some application should be secure from all types of attacks. A lot of security protocols or mechanisms have been designed for sensor networks. For example, SPINS (Sensor Protocol for Information via Negotiation), a set of protocols, provides secure data confidentiality, two-party data authentication, and data freshness and authenticated broadcast for sensor network [2]. LEAP (Localized Encryption and Authentication Protocol), is designed to support in-network processing bases on the different security requirements for different types of messages exchange [3]. INSENS is an intrusion tolerant routing protocol for wireless sensor networks [4]. In general, security solutions in the network can be divided into two categories: prevention and detection. Prevention techniques, such as encryption, authentication, firewalls, in WSNs, physical links may always be invaded, therefore, Prevention techniques seem to be relatively weak. In this case, Intrusion detection can become the second line of defense in WSNs; especially for those networks that require a relatively long lifetime, intrusion detection is especially necessary. According to the experiences in research on security issues, no matter how many safety precautions are physical isolation, as the first line of defence, are usually to prevent attacks from outside. The goal of intrusion detection is that when preventive measures fail, WSNs can identify and resist the attacks by means of intrusion detection techniques. Intrusion detection systems (IDSs) are an important tool for the security of networks. Although, there have existed several intrusion detection techniques in wired networks, they are not suitable for WSNs and cannot transfer directly to WSNs. Therefore, these techniques must be modified or new techniques must be developed to make IDSs work well in WSNs. It is defined as a monitoring system for detecting any malicious intruder that is invading the network domain [5], [6],7], [8]. For this purpose, a number of sensors, N, are deployed in an area of interest, A, to monitor the environmental changes by using optical, mechanical, acoustic, thermal, RF and magnetic sensing modalities . In this way, possible intruder approaching or traveling inside the deployment field can be detected by the WSN if it enters into the sensing range(s) of one or multiple sensor.

A wireless sensor network consists of a large set of inexpensive sensor nodes with wireless communication interface. These sensor nodes have limited processing and computing resources. We are interested in wireless sensor networks which are used to detect intrusion objects such as enemy tanks, cars etc. But this problem has not been studied extensively in three dimensional space in WSNs because of its complexity reasons.However, in some real world application scenario the deployed sensor network operates over a three dimensional area rather than in a two dimensional area. Deployment of WSNs for surveillance of terrains, study of underwater ecosystem, space monitoring and exploration, etc is examples of such applications. But, so far only

a few researchers have addressed the problem of intrusion detection for these 3D scenarios.

WSN have many applications. However, in many scenarios WSNs are vulnerable to be attacked by adversaries as they are deployed in open and exposed environments and are constituted of cheap small devices and are power limited. Intrusion is one of the main attacks in WSN. So it is essential to device some mechanism to handle such types of attacks. The high density deployment in WSN helps to detect the intruder as soon as it enters the network as the union of all the sensing ranges covers the entire area of deployment.However,this policy cannot be practically applied in the systems because of the cost requirements. In fact, it is not necessary to deploy so many sensors to cover the entire WSN area in many applications , since a network with small and scattered void areas will also be able to detect a moving intruder within a certain intrusion distance. In this case, the application can specify a required intrusion distance within which the intruder should be detected. As shown in Fig. 1, the intrusion distance is referred as D and defined as the distance between the point the intruder enters the WSN , and the point the intruder is detected by the WSN system.

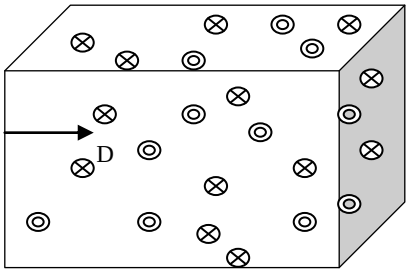

Figure 1. Distance moved by intruder

Intrusion detection is analyzed in two scenarios: single sensing detection and multiple sensing detection .In single sensing detection the intruder is detected by a single sensor. But at least three sensors should detect the intruder in a collaborative manner to find out the exact location of the Intruder. Therefore we have analyzed the multiple sensing detection too. We derive the expected intrusion distance and evaluate the detection probability in different application scenarios. Given a maximal allowable intrusion distance Dmax = η, we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range. For example, given an expected detection distance E(D), we can derive the node density with respect to sensor's sensing range. In this paper, we derive the expected intrusion distance and evaluate the detection probability in different application scenarios.

2. RELATED WORKS

There exist several tools for security in networks and IDSs are important tools. Many solutions have been proposed in traditional networks but it cannot be applied directly to WSN because the resources of sensor nodes are restricted . Ad-hoc and WSNs security has been studied in a number of proposals. Zhang and Lee [9] are among the first to study the problem of intrusion detection in wireless Ad-hoc networks. They proposed architecture for a distributed and cooperative intrusion detection system for Ad-hoc networks; their scheme was based on statistical anomaly detection techniques. But the scheme need much time, data and traffic to detect intrusion. In WSNs, the nodes can not afford the cost.

Detecting a moving intruder is a crucial application in wireless sensor networks, thus, attracting considerable research attention in the literature. Intrusion detection is defined as the first contact time when the intruder hits the sensing range of a sensor belonging to the large sensor cluster. To date, most of the existing work focus on the problem of network configuration for efficiently detecting the intruder within a pre-specified time threshold, under the constraints of tight power saving and/or cost efficiency. Liu et al. [10] have explored the effects of sensor mobility on sensing coverage and detection capability in a mobile WSN. It is demonstrated that sensor mobility can improve the sensing coverage of the network, and provide fast detection of targeted events.

Wang et al. [5] have provided a unifying approach in relating the intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range and transmission range), under single-sensing detection and multiple-sensing detection models, in both homogeneous and heterogeneous WSNs. A straight line or linear motion intrusion path is assumed for an intruder.An intruder can attack the network following a curved path or even a random walk in order to improve its attacking probability. Yun Wang, Yoon Kah Leow, and Jun Yin[11] have provided an approach where the intruder takes a curved path. They propose a novel Sine-curve mobility model to explore the effects of different intrusion paths on the intrusion detection probability using single-sensing and K-sensing detections in a given wireless sensor network.

Yang Xiao[12] have provided the performance of the randomized scheduling algorithm via both analysis and simulation in terms of intrusion coverage intensity when an intrusion object occupies an area. They also study the impact of the size of intrusion object on the sensor network's configuration. For intrusion object detection, the detection probability is determined by the object size, the number of sensors, sensing radius, the number of subsets, as well as the size of the monitored region.

Tran Hoang Hai[13] has proposed two algorithms to optimal select and activate the intrusion detection agents for sensor networks. These are based on trust value and neighbor of each node. They also apply over-hearing technique to reduce the transmission of alert packets in WSNs.

Xi Peng et al[14] proposed a security management model for self organizing wireless sensor networks based on intrusion detection. It can prevent most of attacks. Then an analysis of each layer of networks in security model is discussed and the security management measures in the data link layer and network layer are described in detail especially. Such a structure is built based on the existing encryption and authentication protocols, and can detect most types of attacks in the sensor.

3. SENSOR NETWORK DEPLOYMENT

A heterogeneous WSN in a three dimensional (3D) plane with N sensors, denoted by a set N=(n_1,n_2,n_3…n_n) is considered , where n_i is the ith sensor. These sensors are uniformly and independently deployed in a cube area A = L*L*L. Such a random deployment results in a 3D Poisson point distribution of sensors. All sensors are static once the WSN has been deployed. In a heterogeneous WSN, here we consider two types of sensors ,that is, Type 1 and Type 2.Type 1 sensors have the sensing radius of r_{s1}, and the transmission range of r_{x1} and Type 2 sensors have the sensing radius of r_{s2}, and the transmission range of r_{x2}. A Type 1 sensor can only sense the intruder within its sensing coverage area that is a disk with radius r_{s1} centered at the sensor. Similarly Type 2 sensor can only sense the intruder within its sensing coverage area that is a disk with radius r_{s2} centered at the sensor. Denote the node density of the Type 1 Sensor in a heterogeneous WSN as $\lambda 1$. Denote the node density of the Type 2 Sensor in a heterogeneous WSN as $\lambda 2$ In a WSN, a point is said to be covered by a sensor if it is located in the sensing range of any sensor(s). The WSN is thus divided into two regions, the covered region, which is the union of all sensor coverage disks, and the uncovered region, which is the complement of the covered region within the area of interest A. In our network model, the intruder does not know the sensing coverage map of the WSN.

3.1 Intrusion Strategy Model

As illustrated in Figs. 2 and 3, we consider two intrusion strategies for the movement of the intruder in a WSN. If the intruder (say, a panzer) already knows its destination before entering the network domain, it follows the shortest path to approach the destination. In this case, the intrusion path is a straight line D from the entering point to the destination, as illustrated in Fig. 1. The main idea behind this strategy is that the straight movement causes the least risk for the intruder due to the least area that it has to explore by following a straight line toward the destination. The corresponding intrusion detection area S1 is determined by the sensor's sensing range rs and intrusion distance D1 as shown in Fig. 2 It is because the intruder can be detected within the intrusion distance D by any sensor(s) situated within the area of S.

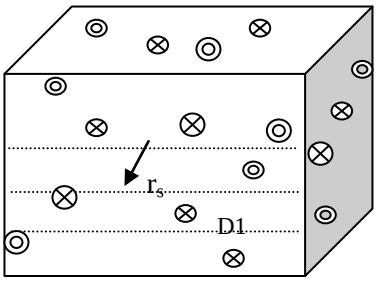

Figure 2. Intruder follows straight path

On the contrary, if the intruder does not know its destination, it moves in the network domain in a random fashion. We consider that the intruder tends to minimize the overlapping on its path. Thus, the intrusion path of the intruder can be regarded as a non overlapping curved line D2, and the intrusion area accordingly is a curved band S2, as illustrated in Fig. 3. In the above two strategies, if the intruder travels the same distance, i.e., D1=D2,the corresponding intrusion detection areas approximately satisfy S1 = S2. Therefore, we adopt a straight path in the following discussion, and the analytical results can be directly applied to the case of the curved path. Furthermore, the intruder can start its intrusion from the network boundary or a random point inside the network domain. For example, the intruder can be dropped from the air and starts from any point in the network domain.

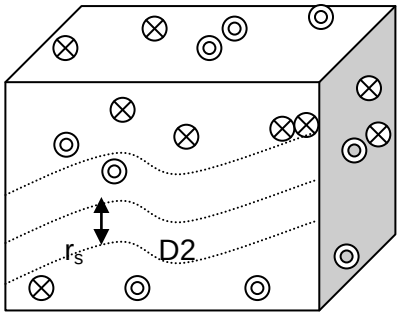

Figure 3. Intruder follows curved path

4. INTRUSION DETECTION IN HETEROGENEOUS WIRELESS SENSOR NETWORK

In this paper, an Intruder is defined as any moving object that enters into the WSN area .It may enter from a random point ,or through boundary of the deployment area. If dropped from the air then the entry point can be considered as a random point. In this paper, we present the analysis of intrusion detection in a heterogeneous WSN. We derive the detection probability for single-sensing detection and multi-sensing detection. Single-Sensing Detection is explained next.

4.1. Single-Sensing Detection

An intruder is detected when it enters the sensing range of a sensor. 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. When the intruder starts from a point of the network boundary, as shown in Fig. 3, given an intrusion distance D > 0, the corresponding intrusion detection volume V is almost an oblong volume. This volume includes a cylindrical volume with length D and width 2rs and a half sphere with radius rs attached to it. It has V= $\pi r_s^2 D + (2/3)\pi r_s^3$

According to the definition of single-sensing detection, the intruder is detected if and only if there exists at least one sensor within this volume V. Means that the intruder will only be detected if it comes the sensing range of any of the sensors. Otherwise, the intruder is not detected. Similarly, when the intruder starts from a random point in the network domain, the corresponding intrusion detection volume is given by the following equation. Here the sensing area includes the volume

of the sphere and that of the cylinder. The radius of the sphere is rs and the length of the cylinder is D. We can see that the area includes the complete spherical area.

V= $\pi r_s^2 D + 4/3(\pi r_s^3)$,

It is shown clearly in Fig. 4.

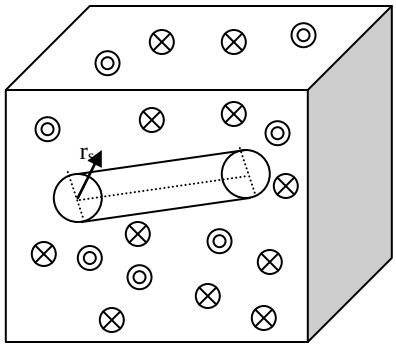

Figure 4 Area moved in case of random point entry

In the following analysis, we focus on the case that he intruder starts from the boundary of the network. The case is illustrated in figure 5

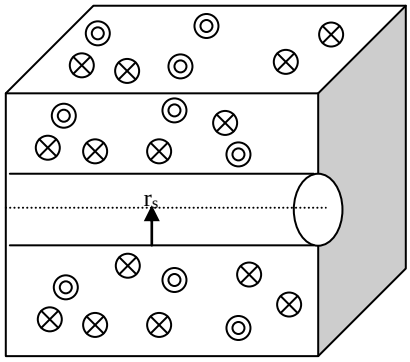

Figure 5 Area moved in case of boundary entry

Theorem 1: The probability $P(D=0)$ that an intruder can be immediately detected once it enters a heterogeneous WSN in a single sensing detection model can be given by

$$P(D=0) = 1 - e^{-\lambda_1((2/3)\pi r_{s1}^3)} * e^{-\lambda_2((2/3)\pi r_{s2}^3)}$$

Proof: According to Poisson distribution

$$p(m,V) = \frac{(V\lambda)^m e^{-V\lambda}}{m!}$$

where m is the number of sensors and V is the volume. If there is no sensors in the volume V, then the probability will be equal to P(0,V)= $e^{-V\lambda}$. Here in this case we are considering 2 types of nodes. So the volume V1 and V2 represents the volume covered by type 1 and 2 nodes respectively. The probability that there is neither type 1 nor type 2 sensor is there to detect the intruder = P(0,V1)P(0,V2)= $e^{-V1\lambda 1} e^{-V2\lambda 2}$ Based on complement of the probability , the probability that there is at least one sensor in the volume and the intruder is detected by any of these sensors

1-P(0,V1)P(0,V2)=1- $e^{-\lambda_1((2/3)\pi r_{s1}^3)} * e^{-\lambda_2((2/3)\pi r_{s2}^3)}$.

Hence the theorem is proved.

Theorem 2: Suppose η is the maximal intrusion distance allowable for the intruder to travel within the heterogeneous WSN network in single sensing detection , the probability P(D<= η) that the intrusion distance D is less than η can be calculated as

$$p(D <= \eta) = 1 - e^{-\lambda_1 V_1} * e^{-\lambda_2 V_2}$$

Where $V_1 = \pi r_{S_1}^2 \eta + (2/3)\pi r_{S_1}^3$ and

$$V_2 = \pi r_{S_2}^2 \eta + (2/3)\pi r_{S_2}^3$$

Proof: Here the volume moved by the intruder is V1= $\pi r_{S_1}^2 \eta + (2/3)\pi r_{S_1}^3$ and

V2= $\pi r_{S_2}^2 \eta + (2/3)\pi r_{S_2}^3$. So if there is no sensor in that volume, then the probability of detection is P(0,V1)P(0,V2). Then complement of P(0,V1)P(0,V2) will give the probability of detecting intruder within the distance D.

Theorem 3: Let $p(D=\Im)$ be the probability that the intruder is detected at an intrusion distance $\Im$ ($\Im$ >0) when it travels within the given heterogeneous WSN in single sensing detection can be derived as

$$p(D=\Im) = \pi(\lambda_1 r_{S_1}^2 + \lambda_2 r_{S_2}^2) e^{-\lambda_1 s_1} * e^{-\lambda_2 s_2}$$

Where $S_1 = \pi r_{S_1}^2 \eta + (2/3)\pi r_{S_1}^3$ and

$$S_2 = \pi r_{S_2}^2 \eta + (2/3)\pi r_{S_2}^3$$

proof: The equation in theorem 2 is the CDF of the intrusion distance. So differentiate it with distance will give the equation above.

4.2. Multi-Sensing Detection

In the multi-sensing detection model, an intruder has to be sensed by at least m sensors for intrusion detection in a WSN. The number of required sensors depends on specific applications. For example, at least three sensors' sensing information is required to determine the location of the intruder. Suppose there

are two models of sensors in a given heterogeneous network and any three sensors take part in intrusion detection in a collaborative manner at a time, then these three sensors can be of any of the following combinations.

1. Three Model I sensors,
2. Three Model II sensors,
3. One Model I Sensor and Two Model II sensor,
4. Two Model I Sensor and One Model II sensor.

Theorem 4: Let Pm(D=0) be the probability that an intruder is detected immediately once it enters the heterogeneous WSN in the multi sensing. It has

$$Pm(D=0) = 1 - \sum_{i=0}^{m-1} \sum_{i=0}^{m-1} P1(i,V1)\, P2(m-i,V2)]$$ where

$V1 = (2/3)\pi r_{S1}^3$ and $V2 = (2/3)\pi r_{S_2}^3$

Proof: for detecting an intruder in multisensing at the boundary there should be more than m sensors located in that specific volume. This can be proved just like theorem 1.

5. NETWORK COVERAGE AND BROADCAST REACHABILITY

The data collected by any of the sensors in WSN has to be transmitted in to the base station. If this transmission fails, it is meaningless even the sensor which may be in any location of the network senses critical information such as the presence of a sensor. Therefore it is essential that the network connectivity is always maintained in a wsn. A Network connectivity can be defined as the probability that a packet broadcasted from any sensor can reach all the other sensors in the network. There is an another term in wsn called Broadcast reachability .Broadcast reachability can be defined as the probability that a packet broadcasted from sensor in the WSN can reach all the other sensors in the network. Given node densities and the transmission ranges of different sensors deployed in a WSN, we can calculate the network connectivity or the broadcast reachability. On the other hand, if the required network connectivity (or broadcast reachability) is specified, we can compute the required transmission ranges in terms of node density. Thus, the minimal transmission power can be obtained for the purpose of power efficiency.

6. SIMULATION AND VERIFICATION

The simulation is done using MatLab. The analytical results are compared with simulation results. We can see that both are matching.

6.1 Performance Evaluation

The sensors are uniformly distributed in a cubicle three dimensional space of 100*100*100 meters . The sensing range is varied from 0 to 40 meters and maximal allowable intrusion distance is 5 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 6 shows Single-Sensing detection probability and Multi sensing- detection probability. It is evident that the single sensing detection probability is higher than that of multi sensing- detection probability .This is because the multi-sensing detection imposes a more stricter requirement on detecting the intruder (e.g., at least 3 sensors are required).

Fig. 6 also demonstrates that the detection probability in single-sensing detection approaches the value 1 when the sensing range of type 1 increases to a certain threshold. For example, in the single-sensing detection, the intruder can be detected with probability 1 if the sensing range exceeds 25. In order to get the result we fixed the type 2 sensors as 300 and its sensing range is set as 10. Total 200 type 1 sensors are deployed uniformly and its sensing range is varied from 0 to 40. Fig. 6 shows that the sensing range significantly impacts the detection probability of a heterogeneous WSN. To investigate the influence of a sensor's sensing range on an average intrusion distance of a WSN, we fix the number of sensors as N = 500 and vary the sensing range.

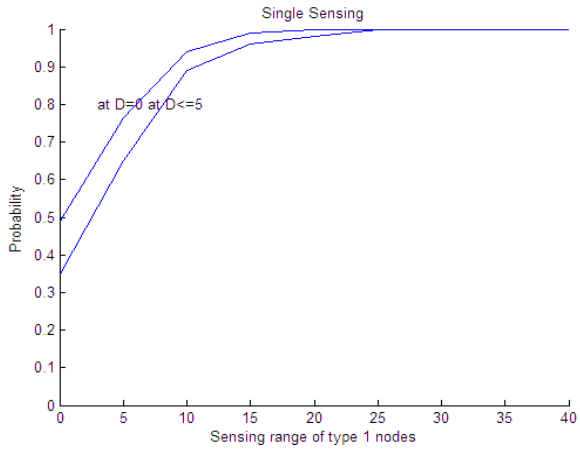

Figure 6. Single sensing probability analysis

Fig. 7 demonstrates multi sensing detection probability in the same environment as that used for single sensing.

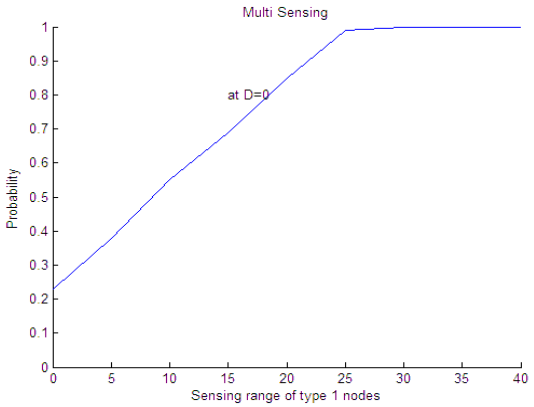

Figure 7. Multisensing probability analysis

7. CONCLUSION

This paper discuss the probability of intrusion detection in a WSN deployed in a three dimensional space. This probability gives an insight in to the required number of sensors in a given deployment, their sensing and transmission range to efficiently detect an intruder in a given WSN.We have developed an analytical model for intrusion detection and applied the same into single-sensing detection and multiple-sensing detection scenarios for heterogeneous WSNs.The correctness of the analytical model is proved by simulation .It defines and examines network connectivity in heterogeneous WSN which helps to select critical network parameters according to the application.

8. REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, vol. 40, no. 8, pp. 102-14, Aug. 2002 "A Survey on Sensor Networks", IEEE Communication Magazine.

[2] A. Perrig, et al., 8(5):521- 534, Sep. 2002, "SPINS: Security Protocols for Sensor Networks", Wireless Networks.

[3] S. Zhu, S. Setia, and S. Jajodia, Oct. 2003, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03).

[4] J. Deng, R. Han, and S. Mishra, , Apr.2003. "A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks", Proc. of the 2nd Int. IEEE Workshop on Information Processing in Sensor Networks

[5] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, vol. 7, no. 6, pp. 698–711, 2008."Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Transactions on Mobile Computing.

[6] O. Dousse, C. Tavoularis, and P. Thiran, 2006, "Delay of intrusion detection in wireless sensor networks," in Proceedings of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc).

[7] H. Kung and D. Vlah, , ser. 3, vol. 3, March 2003, pp. 1954–1961, "Efficient location tracking using sensor networks," in IEEE Wireless Communications and Networking Conference.

[8] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, vol. 5, no. 8, pp. 1044– 1056, 2006."Efficient in-network moving object tracking in wireless sensor networks," IEEE Transactions on Mobile Computing.

[9]Y. Zhang and W, Lee. pages 275-283,2000, Intrusion Detection in Wireless Ad-Hoc Networks. In Proc. ACM MobiCom.

[10] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, 2005 "Mobility improves coverage of sensor networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc).

[11] Yun Wang, Yoon Kah Leow, and Jun Yin ,2009," Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks," in 15th International Conference on Parallel and Distributed Systems .

[12] Yang Xiao, Hui Chen, Yanping Zhang, Xiaojiang Du, Bo Sun, and Kui Wu, 2008," Intrusion Objects with Shapes under Randomized Scheduling Algorithm in The 28th International Conference on Distributed Sensor Networks",in Computing Systems Workshops.

[13] Tran Hoang Hai, Eui-Nam Huh," Optimal Selection and Activation of Intrusion Detection Agents for WSN".

[14] Xi Peng, Zheng Wu, Debao Xiao,Yang Yu, ,2009," Study on Security Management Architecture for Sensor Network based on Intrusion Detection," International Conference on Networks Security, Wireless Communications and Trusted Computing .