IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Optimization of Intrusion Detection Capability in Wireless Sensor Network

Richa Kumari

M. Tech Scholar, School of Information Communication Tech, Gautam Buddha University, Greater Noida, India

Abstract: Wireless Sensor Network has most widely used applications ranging from health care to military. Wireless Sensor Networks (WSNs) have many tempting features but due to the lack of any defense mechanism, the security becomes an issue in such networks. To operate WSNs in a secure way, any kind of intrusions should be detected before malicious attackers can harm the network. The intrusion detection system identifies the legitimate attackers in the network area. In this paper we have optimized the intrusion detection capability in a wireless sensor network using Gaussian distribution and uniform distribution method. Furthermore, the performance of Gaussian-distributed WSNs is compared with uniformly distributed WSNs. The effect of various network and system parameters such as sensing range of the sensors, number of sensor deployed, intruder's starting distance and maximum allowable intrusion distance on the intrusion detection probability of the network has been observed. Hence detection probability can be analytically formulated in a random WSN and an appropriate deployment strategy can thus be selected to determine critical network parameters.

Keywords: Gaussian and uniform distribution, intrusion detection, WSNs.

I INTRODUCTION

Wireless Sensor Networks (WSNs) are applicable in various fields of science and technology like in health care, military surveillance, highway traffic monitoring; to monitor environmental phenomena, such as ocean, wildlife, earthquake, pollution and wild fire, or to monitor industrial sites, such as building safety, manufacturing machinery and so on. WSNs consist of components that have limited power devices such as sensors that can be installed in open environments. This makes WSNs vulnerable to attacks by intruders. Since WSNs applications are used in fields like environmental sensing, industrial monitoring, and military etc. where confidentiality of information is extremely necessary, intrusion detection becomes an extremely important issue.
In WSNs a huge number of sensors need to be deployed for intruder detection. However, the high cost of this solution makes it impractical. Furthermore, using a huge number of sensors does not guarantee a successful detection of a moving intruder within a certain distance since void area may be found in the WSN. There are two main categories for intrusion detection problem. The first one uses a component to monitor WSN security.

This component may be software, hardware or human. The target of this component is accomplished by using some sensors to ensure that the security level in WSN is acceptable. The second one detects the intruder when it tries to storm unauthorized area. The time consumed for intruder detection process is an important parameter that should be considered. Accordingly, the intruder should be detected at the same time of its entrance. So, raising the probability of intruder detection in WSNs is concerned to sensor deployment plan more than the number of sensors [1]. The model uses various probability distributions to deploy sensors within the entire network. A simulator is created so as to simulate the intrusion detection process and evaluate its efficiency based on the probability distribution used. This will further guide the WSN designer to select the optimal sensors distribution that yields the best intrusion detection efficiency. This resulted into the research that aimed to propose new lightweight and secure solutions.

II RELATED WORKS

Wireless sensor networking is one of the most promising technologies that have many applications ranging from tactical military to health care. Wireless sensor networks are applied to various fields of science and technology to collect information regarding human activities and behaviour, such as military surveillance, health care and reconnaissance, highway traffic, to monitor physical and environmental phenomena, such as ocean and wildlife, pollution, earthquake, wild fire, water quality; to monitor industrial sites, such as building safety, manufacturing machinery performance, so on [2]. Intrusion detection (sometimes refers to target detection or object detection/tracking) as a surveillance problem of practical importance in WSNs has received considerable attention in the literature.

Aiming at effectively detecting the presence of an intruder and conserving network resources, researchers have been studying the problem from both practical and theoretical perspectives under different constraints and assumptions [5], [4], [3]. Intrusion detection in WSNs of problem under energy, cost, and detection accuracy constraints, Ren et al. [6] examine the tradeoff between the network detection quality (i.e., how fast the intruder can be detected) and the network lifetime, and propose three wave sensing

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

scheduling protocols to achieve the bounded worst case detection probability. Wang et al. [7] propose a two-level cooperative and energy-efficient detection algorithm to reduce the energy consumption rate of a WSN by limiting the number of sensors in operation through a face-aware routing and wake-up mechanism. Based on multiple-sensing detection, data aggregation and fusion techniques are employed to improve the detection accuracy and false-tolerance of WSN systems. Guerriro et al. [8] employ a 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 rate and lower false alarm rate compared to the weighted averages of individual sensors. Moreover, Liu et al. [10] take the node mobility into consideration and present a strategy for fast detection by illustrating that a mobile WSN improves its detection quality due to the mobility of sensors.

In this paper, we address the problem of intrusion detection by examining a Gaussian distributed WSN and comparing its performance with a uniformly distributed WSN. We have investigated such a problem by modeling, analysis, and simulations, under both single-sensing and multiple-sensing detections. The analytical results are shown to match with the simulation outcomes, validating the precision of the work. A preliminary version of this work was presented in conference [11]. We have further extended it by considering a truncated Gaussian-distributed WSNs and comparing the intrusion detection performance of a random WSN with a Gaussian, truncated Gaussian and a uniformly distributed system under the same application scenarios; illustrating how two network variables affect the detection probability together; and discussing the practical implication of the results. This work provides the complete insight into the intrusion detection problem in a randomly distributed WSN following a Gaussian, truncated Gaussian, or uniform distribution and compares their performance.

III INTRUSION DETECTION IN WSN

Recent studies on the intrusion detection problem into two major categories. First, A system component for monitoring the security of a WSN and diagnosing compromised/vulnerable sensors to ensure the correct network behavior and avoid false alarm [12]. Further, it is defined as monitoring or surveillance system for detecting a malicious intruder that invades the network domain. This work focuses on the second category. Fig. 1 gives an example in which a number of sensors are deployed in a circular area (A = πR2) for protecting the centric located target by sensing and detecting the presence of a moving intruder.

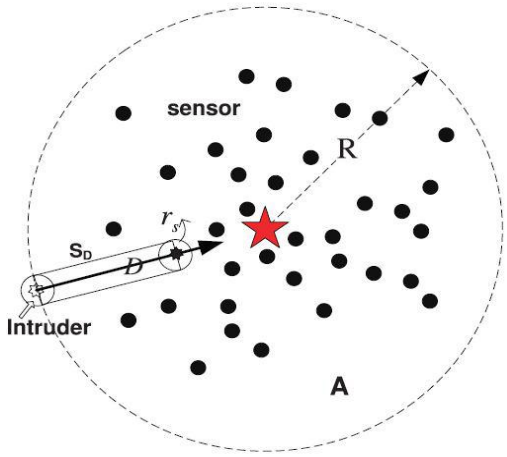

Fig. 1: Intrusion detection in a wireless sensor networks [1].

Intrusion detection import how effectively an intruder can be detected by the WSN, Definitely, the intruder can be detected, better is the intrusion detection capability of the WSNs. Which is densely deployed with sensors and has full sensing coverage, the intruder can be detected immediately after it enters the field of interest (FoI).

Full sensing coverage means immediate intrusion detection. However, full sensing coverage demands for a large number of sensors and can be hardly feasible in an actual practice. Intrusion detection applications do not have such a strict requirement of immediate detection. Instead, maximum allowable intrusion distance (ξ) is specified. Suppose the intruder moves a distance of D in the WSN before it is detected.

If D < ξ, the WSN meets the performance requirements. Otherwise, the WSN needs to be reconfigured. Apparently, intrusion distance is a central issue in an intrusion detection application using a WSN.

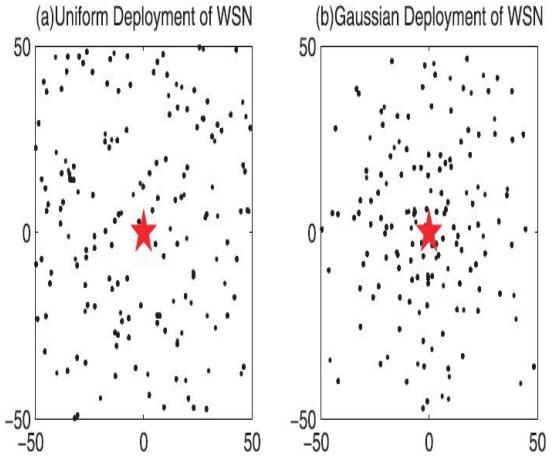

Fig.2: WSN deployments following uniform and Gaussian distribution [1].

A sensor deployment strategy plays a basic role in determining the intrusion detection capability of a WSN. Random sensor deployment is commonly adopted 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

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

deployed WSN can have uniform node density or differentiated node density in the FoI. If all of the sensors are deployed randomly and uniformly, the resulting network conforms to a uniform distribution. Further, if all sensors are to protect an important entity, the resulting sensor network conforms to a Gaussian distribution. Fig.2 sketches two example WSNs following a uniform and a Gaussian distribution, respectively.

The problem of intrusion detection is analyzed in a randomly deployed WSN following a uniform distribution. The intrusion detection probability is the same for any point in the field of interest (FoI), and the expected intrusion distance is derived as:

$$E(D) = \int_0^{\sqrt{2}L} 2\xi\lambda r_s e^{-\lambda\left(2\xi r_s + \frac{\pi r_s^2}{2}\right)} d\xi$$

Where λ is the node density, r_s is the sensor's sensing range, and L is the side length of the FoI. This work provides a systematic and complete insight for intrusion detection in uniformly deployed WSNs, when the intruder approaches the network from the boundary. However, if an intruder enters the network at an arbitrary point inside the FoI, the uniform WSN deployment can have an inherent serious problem. Suppose the intruder is dropped from an airplane at an arbitrary position $P= (x_p, y_p)$ in the WSN, and the distance between P and the target point $T=(x_t, y_t)$is less than the expected intrusion distance, i.e.

$$\sqrt{(x_p - x_t)^2 + (y_p - y_t)^2} \leq E(D)$$

Truncated Gaussian distribution allows the placement of sensors in a bounded field and our results based on truncated Gaussian distributed sensor networks thus have significant importance in directing real-life WSN design for intrusion detection, especially for small-scale WSNs. To sum up, the main contributions of this work include [13].

- Develop an analytical model for intrusion detection in a (truncated) Gaussian-distributed WSN, and mathematically derive detection probability with respect to various network parameters, employing both single sensing detection and multiple-sensing detection models.
- Investigate the interplays between the network parameters and the detection capability of the (truncated) Gaussian-distributed WSN.
- Compare the performance of intrusion detection in a WSN following uniform distribution with that of (truncated) Gaussian distribution and provide guidelines in choosing a random sensor deployment strategy and parameters.

IV MODEL DESCRIPTION

1. Network Deployment Model

In Fig.1, Consider a WSN with randomly deployed N sensors around a target point (i.e., the central red star) following a 2D Gaussian distribution. The FoI A is assumed to be a square area with side length L. Without loss of generality, we assume the coordinate of the target point as G= (0, 0) and the same standard deviation (i.e.,$\sigma_x = \sigma_y = \sigma$) along X and Y dimensions in the deployment field ($-\frac{L}{2} \leq X \leq \frac{L}{2}, -\frac{L}{2} Y \leq \frac{L}{2}$). The PDF for point (x, y) to be deployed with a sensor, PDF of sensors deployed in a 2D area A = 100 × 100 with mean deployment point G = (0, 0) and deployment standard deviation σ = 25 and σ = 50, respectively. We can see that different deviation leads to different sensor distribution. Furthermore, the closer the location is to the center, the higher is the probability of deploying sensors there. Note that when the standard deviation σ is increased to some extent, some sensors may be deployed outside the FoI A. If all sensors ought to be deployed inside A, a truncated Gaussian distribution can be used and the corresponding PDF. Gaussian-distributed WSN with the corresponding truncated Gaussian-distributed WSN with σ = 15 and σ = 50, respectively. Note that when σ increases toward infinity, the truncated Gaussian distribution tends toward a uniform distribution. The methodology we develop in the following analysis can be applied to both Gaussian and truncated Gaussian-distributed WSNs by replacing $f'_{xy}(\sigma)$ with $f(x, y, \sigma)$ or $f'(x, y, \sigma)$ respectively.

2. Sensing and Detection Model

All sensors are assumed to be equipped with the same sensing range r_s, and their sensing coverage is assumed to be circular and symmetrical following a Boolean sensing model. There are two ways to detect an intruder: single-sensing detection and multiple-sensing detection in WSNs. The intruder can be successfully detected by a single sensor when entering its sensing range in single-sensing detection, further, in the m-sensing detection model, an intruder has to be sensed by at least m sensors and m depends on a specific application. Note that these m sensors need not sense the intruder simultaneously in the considered model [13].

3. Intrusion Strategy Model

We assume that the intruder can enter the WSN from an arbitrary point with distance R to the target (R is a random variable). The corresponding intrusion detection region S_D is indirectly determined by the sensor's sensing range r_s and intrusion distance D as in Figure3.1, and the area of S_D is given by

$$|S_D| = |S_{c1}| + |S_r| + |S_{c2}| = 2 * D * r_s + \pi r_s^2$$

It is important to observe that in a single-sensing Detection; at least one sensor should be located in the region S_D for detecting the intruder. Similarly, in multiple-sensing detection, at least m sensors should reside in the region S_D for recognizing the intruder [13].

V PERFORMANCE EVALUATION

A Comparison on the Effect of the Number of Sensors

Fig.3 shows the detection probability for uniform and (truncated) Gaussian-distributed WSNs under multi sensing detection when the number of deployed sensors is varied from 10 to 200. The detection probability for all of the cases increases with the increase of the number of sensors N. In addition, there are two important observations as illustrated in Fig.3. First, when the distance of the intruder's starting point is changed from

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

R=50 to R=30, the detection probability in the uniform distributed WSN remains the same, but the detection probability in the (truncated) Gaussian-distributed WSN changes dramatically. This validates the fact that a WSN having a uniform distribution provides uniform detection capability in its deployment field, while the (truncated) Gaussian-distributed WSNs can provide location-related detection capability. Another important observation is that neither the (truncated) Gaussian-distributed WSNs nor the uniform-distributed WSNs are always better than the other ones.

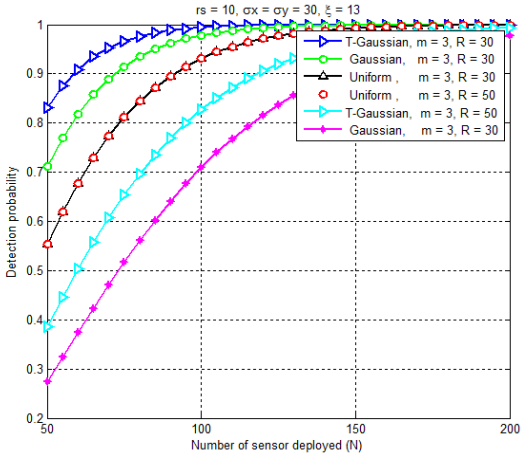

Fig.3: (Truncated) Gaussian versus uniform distribution.

B Comparison on the Effect of the Intruder's Starting Distance

In figure 4, the effect of the normalized intruder's starting distance R_{norm} in terms of network radius $\sqrt{A}/2$on the detection probability of WSNs following a uniform distribution and a Gaussian distribution under both one sensing detection and three-sensing detections. And observe that the detection probability in a uniformly distributed WSN keeps constant when the starting point (R, 0) of the intruder is varied for both one and three-sensing detections.

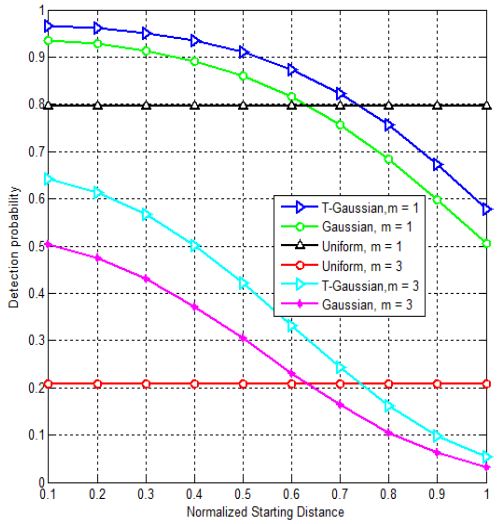

Fig.4: (truncated) Gaussian versus uniform distribution on normalized intruder's starting distance.

It does not matter where the intruder enters the WSN domain and the number of sensors located in the intrusion detection region S_ξ is expected to be the same in a uniform-distributed WSN. In a (truncated) Gaussian-distributed WSN, the detection probability drops gradually at the increase of the intruder's starting distance R under both one and three-sensing detection cases. The underlying reason is that, in (truncated) Gaussian-distributed WSNs the further the intruder's starting point is away from the center, the fewer sensors are deployed in the corresponding intrusion detection regionS_ξ.

C Comparison on the Effect of Maximal Allowable Intrusion Distance

Fig.5 demonstrates the effect of the maximal allowable intrusion distance on the detection probability for uniform and (truncated) Gaussian-distributed WSNs under one-sensing and multi sensing detections. From the figure, it is understood that with an increase in the maximal allowable intrusion distance ξ, the detection probability increases for all the cases.

In addition, it is also seen that there exists a threshold in the maximal allowable intrusion distance that can be used as a reference in selecting appropriate deployment strategy for intrusion detection applications with different tolerance of the intruder, i.e., ξ. In brief, when using a WSN for intrusion detection, the deployment strategy should be carefully selected according to the given application's requirements (i.e., ξ) and the intruder's approaching strategy (i.e., R).

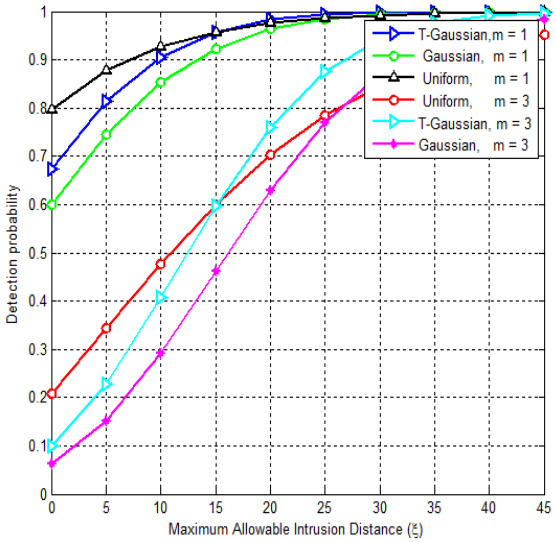

Fig.5: Gaussian versus uniform distribution on maximal allowable intrusion distance.

Fig.6, illustrates the detection probability for Uniform, Gaussian and Truncated Gaussian distributed WSNs varying with the standard deviation (σ). Gaussian and truncated Gaussian both reach the peak point and after that they decrease. Uniform distributed remains constant with a variation in the standard deviation (σ). This implies that the truncated Gaussian distributed is better than the other.

DOI 10.17148/IJARCCE.2016.55100

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

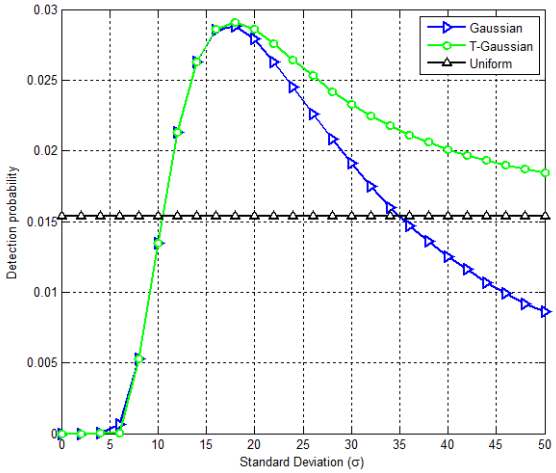

Fig.6: Probability of a sensor being deployed in the intrusion detection region S_ξ of Gaussian, truncated Gaussian, and uniform-distributed WSNs with varying σ.

D. Comparison on the Effect of the Sensing Range r_s

Fig.7 depicts the impact of sensing range on the intrusion detection probability in one and multi sensing detection for Gaussian truncated Gaussian and uniformly distributed WSNs. To analyze the effect of the sensing range on the detection probability the values of intruder's starting distance, standard deviation, number of deployed sensors, and the maximal allowable intrusion distance are taken as R = 80, σ= 25, 00, and ξ=30, respectively. The detection probability is observed to improve as the sensing range increases, as an increase in the sensing range improves the network coverage and thus the probability of intrusion detection to a quicker detection of the intruder. Performance of truncated Gaussian is better than Gaussian and Uniform distribution WSNs on every Parameter which are used.

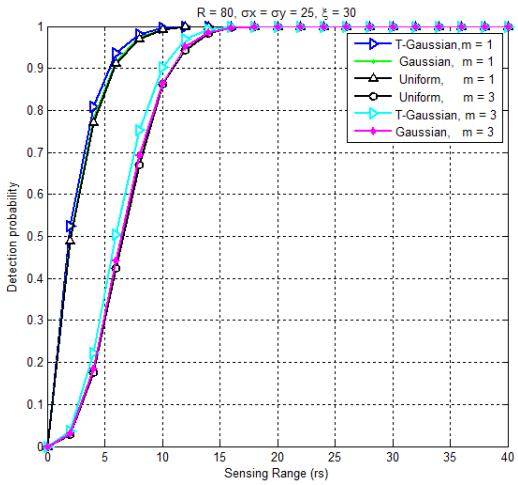

Fig.7: Effect of sensing range rs on the detection probability in a Gaussian, truncated Gaussian, and uniform-distributed WSN.

V CONCLUSION

Intrusion is a major threat to many WSN applications such as military surveillance, industrial monitoring etc. This paper provides ample insights into the intrusion detection problem in a randomly distributed WSN following a Gaussian, truncated Gaussian, or a uniform distribution. We have analyses the intrusion detection for a truncated Gaussian-distributed WSN via evaluating the intrusion detection probability with respect to numerous network parameters by simulations. Performance of truncated Gaussian is better than Gaussian and Uniform distribution WSNs on every Parameter which are used. Likewise, the performance of the intrusion detection in a Gaussian-distributed WSN is compared with a uniformly distributed WSN and a truncated Gaussian distributed WSN from the perspectives of network settings, application requirements, and intruder's approaching strategy.

REFERENCES

[1]Yun Wang, Weihuang Fu and Dharma P. Agrawal, "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, pp.342-355, Feb. 2013.

[2]I. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks", in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '2005), pp. 253– 259, Aug. 2005.

[3] E. Yanmaz and H. Guclu, "Stationary and Mobile Target Detection Using Mobile Wireless Sensor Networks," Proc. IEEE INFOCOM, 2010,

[4]M. Zhu, S. Ding, Q. Wu, R.R. Brooks, N.S.V. Rao, and S.S. Iyengar, "Fusion of Threshold Rules for Target Detection in Wireless Sensor Networks," ACM Trans. Sensor Networks, vol. 6, pp. 18:1- 18:7, Mar. 2010.

[5]T. Wimalajeewa 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.

[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] G. Wang, M.Z.A. Bhuiyan, and L. Zhang, "Two-Level Cooperative and Energy-Efficient Tracking Algorithm in Wireless Sensor Networks," Concurrency and Computation: Practice and Experience, vol. 22, pp. 518-537, Mar. 2010.

[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] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility Improves Coverage of Sensor Networks," Proc. MobiHoc, 2005

[11] Y. Wang, W. Fu, and D.P. Agrawal, "Intrusion Detection in Gaussian Distributed Wireless Sensor Networks," Proc. Sixth IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems, 2009,

[12] 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.

[13]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.