Optimizing Sensors Distribution for Enhancing WSN Intrusion Detection Probability in Euclidian's Space

Omar Said
Information Technology
Department, College of Computers
and Information Technology
Taif University, Taif, Saudi Arabia

Alaa Elnashar
Information Technology
Department, College of Computers
and Information Technology
Taif University, Taif, Saudi Arabia

ABSTRACT
Intrusion detection is one of the most important issues in Wireless Sensor Networks (WSNs). WSN sensors distribution plays an important role in intrusion detection process; uniform distribution of sensors yields the same intruder detection capability for all WSN points. Many applications require different levels of security (i.e. the security level should be increased around some specific locations in WSN. Most of the related works focus on using Normal and Uniform distributions in 2D WSN applications with homogenous sensors. Many applications may be applied in 3D such as space monitoring and underwater ecosystem which still need extensive studies for intruder success probability. Sensors heterogeneity is also another important issue that should be well studied since most of intrusion detection researches focus on using homogenous sensors. So, in this paper, the normal and the uniform distributions in 3D WSN applications with heterogeneous sensors are studied. This proposed study presents two situations for intrusion detection process. In the first situation, only one sensor is enough to detect the intruder. The second situation, uses multiple sensors (k, k>1), to detect the intruder. Furthermore, the probability of intrusion detection with Normal distribution, Uniform distribution, and a mixture between them are compared. Finally, the results proved that the performance of the Normal distribution is better than the Mixture and the Uniform distributions as regard the ability of intruder detection and the general WSN efficiency.

General Terms
Computer Networks.

Keywords
Intrusion Detection, WSNs, Sensors, WSNs Security.

1. INTRODUCTION
In wireless communication, wireless sensor networks are installed in unsecured places and their main components are small and have limited power (sensors). So, WSNs are vulnerable to be attacked by adversaries and intrusion is one of the main attacks. Hence; intrusion detection became an extremely important issue in civil WSNs important applications. To detect the intruder in an accurate manner, an extremely large number of sensors should be used in WSN. However, this idea may not be considered as a long term solution because the system cost will be increased. In addition, it is not necessary to use large number of sensors because WSNs void areas can detect a moving intruder within a certain distance (the application can determine the required distance in which the intruder should be detected) [1, 2, 3, 4, 5]. Many researches are related to watching the security level in the WSN which is considered as a detector. Also, many researches are related to system monitoring and intruder detection [6, 7, 8, 9, 10, 11, 12, 13]. The time consumption in detection process is an important parameter in the intruder detection process. Also, the intruder detection systems of wired networks are not suitable for WSN due to different natures [14, 15, 16, 17].

This paper proceeds as follows; in Section 2 the research problem is defined. In Section 3 the related works are demonstrated. In Section 4 the proposed model is presented. In Section 5 the simulation environment is constructed and the results are discussed. Finally, In Sections 6 and 7 the conclusion and the future work are introduced respectively.

2. PROBLEM DEFINITION
The infrastructure of WSNs is huge number of sensors with wireless communication protocols. There are many types of sensors which are used to accomplish different functions such as heat sensors and light sensors. Two and three dimensions environments have many WSN applications with multifunctional targets that comprise sensitive data. So, intrusion detection problem became more focused by many researchers. This problem was studied extensively with WSN that contains similar sensors (homogenous). Unfortunately, the problem of intrusion detection in different sensors WSN, which installed in two dimensions, is studied in superficial manner. In addition, the complexity of solutions may be increased with three dimensions environment. Hence, there is a need to study this WSN security problem extensively in 3D environments with heterogeneous WSNs.

3. RELATED WORKS
There are many parameters in the intrusion detection problem such as sensor types, numbers and positions. Many researches are introduced to provide short-run solutions for intrusion detection problem. Some of these researches used different factors other than the factors that are introduced in this paper. Also, there are retrenches closed to this paper but in different ideas.

Some models are demonstrated to detect intruders in Ad-hoc network such as in [18]. The main drawback in these models is a long time which is consumed to detect the intruder in addition to big data transmission. [19] introduced a model that determines a relationship between detection probability and coverage. This model uses 2D environment in testing process. The distance between the intruder and the target as regards the detection probability is determined in [20] using some parameters such as transmission ranges. The motion of intruder in random directions is studied in [21]. [22] presented the relation between WSN with different sensor types that are

distributed using Normal and intrusion detection probability. [23] demonstrated conclusion for two models introduced in [23] and [25] that determined the relation between intrusion detection and distributed of sensors in WSN. The relation between the consumed time in intrusion detection process and the intruder/target distance is studied in [26]. Also, the sensor mobility can improve the coverage and compensate the little number of sensors in WSN [27, 28]. The most closed related work to this paper is introduced in [29] which determined the relation between the probability of intruder detection and WSN application requirements in addition to parameters of WSN. This model didn't study its proposal in 3D environments. On the other hand, [30] uses Poisson and Gaussian as a mixture to distribute the sensors in the WSN but it used 2D environment for testing the proposed idea. The technique in [31] used 3D environment with heterogeneous WSN but unfortunately, this model is not well defined due to lack in probability density function definition and cubic style which made the results are uncertain.

4. THE PROPOSED MODEL

There are many applications that are installed in 3D spaces. Hence, sensors distributions over these types of spaces should be considered. Furthermore, the WSN have multifunctional applications which indicate that they use different types of sensors. So, the heterogeneous WSN is mandatory parameter during the process of proposed model construction. The major target of the suggested model is to determine the probability of intrusion detection that facilitate the security managers in sensors distribution and deployment. This will raise the security level and provide safety applications. The intrusion detection probability with sensor distribution using Normal and Uniform is studied. Sample from these types of distributions over 3D environment is found in Fig. 1 (a). The problem of intrusion detection contains four parameters which can be stated as follows, the sensors, the environment, the intruder, and the target. All of the parameters are in 3D style. In the proposed model, the cubic with predefined dimensions is used to represent the 3D environment. Other model parameters, the sensors, the intruder, and the target, are represented by spheres. To represent heterogeneous WSN, many spheres with different dimensions are used such that each sphere represents one sensor. The dimensions of each sphere are determined dynamically. In the same manner, the intruder can be represented by different dimensions spheres. The target term is defined as the area which required to be protected. Fig. 2 shows sample state which is determined by the position of an intruder as regards his target sphere.

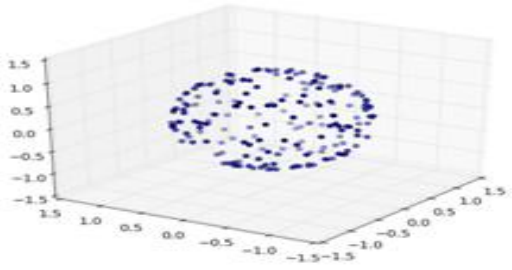

Fig. 1: Sample from sensor distribution views [32]

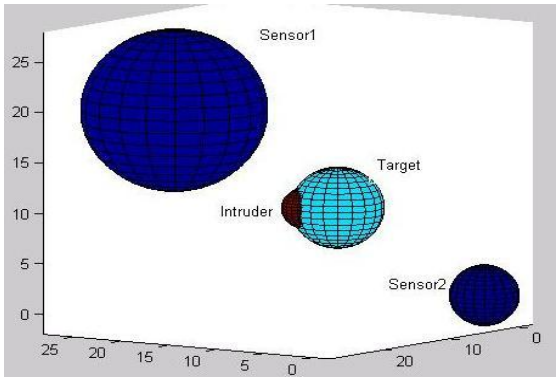

Fig. 2: 3D intruder/3D sensors/3D target Samples

5. SIMULATION

To test the sensor probability distribution in 3D space, a simulation environment should be constructed that contains multifunctional sensors. Furthermore, another simulation environment is constructed to test the distribution of sensors as regards network parameters such as number of control bits, number of hops, and end-to-end delay. The network simulation package OPNET 14.5 [33] is used in simulation building process. The simulation parameters are stated as follows; the packet size equals 512 bytes, the sources and destinations are determined randomly, the time of simulation is 30 minutes, the maximum number of nodes is 800, the packet inter-arrival time is random, the environment area is 10 x 10 km2, and the used MAC protocol is 802.15.4 with CSMA/CD. Infrared transmission channels are used to communicate sensors in WSN using mesh topology with different types of distributions; Normal, Uniform, and the Mixture between them.

5.1 Ability of Intrusion Detection

The main idea of efficiency evaluation is built on the distances between intruder/sensor/target. These distances are extracted from the relation between the spheres which represent the intruder, the sensor, and the target (i.e., if they are intersected, touched, or faraway from each other). The danger case in the problem is occurred when the distance between the intruder and the target is less than the distance between the intruder and his nearest sensor from the target in the same direction. The probability of this case occurrence should be minimized. Eq.1 and Eq.2 are for Normal and Uniform distributions. Eq.3 describes the intersection between the spheres. The positions of the intruder and his target are determined randomly. Two tests are executed in the simulation environment. The first test neglects the distance between intruder/target/sensor objects and the intruder velocity. In contrast, the second test considers the intruder/target distance in addition to the intruder/ target nearest sensor.

$$F(x,\mu,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \qquad \text{Equation 1}$$

$$f(x,k) = \begin{cases} \frac{1}{u-1}, & \text{if } x \in R_x \\ 0, & \text{if } x \notin R_x \end{cases} \qquad \text{Equation 2}$$

$$1/(2*d)[(-d+r-R)*(-d-r+R)*(-d+r+R)*(d+r+R)]^{1/2} \qquad \text{Equation 3}$$

Fig. 3 presents the first test results. It shows that the sensor distribution using mixture between Normal and Uniform distributions has the best performance approximately at all numbers of sensors. A lower performance is provided by using Normal distribution. Uniform distribution has the lowest performance. Fig. 4 presents the second test results. It shows that the sensor distribution using Normal has the best performance. But, the mixture between Normal and Uniform distributions provides lower performance. A lowest performance is for Uniform distribution.

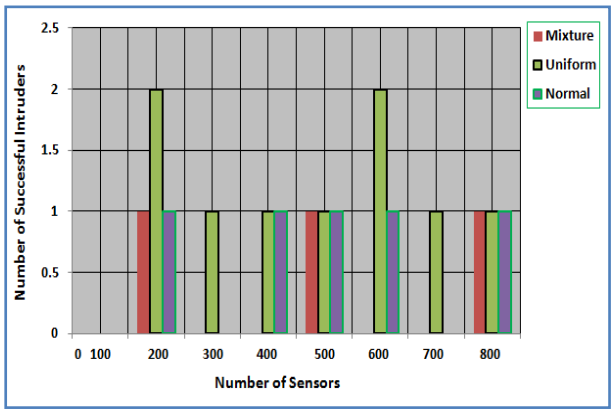

Fig. 3: Successful intruders (distance and velocity are not considered)

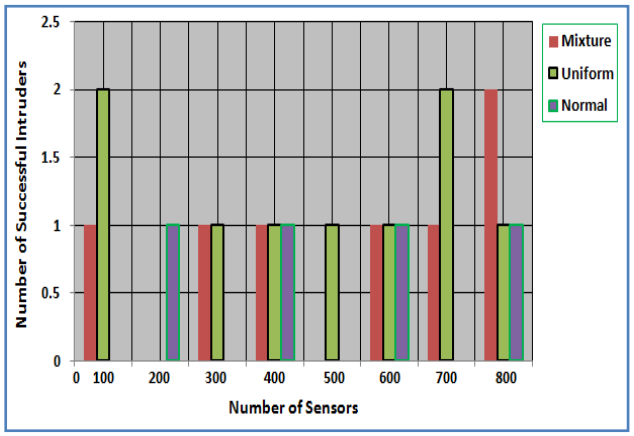

Fig. 4: Successful intruders (distance and velocity are considered)

5.2 Evaluation of WSN Sensor Distribution

The efficiency of WSN is an important parameter to test the proposed model. The intruder may be detected but the reaction of WSN against this intruder should occur in an accurate time. So, the information, which is needed by the security manager, should be transmitted successfully. Hence, the WSN should be evaluated as regards the network parameters. These parameters are the transmitted control bits, the number of hops, and the end-to-end delay.

5.2.1 Average Number of Control Bits

The average number of control bits is an important parameter due to the bottlenecks which may be occurred during the WSN sessions. This parameter should be minimized to decrease the transmitted bits which decrease the probability of network problems occurrence such as congestion. In addition, the sensors have limited power sources which mean that if the number of control bits decreases the sensor power consumption will be decreased. Fig. 5 shows the results of control bits as regards the Normal, Uniform, and Mixture between them probability distributions. These results show that the Normal distribution has the minimum number of control bits in contrast of the mixture which has large number of control bits. But, the Uniform distribution has maximum number of transmitted control bits.

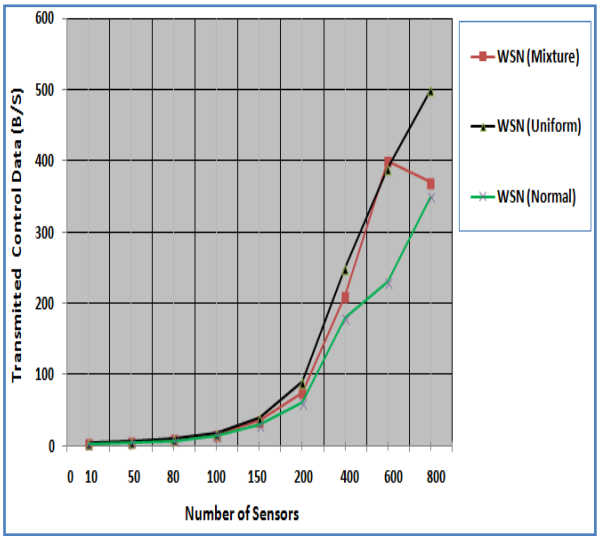

Fig. 5: Control bits (Normal, Mixture, and Uniform)

5.2.2 The Number of Hops

The number of hops determines the complexity of routing process. So, if this complexity is increased, the transmission of data in the WSN may face routing problems. In addition, the best routing paths is not sufficient but finding an alternative path in case of basic one failure is necessary. Fig. 6 presents the results of number of hopes that used to transmit information from source to destinations in each probability distribution. The results proved that the distribution of sensors by Normal uses number of hops less than other distributions. The mixture between Normal and Uniform uses higher number of hopes but less than Uniform distribution that has highest number of hops. The random selection of source and destination makes the curve hesitated. Furthermore, there are some nodes that are failed during the simulation of transmission process which cause sudden events.

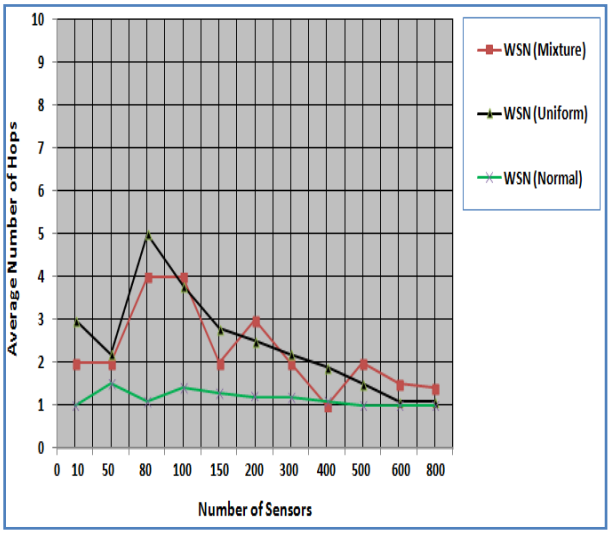

Fig. 6: Number of hops (Normal, Mixture, and Uniform)

5.2.3 Average End- to-End Delay

The average end-to-end delay is calculated by the difference between full packet buffering time and full packet receiving time [35]. The transmission delay is an important parameter in the security systems especially for sensitive organization. The result of end-to-end delay is presented in Fig. 7. The average end-to-end delay values for the three different distribution types are approximately closed. But, the minimum values are for the Mixture and the Uniform distributions respectively. In case of Normal, there are many restrictions in the routing hops spec such as buffer size that cause high delay than other distributions.

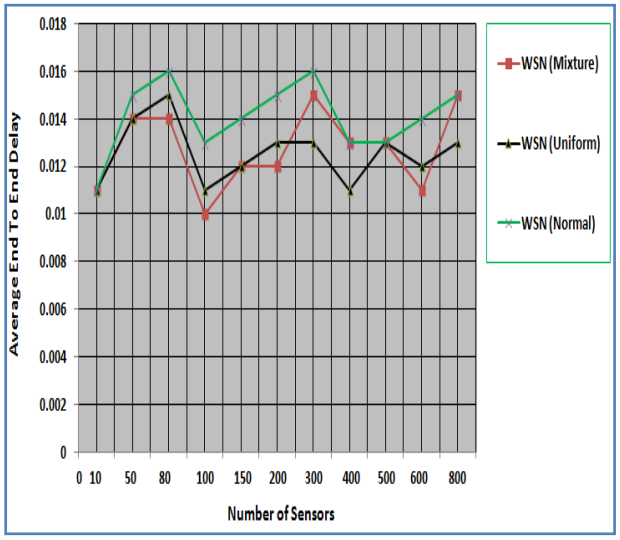

Fig. 7: End-to-End delay (Normal, Mixture, and Uniform)

6. CONCLUSION

In this paper, a model to test the sensor distribution in WSN environments is proposed. The sensor, the intruder, the target, and the environment are in 3D style. The used probability distributions in the WSN are Normal, Uniform, and Mixture between them. This paper presented two types of simulations. The first simulation is for testing the efficiency of WSN in detecting intruders in case of using Normal, Uniform, and Mixture between them distributions. The second simulation is for testing the efficiency of WSN as regards network parameters when the sensors are distributed using Normal, Uniform, and Mixture between them. The result in the first test proved that the Normal and the mixture have the best performance in intruder detection. In the second test, the Normal distribution has the best performance as regards the average number of transmitted control bits and the number of hopes. But in the average end-to-end delay parameter, the mixture distribution has the best performance. The Uniform distribution has a middle performance between the Normal and the Mixture distributions.

7. FUTURE WORK

Other distributions of sensors such as Beta, Qui Square, or more mixtures should be tested and the results should be compared.

8. ACKNOWLEDGMENTS

I wish to express my sincere gratitude to Taif University for its support and co-operation to accomplish this work.

9. REFERENCES

[1] YangXia Luo, et al, A Survey on Intrusion Detection of Wireless Sensor Network, IEEE 2nd International Conference on Information Science and Engineering (ICISE), China, pp: 1798 - 1802, 4-6 Dec. 2010.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Wireless Sensor Networks,” IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[3] K. Sohraby, D. Minoli, and T. Znati, Wireless Sensor Networks: Technology, Protocols, and Applications. John Wiley and Sons, Inc., 2007.

[4] J.N. Al-Karaki and A.E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Wireless Comm., vol. 11, no. 6, pp. 6-28, Dec. 2004.

[5] S. Tilak, N.B. Abu-Ghazaleh, and W. Heinzelman, “A Taxonomy of Wireless Micro-Sensor Network Models,” ACM Mobile Computing and Comm. Rev., vol. 6, no. 2, pp. 28-36, Apr. 2002.

[6] A. Agah, S. Das, K. Basu, and M. Asadi, “Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach,” Proc. Third IEEE Int’l Symp. Network Computing and Applications (NCA ’04), pp. 343-346, 2004.

[7] A. Agah, S. Das, and K. Basu, “A Game Theory Based Approach for Security in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Performance, Computing, and Comm., pp. 259-263, 2004.

[8] V. Giruka, M. Singhal, J. Royalty, and S. Varanasi, “Security in Wireless Sensor Networks,” Wireless Comm. and Mobile Computing, vol. 8, no. 1, pp. 1-24, 2008.

[9] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, and M. Gouda, “A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking,” Computer Networks, vol. 46, no. 5, pp. 605-634, 2004.

[10] Y. Wang, X. Wang, B. Xie, D. Wang, and D.P. Agrawal, “Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks,” IEEE Trans. Mobile Computing, vol. 7, no. 6, pp. 698- 711, June 2008.

[11] O. Dousse, C. Tavoularis, and P. Thiran, “Delay of Intrusion Detection in Wireless Sensor Networks,” Proc. MobiHoc, 2006.

[12] H. Kung and D. Vlah, “Efficient Location Tracking Using Sensor Networks,” Proc. IEEE Wireless Comm. and Networking Conf., vol. 3, pp. 1954-1961, Mar. 2003.

[13] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, “Efficient In-Network Moving Object Tracking in Wireless Sensor Networks,” IEEE Trans. Mobile Computing, vol. 5, no. 8, pp. 1044-1056, Aug. 2006.

[14] 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.

[15] 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).

[16] 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.

[17] 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.

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

[19] 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).

[20] 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.

[21] 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 .

[22] Y. Wang, W. Fu, and D. P. Agrawal, "Intrusion detection in Gaussian distributed heterogeneous wireless sensor networks," 6th IEEE International Conference on Mobile Ad Hoc and Sensor Systems Oct. 2009.

[23] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility Improves Coverage of Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc'05), pp. 300-308, 2005.

[24] 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.

[25] O. Dousse, C. Tavoularis, P. Thiran "Delay of Intrusion Detection in Wireless Sensor Networks," MobiHoc '06 Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing ,New York, NY, USA 2006.

[26] Q. Shi, C. Comaniciu," Efficient cooperative detection for wireless sentinel networks" 44th Annual Conference on Information Sciences and Systems (CISS), March 2010.

[27] D. Turgut, B. U. Turgut, and L. Boloni, "Stealthy dissemination in intruder tracking sensor networks," IEEE 34th Conference on Local Computer Networks LCN, Oct. 2009.

[28] Yun Wang, Weihuang Fu, and Dharma P. Agrawal, "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks", IEEE Transaction on Parallel and Distributed Systems, Vol. 24, No. 2, Feb. 2013.

[29] Maduri Chopde, Kimi Ramteke and Satish Kamble, "Probabilistic model for Intrusion Detection in Wireless Sensor Network", International Journal of Communication Network and Security (IJCNS), Vol-1, Issue-3, 2011.

[30] Mohamed Mubarak.T et al.,"Intrusion Detection: A Probability Model for 3D Heterogeneous WSN", International Journal of Computer Applications, Volume 6– No.12, September 2010.

[31] C. Ortiz, J. Puig, C. Palau, M. Esteve, "Wireless sensor network modeling and simulation, International Conference on Sensor Technologies and applications, Valencia, Spain, pp: 307-312, October 14-20, 2007.

[32] George Marsaglia, "Choosing a Point from the Surface of a Sphere," Ann. Math. Statist. Volume 43, Number 2, pp: 645-646, 1972.

[33] OPNET IT GURU: A tool for Networking Education, MSCIT Practicum Paper, REGIS UNIVERSITY, http://staff.ustc.edu.cn/~bhua/experiments/ITGAE_Tool_Ntwrk_Ed.pdf

[34] http://mathworld.wolfram.com/Sphere-SphereIntersection.html

[35] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: a Survey," Elsevier Journal of Computer Networks, Vol N. 38, pp: 393–422, 2002.