*IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*
*e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 5, Ver. II (Sep - Oct .2015), PP 87-91*
*www.iosrjournals.org*

# Likelihood of Intruder Detection in Uniform, Gaussian and Cohesive Network Distribution by Single and Multiple Sensing Models

Miss. Samidha Davari[1], Prof. U. A Patil[2]
[1,2]*(Electronics Department /Shivaji University, India)*

***Abstract:*** *This paper analyzes the problem of intrusion detection in a Uniform, Gaussian and cohesive distributed WSN by characterizing the detection probability with respect to the application requirements and the network parameters under both single sensing detection and multiple sensing detection model. Effects of different network parameters and sensing range on the likelihood of intruder detection are examined. Furthermore, performance of the network cohesive distributed WSNs is compared with uniformly and Gaussian distributed WSNs. This work gives guidelines for likelihood of intruder detection in a wireless sensor network for selecting an appropriate deployment strategy and determining network parameters.*

***Keywords:*** *Gaussian distribution, intrusion detection, network deployment, uniform distribution, sensing range, wireless sensor network*

## I. Introduction

A wireless sensor network consists of a number of small autonomous sensing devices, each of which is called a sensor node with a power unit, a sensing unit, a processing unit, a storage unit and a wireless transmitter/receiver. The sensor nodes can be deployed in controlled environment such as factories, homes, or hospitals. They can also be deployed in uncontrolled environment such as a disaster or hostile area, and dangerous environment such as battlefields, toxic regions etc. Applications of WSNs are numerous and growing, and range from indoor deployment scenarios in the home and office to outdoor deployment scenarios in natural, military and embedded settings.

Wireless sensor network are vulnerable to security attacks due to the broadcast nature of transmission and the limited computation and communication capabilities of the sensor node. Moreover the majority of the WSN applications should be run continuously and reliably without interruptions. Hence, survivability implies that networks should have the capability to operate under node failures and attacks. On the other hand, security encompasses the aspects of confidentiality, authentication, and integrity of the application information. security and survivability in WSNs face many common challenges, ranging from the wireless nature of Communications, resource limitations on sensor nodes, very large and dense networks, and unknown network topology prior to deployment, to high risk of physical attacks to unattended.

A sensor deployment approach is responsible for intrusion detection capability of a WSN. Random sensor deployment is usually approved due to its fast deployment, easy scalability, fault tolerant, and can be used in a hostile and human-inaccessible region. Depending on specific deployment approach, a randomly deployed WSN can have uniform node density or differentiated node density in the Field of Interest. If all of the sensors are deployed randomly and uniformly, the resulting network imitates to a uniform distribution. If all sensors are to protect an important entity, the resulting sensor network imitates to a Gaussian distribution. And if some the sensors are deployed uniformly and some belong to protect specific entity, which results cohesive distribution of uniform and Gaussian.

## II. Literature Survey:

Kung and Vlah [3] implemented hierarchical tree structure to effectively track the movement of an intruder to support fast querying of intruder information. The hierarchical tree consists of connected sensors and is built upon expected properties of intruder mobility patterns such as its movement frequency over a region.

Lin et al. [4] implemented the logical object tracking tree structure for tracking an intruder, to minimize the total communication cost. It reduces the communication cost for data updating and querying by taking into account the physical network topology.

Chao et al. [5] have addressed the issue of tracking a moving intruder by power-conserving operations and sensor collaboration to minimize the power consumption. Author proposed the set of novel metrics for detecting a moving intruder and developed two efficient sleep-awake schemes called PECAS and MESH.

Ren et al. [6] studied the trade-off between the network detection quality (i.e., how fast the intruder can be detected) and the network lifetime and proposed three wave sensing scheduling protocols to achieve the bounded worst case detection probability.

Liu et al. [7] have modeled the intrusion detection problem in a mobile WSN, where each sensor is capable of moving. For fast detection of quality due to the mobility of sensors.

Guerriro et al. [8] used Bayesian framework to exploit prior knowledge such as the target's location for data fusion in WSN. They derive the closed form for the Bayesian detector and show the performance improvement over the Scan statistic without using extra sensor observations.

Zhu et al. [9] propose a binary decision fusion rule that reaches a global decision on the target detection by integrating local decisions made by multiple sensors. They derive the fusion threshold using Chebyshev's inequality without assuming a priori probability of target presence that ensure a higher hit.

In this paper, we address the intrusion detection problem from the other angle. Most of the above efforts consider intrusion detection and its efficiency in terms of the single-sensing model in a homogeneous WSN. Instead of the network architecture and detecting protocol design so we implemented likelihood of intruder detection using heterogeneous network as fusion of uniform and Gaussian and compared result with uniform and Gaussian distribution network.

## III. System Model And Architecture

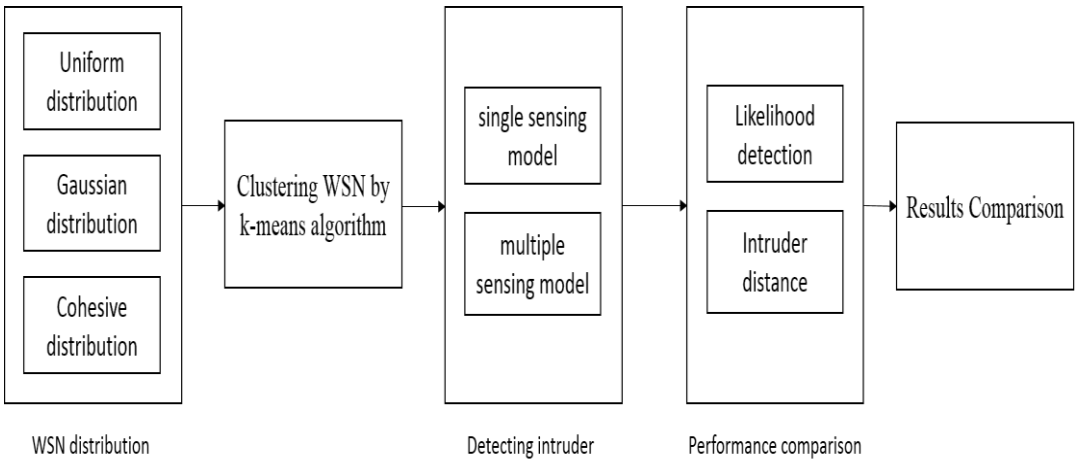


Fig.1: System Block Diagram

The Implemented system helps to guide the selection of an appropriate random sensor deployment strategy, the design of a WSN and determining critical parameters for intrusion detection such as Detection likelihood and intruder distance. In the Uniform distribution, all sensors are deployed uniformly and randomly. Gaussian distribution, some sensors are concentrated at the target area and remaining get rare towards the boundary of the network. We implemented the combined likelihood model of uniform and Gaussian distribution in WSN for intruder detection. The theoretical analysis [1] of implemented system is as follows.

Suppose ($\xi > 0$) is the maximal allowable intrusion distance for intrusion detection in a given application, and the intruder starts at a distance R to its target (0, 0). Let P1 [$D<\xi$] be the probability that the intruder can be detected within $\xi$ in the considered network model. P1 [$D<\xi$]

$$P_1[D \le \xi] = 1 - \left\{ 1 - \int_{R-\xi}^{R} \int_{-r_s}^{r_s} f'_{xy}(\sigma)\,dydx - \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma)\,dydx - \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma)\,dydx \right\}^N$$

Eq.1

## IV. Sensing And Detection Model

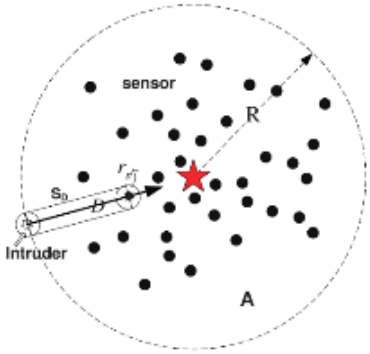


**Fig.2** Intrusion detection in a wireless sensor network

We assumed the same sensing range for all sensors there are two ways to detect an intruder: single-sensing detection and multiple-sensing detection. In single-sensing detection, the intruder can be detected by a single sensor when entering its sensing range. And in the m-sensing detection model, an intruder has to be sensed by at least m sensors where m depends on a specific application. We assume that the intruder can enter the WSN from an arbitrary point. In a single-sensing detection, at one sensor should be located in the region for detecting the intruder. Similarly, in multiple-sensing detection, at least m sensors should be inherent in the region for distinguishing the intruder. In the case of $\xi > 0$, the intruder is allowed to travel some distance within the WSN. Likelihood of intruder detection is formulated [1] as

$$P_m[D \le \xi] = 1 - \sum_{i=0}^{N} \binom{N}{i} (1 - p_\xi)^{(N-i)} * p_\xi^i,$$

*where*

$$p_\xi = \int_{R-\xi}^{R} \int_{-r_s}^{r_s} f'_{xy}(\sigma) dy dx + \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma) dy dx + \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma) dy dx.$$

Eq.2

## V. Clustering Network Using K-Means Algorithms

K-means [10] is the Clustering algorithm which partitions the data set into k clusters using the cluster mean value so that the resulting clusters intra cluster similarity is high and inters cluster similarity is low. A critical task in Wireless Sensor Networks for energy efficiency and network stability. This clustering has following properties as the clusters are non-hierarchical and they do not overlap. Every member of a cluster is closer to its cluster than any other cluster because closeness does not always involve the center of clusters. With a large number of variables, K-Means is computationally faster than hierarchical clustering. K-Means may produce tighter clusters than hierarchical clustering, especially if the clusters are globular. Hence we used existing kmeans algorithm for clustering and energy conservation

## VI. Experimental Results

The performance of system is evaluated by likelihood of Detection which is defined as the probability that an intruder is detected within the maximal allowable intrusion distance that is specified by a WSN application. The impact of sensing range on the intrusion detection probability in single sensing and multi-sensing detections in Uniform, Gaussian and cohesive is analyzed. The table 1 shows the results of likelihood of intruder detection by varying sensing range.

We considered the network parameter as the number of deployed sensors N is 100, the standard deviation is 25, and the maximal allowable intrusion distance is 30. Table 1 shows results of likelihood of intruder detection by varying sensing range by single sensing range.

| SENSING RANGE | UNIFORM | GAUSSIAN | COHESIVE |
|---|---|---|---|
| 10 | 0.74 | 0.814286 | 0.88 |
| 15 | 0.75 | 0.8375 | 0.92 |
| 20 | 0.88 | 0.91 | 0.95 |
| 25 | 0.911111 | 0.94 | 0.96 |
| 30 | 0.93 | 0.97 | 1 |
| 35 | 0.98 | 0.988889 | 1 |
| 40 | 0.988889 | 1 | 1 |
| 45 | 1 | 1 | 1 |
| 50 | 1 | 1 | 1 |

Table 1: Likelihood of detection by varying sensing range by single sensing

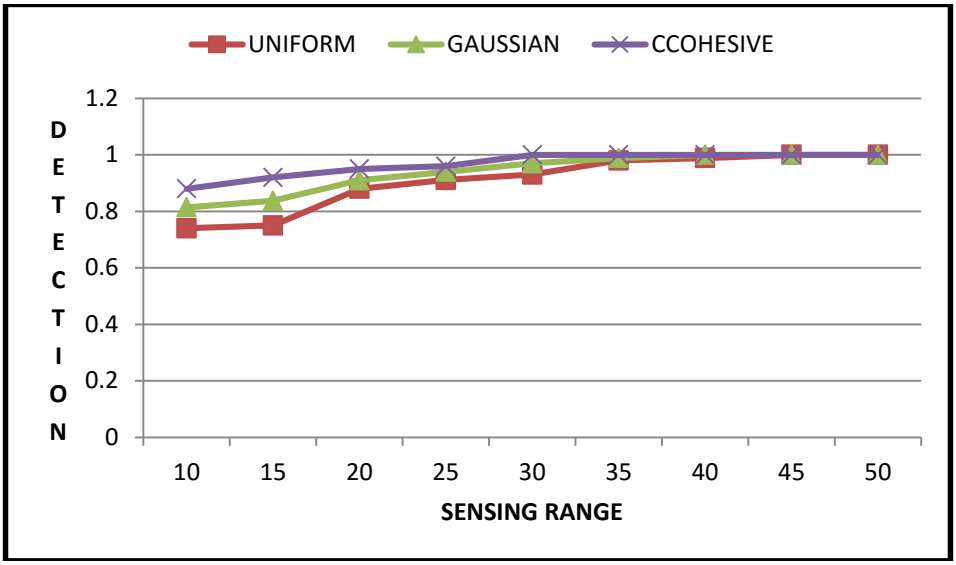


**Fig3**: Likelihood of intruder detection comparison of uniform, Gaussian and cohesive distribution

From table1 and figure 3 shows the results of likelihood of intruder detection by varying sensing range by single sensing technique. We observed that likelihood of intruder detection is increases as a larger sensing range as compared to uniform and Gaussian distribution.

| SENSING RANGE | UNIFORM | GAUSSIAN | COHESIVE |
|---|---|---|---|
| 10 | 0.42 | 0.43 | 0.5 |
| 15 | 0.49 | 0.577778 | 0.7444 |
| 20 | 0.5 | 0.666667 | 0.788889 |
| 25 | 0.6 | 0.8125 | 0.8375 |
| 30 | 0.75 | 0.833333 | 0.875 |
| 35 | 0.766667 | 0.911111 | 0.922222 |
| 40 | 0.922222 | 0.97 | 0.98 |
| 45 | 0.99 | 1 | 1 |
| 50 | 1 | 1 | 1 |

Table 2: Likelihood of detection by varying sensing range by multiple sensing

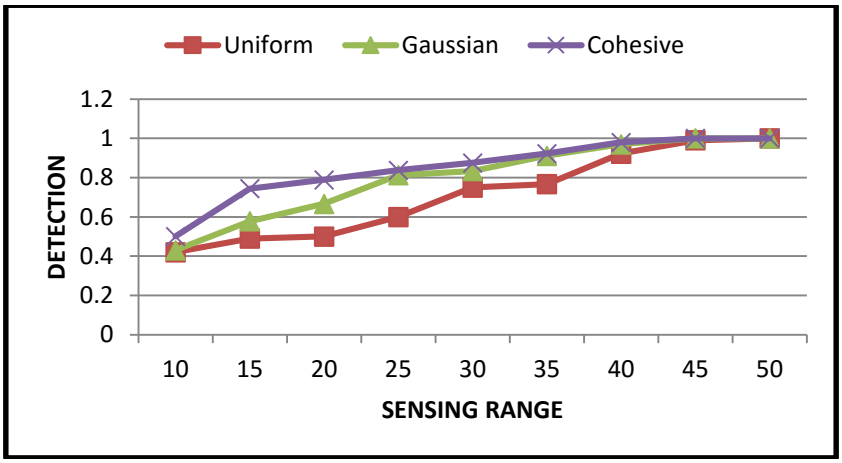


**Fig.4**: Likelihood of intruder detection comparison of uniform, Gaussian and cohesive distribution by multiple sensing

From table2 and figure 4 shows the results of likelihood of intruder detection by varying sensing range by multiple sensing techniques. Here we observed that the likelihood of intruder detection is increases as a sensing range increases and shows better likelihood of intrude detection as compared to uniform and Gaussian distribution.

## VII. Conclusion

In this paper we examined the likelihood of intruder detection in different network deployment approaches as uniform, Gaussian and cohesive. We found the results by varying sensing range under single sensing, multiple sensing model by keeping number of sensors, standard deviation and maximum allowable distance constant. Our result shows that the likelihood of intruder detection in cohesive distribution is increases as a larger sensing range as compared to uniform and Gaussian distribution by single and multiple sensing model. Hence cohesive network distribution improves the network coverage, and higher network coverage leads to a quicker detection of the intruder.

## References

[1]. Yun Wang, Wei huang Fu, and Dharma P. Agrawal, Life Fellow, IEEE IEEE Transactions on parallel and distributed systems, vol. 24, no. 2, february 2013
[2]. T. Wimala jeewa and S.K. Jayaweera, "Impact of Mobile Node Density on Detection Performance Measures in a Hybrid Sensor Network," IEEE Trans. Wireless Comm., vol. 9, no. 5, pp. 1760-1769, May 2010.
[3]. 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
[4]. 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.
[5]. Chao, S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, "Design and Analysis of Sensing Scheduling Algorithms under Partial Coverage for Object Detection in Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 3, pp. 334-350, Mar. 2007.
[6]. S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, "Design and Analysis of Sensing Scheduling Algorithms under Partial Coverage for Object Detection in Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 3, pp. 334-350,Mar. 2007
[7]. B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility Improves Coverage of Sensor Networks," Proc. Sixth ACM Int'lSymp. Mobile Ad Hoc Networking and Computing (MobiHoc '05),pp. 300-308, 2005.
[8]. M. Guerriero, L. Svensson, and P. Willett, "Bayesian Data Fusion for Distributed Target Detection in Sensor Networks," IEEE Trans. Signal Processing, vol. 58, no. 6, pp. 3417-3421, June 2010.
[9]. M. Zhu, S. Ding, Q. Wu, R. Brooks, N. Rao, and S. Iyengar,"Fusion of Threshold Rules for Target Detection in Wireless Sensor Networks," ACM Trans. Sensor Networks, vol. 6, no. 2,article 18, 2010.
[10]. Sasikumar, P. ; Sch. of Electron. Eng., VIT Univ., Vellore, India ; Khara, S. K-Means Clustering in Wireless Sensor Networks" Computational Intelligence and Communication Networks (CICN), 2012
[11]. I.F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, "A Survey on Wireless Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.
[12]. 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.
[13]. 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.
[14]. S. Kumar, T.H. Lai, and J. Balogh, "On K-Coverage in a Mostly Sleeping Sensor Network," Proc. 10th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom '04), pp. 144-158, 2004.
[15]. 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.
[16]. 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.