International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 4 Issue 7, July-2015

Cluster Based Intrusion Detection System for Wireless Sensor Networks

S. P. Predeep Kumar[1], Dr. E. Babu Raj[2] and Dr. M. Chithirai Pon Selvan[3]

[1]Research Scholar, St.Peter's University, Chennai, Tamilnadu, India
[2]Principal, N S College of Engineering, Kanayakumari Dist., Tamilnadu, India
[3]Associate Professor - School of Engineering & IT, Manipal University, Dubai, P.O.Box 345050, UAE

ABSTRACT

The intrusion detection system identifies the legitimate and attackers in the network area. The intrusion detection system is designed in two categories. In the first model a system component is used for monitoring the security of a WSN and diagnosing compromised or vulnerable. Second model is the monitoring or surveillance system for detecting a malicious intruder that invades the network domain.Intrusion detection is applied to detect malicious or unexpected attackers in Wireless Sensor Network (WSN). Gaussian-distributed WSNs can provide differentiated detection capabilities at different locations. Different degrees of probability is used in Gaussian distribution modeled WSN. There are two sensing scenarios are used in the intrusion detection system. They are single-sensing detection and multiple-sensing detection scenarios. The intrusion detection system is enhanced to support different deployment schemes. Sensor node clustering scheme is integrated with the IDS to handle single and multiple detection mechanisms. Sensing and transmission coverage factors are included in the intrusion detection process.

Keywords: Gaussian-distributed WSN, IDS, Network Deployment Model, Cluster Based Intrusion Detection System.

INTRODUCTION

A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoebox-sized nodes down to devices the size of grain of dust, although functioning 'motes' of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year.

RELATED WORKS

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 [16], [8], [10].

Many works investigate this problem under various metrics and assumptions [9]. Arora et al. defined the system models and examine the intrusion detection problem in the context of a security scenario called A Line in the Sand by quantitatively analyzing the effect of network unreliability on application performance, assuming that the nodes are deployed with uniform density and subject to some local variations. Wang et al. [9] provide a unifying approach in relating the intrusion detection probability with respect to various network settings. They assume a random WSN with uniform node density and disk sensing model. Given an intruder that moves on a straight line, they derived the probability of detecting the intruder within a predefined distance. Based on a Poisson approximation of uniform sensor distribution, Wang et al. [6] analytically compared its performance to that of a Gaussian distributed WSN. Dousse et al. analyze the delay in intrusion detection, which is defined as the first contact time when the intruder hits the sensing range of a sensor belonging to the large sensor cluster. The key result in this work demonstrates a significant gap in the delay between the first contact time with a sensor and the first contact time with the large connected sensor cluster in a random WSN with uniform node density. Cao et al. derive analytical formulas for detection probability and the mean delay in a uniformly distributed WSN with tunable system parameters such as node density and sleep duty cycle. They consider both stationary intruder and mobile intruder that moves on a straight line at a constant speed. Lazos et al. [11] formulate the intrusion detection problem as a line-set intersection problem and derive analytic formulas of the intrusion detection probability until a target is detected in a random WSN with uniform node density. Most recently, Medagliani et al. [1] propose an engineering toolbox which contains a set of models for describing the probability of missed detection, the alert transmission latency, and the energy consumption to optimally configure a given WSN for a variety of quality of service requirements. This work adopts and extends the analytical framework used in [11] and assumes a linear intrusion path. Different from adopting a linear path, Wang et al. [15], [2] propose a Sine-curve mobility model that can simulate different intrusion paths by adjusting its features and examine the interplays between network settings and the intruders mobility patterns. It is found that an intruder following a Sine-curve intrusion path can be more beneficial than following a straight-line path as the probability of being detected can be decreased, however with a side effect of reducing intrusion progress toward the destination to some extent. In other words, the straight-line path provides the maximum possible intrusion progress toward the destination when the moving distance is fixed.

Other works study the intrusion detection problem under energy, cost, and detection accuracy constraints. Ren et al. examine the tradeoff between the network detection quality and the network lifetime, and propose three wave sensing scheduling protocols to achieve the bounded worst case detection probability. Wang et al. 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. [4] 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. [5] 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 averages of individual sensors. Moreover, Liu et al. 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 from another angle 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 correctness of this work. A preliminary version of this work was presented in conference [13]. We extend it by considering the truncated

Gaussian-distributed WSNs; comparing the intrusion detection performance of a random WSN with a Gaussian, a truncated Gaussian, a uniform distribution 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 comprehensive insights into the intrusion detection problem in a randomly distributed WSN following a Gaussian, truncated Gaussian, or uniform distribution and compares their performance in a bounded field of interest.

INTRUSION DETECTION IN WSN

Due to recent technological advances in wireless communication, manufacturing of small- and low-cost sensors has become economically feasible. A large number of sensors can be deployed in an ad hoc fashion to form a Wireless Sensor Network (WSN) for many civil and military applications. Intrusion detection has received a great deal of attention since it supports various applications such as environmental monitoring and military surveillance.

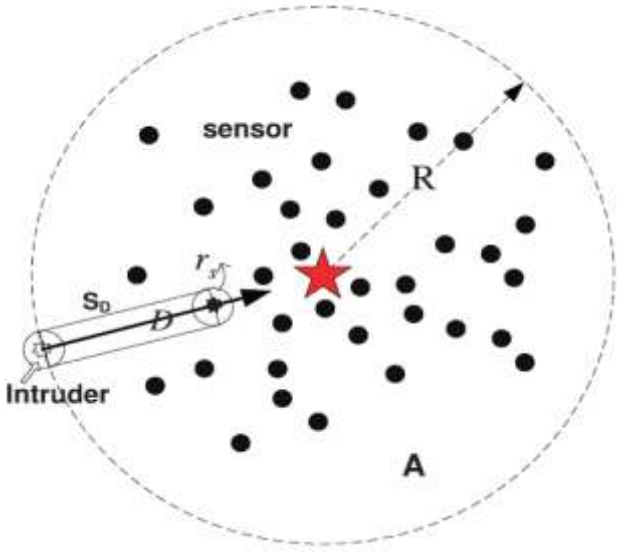

Fig. 1. Intrusion detection in a WSN

Recent studies on the intrusion detection problem fall into two major categories. First, it is considered as 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 [7]. On the other hand, 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 ($A = \pi R^2$) for protecting the central located target by sensing and detecting the presence of a moving intruder. Intrusion detection implies how effectively an intruder can be detected by the WSN. Obviously, sooner the intruder can be detected, better is the intrusion detection capability of the WSN.

In the extreme, the intruder can be detected immediately after it enters the field of interest (FoI), which is densely deployed with sensors and has full sensing coverage. 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. Therefore, most intrusion detection applications do not have such a strict requirement of immediate detection. Instead, a maximum allowable intrusion distance (ξ) is specified. Suppose the intruder moves a distance of D in the WSN before it is detected. If $D < \xi$, 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.

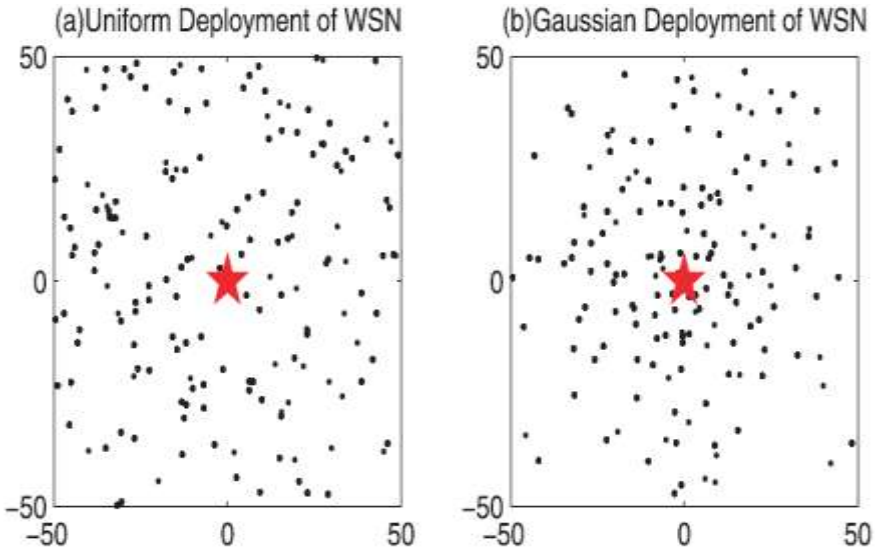

Fig. 2. WSN deployments following uniform and Gaussian distribution

A sensor deployment strategy plays a vital role in determining the intrusion detection capability of a WSN. Random sensor deployment is usually 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 deployed WSN can have uniform node density or differentiated node density in the FoI. To be specific, if all of the sensors are deployed randomly and uniformly, the resulting network conforms to a uniform distribution. On the other hand, 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.

To date, most of the related work assumes a WSN following uniform distribution for intrusion detection analysis [9]. In [9], 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 FoI and the expected intrusion distance is derived as: $E(D) = \int_0^{\sqrt{2}L} \xi\lambda r_s e^{-\lambda(2\xi r_s + \pi r_s^2/2)} d(\xi)$, 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 [14]. 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.,

$$\sqrt{(x_i - x_t)^2 + (y_i - y_t)^2} \leq E(D) \qquad (1)$$

In this case, the target can be attacked no matter how large the area of the uniform WSN is deployed. In addition, many intrusion detection applications in WSNs require different degrees of intrusion detection capability at different locations. The system may require extremely high detection capability with densely deployed sensors at certain hot spots (e.g., areas close to an important entity in a battlefield). For some not-so-sensitive areas, relatively sparsely deployed sensors could be acceptable. Uniform sensor deployment cannot fulfill such requirements either.

Fortunately, WSNs with Gaussian distributed sensors can provide differentiated node densities at different locations as illustrated in Fig. 2b. Different from uniformly distributed WSNs as illustrated in Fig. 2a, in a Gaussian distributed WSN, the closer the area is to the central deployment point T, more sensors are deployed to provide enhanced detection capability. On the other hand, fewer sensors are deployed in areas that are far away from the hot spot T, which decreases the network deployment cost as well. This makes it important to address the intrusion detection problem in a Gaussian-distributed WSN and we will establish the results from modeling, analysis, and simulation perspectives. We extend our discussion to the truncated Gaussian WSNs. It is due to the fact that Gaussian distribution allows the placement of sensors in an unbounded area while most real-life WSN applications take place in a bounded field of interest. 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

- 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, and validate theoretical derivations and results by Monte-Carlo simulations.

- 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.

Issues on IDS

Intrusion detection is applied to detect malicious or unexpected attackers in WSN. The intruder can be an enemy in a battlefield, or a malicious moving object in the area of interest. Same detection probability is used in the uniform distribution modeled WSN. Gaussian-distributed WSNs can provide differentiated detection capabilities at different locations. Different degrees of probability is used in Gaussian distribution modeled WSN. Detection probability is estimated with respect to the application requirements and the network parameters. There are two sensing scenarios are used in the intrusion detection system. They are single-sensing detection and multiple-sensing detection scenarios. Relaxed intrusion detection and immediate intrusion detection models are used in the single sensing scenarios. In the immediate intrusion detection model the intruders are detected before any movement in the WSN. In the relaxed intrusion detection model the intruders are detected after some movements in the WSN. The following drawbacks are identified in the existing system.

- Deployment scheme optimization is not provided
- Detection parameter selection is not provided
- Detection latency is high
- Sensing and transmission capacity are not integrated

SYSTEM MODEL AND DEFINITIONS

The system model includes a network deployment model, a sensing and detection model, and the evaluation metrics.

A. Network Deployment Model

As illustrated in Fig. 1, we consider a WSN with randomly deployed N sensors around a target point 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 ($-{}^{L}/_{2} \leq X \leq {}^{L}/_{2}$, $-{}^{L}/_{2} \leq Y {}^{L}/_{2}$) 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, σ) or f'(x, y, σ), respectively.

B. Sensing and Detection Model

All sensors are assumed to be equipped with the same sensing range rs, and their sensing coverage is assumed to be circular and symmetrical following a Boolean sensing model. In a WSN, there are two ways to detect an intruder: single-sensing detection and multiple-sensing detection. In single-sensing detection, the intruder can be successfully detected by a single sensor when entering its sensing range. On the other hand, in the m-sensing detection model, an intruder has to be sensed by at least m sensors and m depends on a specific application [9]. Note that these m sensors need not sense the intruder simultaneously in the considered model.

C. Intrusion Strategy Model

The intruder is assumed to be aware of its target (i.e., the hot spot), and follows the shortest intrusion path D toward the target as shown in Fig. 1. The straight-line intrusion path model was adopted in [9], [11], etc. It is due to the fact that abstractions and assumptions are inevitable to conduct theoretical analysis [12] and make influencing factors tractable.

Further, 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 Fig. 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 SD for detecting the intruder. Similarly, in multiple-sensing detection, at least m sensors should reside in the region S_D for recognizing the intruder.

Cluster Based Intrusion Detection System for WSN

The intrusion detection system is enhanced to support different deployment schemes. Automatic parameter learning model is integrated with the intrusion detection system. Sensor node clustering scheme is integrated with the IDS to handle single and multiple detection mechanisms. Sensing and transmission coverage factors are included in the intrusion detection process. The system is divided into four major modules. They are network deployment, coverage analysis, cluster construction and intrusion detection process.

The network deployment module is designed to construct a WSN. The coverage analysis module is designed to analyze sensing and transmission coverage. The cluster construction module is designed to group up neighborhood nodes. The intrusion detection process module is designed to detect legitimate and attackers.

A. Network Deployment

Node placement architecture is analyzed in deployment analysis process. Uniform distribution scheme places the nodes in equal distance. Nodes are placed in different distance level under gaussian distribution environment. The network area and node properties are analyzed in the deployment process.

B. Coverage Analysis

The coverage analysis is performed to analyze the sensing and transmission coverage of the nodes. The sensing coverage deals with the data capture area. The transmission coverage deals with the communication range. The homogeneous sensors are designed with uniform coverage details. Different coverage levels are used in the heterogeneous environment.

C. Cluster Construction

The clusters are used to group up the neighborhood nodes. The sensing and transmission coverage are used in the cluster construction process. The clusters are constructed with resource details. The cluster head is selected with reference to the resource details.

D. Intrusion Detection Process

The sensing range is analyzed for the nodes. Immediate mode identifies the intruder at the time of entry level. In the relaxed model the intruder is detected after some activities. The multiple sensing models detect different data values at node levels. Data requests are verified for each node. Communication range is analyzed for the nodes.

CONCLUSION

Wireless sensor networks are constructed with different deployment schemes. The intruder can be an enemy in a battlefield, or a malicious moving object in the area of interest. Same detection probability is used in the uniform distribution modeled WSN. Intrusion detection systems are used to detect malicious nodes in the sensor network. Dynamic parameter selection based detection scheme is used to improve the detection accuracy. Integrated coverage based cluster scheme is used to enhance the intrusion detection system. In the immediate intrusion detection model the intruders are detected before any movement in the WSN. In the relaxed intrusion detection model the intruders are detected after some movements in the WSN.The system supports fault tolerant detection schemes. Malicious attack controlling model is used in the system. Traffic overhead is reduced by the IDS scheme. Intrusion detection is provided for different deployment scheme.

REFERENCES

[1]. P. Medagliani, J. Leguay, V. Gay, M. Lopez-Ramos, and G. Ferrari, “Engineering Energy-Efficient Target Detection Applications in Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Pervasive Computing and Comm. (PerCom), pp. 31-39, 2010.
[2]. Y. Wang, Y.K. Leow, and J. Yin, “Is Straight-Line Path Always the Best for Intrusion Detection in Wireless Sensor Networks,” Proc. Int’l Conf. Parallel and Distributed Systems, pp. 564-571, 2009.
[3]. 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.
[4]. 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.
[5]. 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.
[6]. Y. Wang, F. Li, and F. Fang, “Poisson versus Gaussian Distribution for Object Tracking in Wireless Sensor Networks,” Proc. Second Int’l Workshop Intelligent Systems and Applications (ISA), pp. 1-4, 2010.
[7]. 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.
[8]. 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.
[9]. 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.
[10]. 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.
[11]. L. Lazos, R. Poovendran, and J. Ritcey, “Analytic Evaluation of Target Detection in Heterogeneous Wireless Sensor Networks,” ACM Trans. Sensor Networks, vol. 5, no. 2, article 18, 2009.

[12]. X. Bai, Z. Yun, D. Xuan, W. Jia, and W. Zhao, "Pattern Mutation in Wireless Sensor Deployment," Proc. IEEE INFOCOM, pp. 1-9, 2010.
[13]. 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.
[14]. 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, February 2013.
[15]. Y. Wang, Y. Leow, and J. Yin, "A Novel Sine-Curve Mobility Model for Intrusion Detection in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, 2011.
[16]. E. Yanmaz and H. Guclu, "Stationary and Mobile Target Detection Using Mobile Wireless Sensor Networks," Proc. IEEE INFOCOM, 2010.