Said and Elnashar *EURASIP Journal on Wireless Communications and Networking* (2015) 2015:46
DOI 10.1186/s13638-015-0240-6

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Scaling of wireless sensor network intrusion detection probability: 3D sensors, 3D intruders, and 3D environments

Omar Said[1,3*†] and Alaa Elnashar[2,3†]

Abstract

In this paper, a new model that deploys heterogeneous sensors in 3D wireless sensor networks (WSNs) is proposed. The model handles the two sensing scenarios, single sensing and multiple sensing. The probabilities of intrusion detection in a 3D environment with sensors distributed using Gaussian, uniform, beta, and chi-square are compared. The resultant probabilities values help the WSN security designers in selecting the most suitable sensors deployment regarding some critical network parameters such as quality-of-service (QoS). WSN efficiency under different probabilistic distributions is also demonstrated. To evaluate the proposed model, a simulation environment is constructed using OPNET and NS2. The simulation results showed that Gaussian distribution provides the best efficiency and performance.

Keywords: WSN; WSN security; Intrusion detection; QoS; 3D sensor applications

1 Introduction

Wireless sensor networks (WSNs) consist of small main components which have limited power devices such as sensors and can be installed in open environments [1-3]. So, WSNs may be attacked by intruders. Since WSNs applications are used in different fields such as environmental sensing, industrial monitoring, and military process management, intrusion detection became an extremely important issue [4,5]. In WSN, a huge number of sensors should 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 [6-8]. The second one detects the intruder when it tries to storm unauthorized area [9-13]. 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. Also, wired network contains many intrusion detection systems which are not accommodating the nature of WSNs [14-17]. Consequently, developing an innovative technique that deals with WSNs nature is an important issue. Furthermore, finding the optimal representation of sensor deployment that provides the best intruder detection is another important issue. In this paper, a model for intrusion detection in 3D environments is introduced. The model uses various probability distributions to deploy sensors within the entire WSN. A simulator is created to simulate the intrusion detection process and evaluate its efficiency based on the probability distribution used. This will guide the WSN designer to select the optimal sensors distribution that yields the best intrusion detection efficiency. The paper is organized as follows: in Section 2, the problem definition is introduced. In Section 3, the related works are demonstrated. In Section 4, the proposed model

*Correspondence: dr_osaid@yahoo.com
†Equal contributors
[1] Department of Computer Science, College of Science, Menofia University, Shebin El Kom, Gamal Abdelnaser St., 32512, Menofia, Egypt
[3] College of Computers and Information Technology, Taif University, Al-Hawyia, 21974, Taif, Saudi Arabia
Full list of author information is available at the end of the article

is presented. In Section 5, the simulation environment is constructed and the results are discussed. Finally, conclusion and future work are introduced in Sections 6 and 7, respectively.

2 Problem definition

WSNs consist of large number of inter communicated sensors via wireless interfaces. These sensors may have various processing capabilities, computing resources, or coverage scenarios. Many WSN applications contain different types of sensors which are used in different types of tasks. Also, there are many applications that are not only used in 2D environment but also in 3D space. The problem of intrusion detection has not been studied extensively in the case of heterogeneous WSNs sensors and also in the case of 3D environments because of its complexity. Also, the effect of mobile sensors on the heterogeneous WSNs is not studied. So, till now, there is no standard model that helps security designers in selecting a suitable sensors distribution that accommodates the nature of WSN 3D applications and available network specifications.

The problem is defined as follows: find the best distribution of network sensors that minimizes the probability value $Pr(V_S \subset (\cup_{m-1}^{n} V_{I_m}))$ or maximizes $Pr((\cup_{m-1}^{n} V_{I_m}) \cap V_S = \emptyset)$, where V_S is the space volume that is covered by a network sensor S, and V_I is the space volume that is covered by an intruder I, see Figure 1.

For simplification, suppose one sensor S and one intruder I. The sensor S covers the volume V_S that is represented by a sphere of radius R_S centered at V_S center $= (x_1, y_1, z_1)$. The intruder I covers the volume V_I that is represented by a sphere of radius R_I centered at V_I center $= (x_2, y_2, z_2)$.

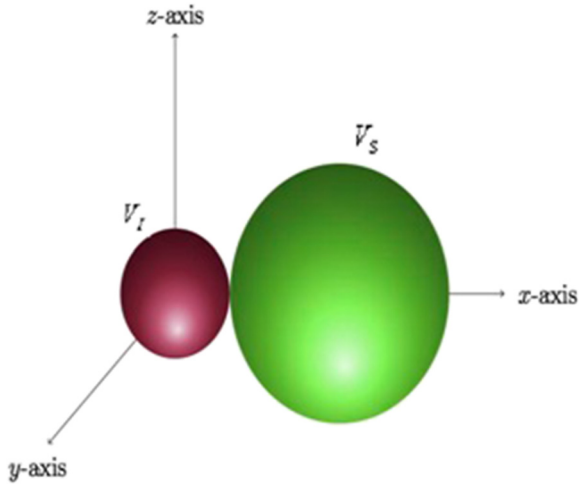

Figure 1 Sensor/intruder spaces in 3D.

3 Related works

WSN intrusion detection is a challenging process since it can be affected by several parameters such as number of sensors, sensor types, quality-of-service (QoS), detection cost, and WSN environment. Few studies have been introduced to solve the intrusion detection problem in different environments with different types of sensors. These studies can be classified into two categories. The first one manipulates the detection problem with different factors rather than the factors that are presented in this paper. The second category is close related work, which tried to study this problem under nearby parameters of the proposed idea but with different problem definitions and models.

3.1 General related work

Several models and studies were presented to handle intrusion detection problem. Anomaly-detection-based model with statistical analysis [18] was introduced for intrusion detection in *ad hoc* network. The model takes a long time to detect the intruder due to huge transmitted data and traffic. In [19], a framework, which enables the network designer to select the optimized intruder detection system according to his particular needs, is proposed. In [20], a method for detecting packet modification attacks and supporting target node location privacy is proposed. Moreover, accuracy of this proposed method is evaluated using small-scale WSN. Detection of a moving intruder in a curved path was studied in [21]. The technique uses sine function to define the moving curve of the intruder with detection probability in WSN. Regarding heterogeneous WSNs with the Gaussian distribution, it was proved that the probability of intrusion detection (PID) increases as the number of sensors increases [22]. The probability of intruder detection in homogeneous and heterogeneous WSNs with consideration of density and sensing range for each WSN node was studied in [23]. A comparison between the performance of WSN with Gaussian and Poisson probability distribution under different network settings was presented in [24]. The area covered by WSN at the exact time or within certain time interval in addition to calculating the time that have been consumed to detect a randomly sited inactive object was proposed in [25]. In [26], the relation between the intrusion detection time and the distance, which the intruder cuts down from the start point until hacking the field of interest, is determined. Furthermore, [27] showed that lack of sensors can be compensated by sensor mobility which improved network coverage. Some other ideas such as furtive wireless communication have been demonstrated in [28].

3.2 Closely related work

There are three close researches to the proposed idea. The first one [29] implemented Gaussian and uniform

distributions to determine the probability of intruder detection in WSN. The proposed technique in distinguished between the detection probability as regards the requirements of each WSN application and the network parameters. In addition, the proposed system was studied under two scenarios: single sensing detection and multiple-sensing detection. But this proposed technique did not study the 3D environment under heterogeneous WSN. The second close research proposed a technique that combines Gaussian and Poisson probability distributions [30]. Gaussian distribution was applied to the central area covered by WSN. Poisson distribution was applied to the remaining area. Therefore, this technique is considered as a mixture of two probability distributions in one test area. Also, this technique supposed that the WSN contains heterogeneous sensors. But the tested environment was not in 3D space. Furthermore, it should test each probability distribution independently on the WSN area before proposing a mixture of them. The last one proposed an analysis for intrusion detection problem in a 3D environment that is represented by a cube with two types of sensors [31]. This technique has some drawbacks such as the probability density function is not calculated and a cube is not sufficient to prove the model results. In addition, this proposed model is not well defined.

4 The proposed model

Since many applications are applied in 3D environment, optimizing sensor distribution to enhance intrusion detection probability should be considered. In addition, sensor heterogeneity is also another important parameter that should be well studied since most of the intrusion detection researches focus on using homogenous sensors. The main purpose of the proposed model is to analyze the intrusion detection probability, which helps in sensor deploying, to gain a satisfied WSN security level. The effect of the used probability distribution such as Gaussian, uniform, beta, and chi-square are also studied. Figure 2a,b shows samples from sensors distribution views using uniform and normal. Reducing communication redundancy can be achieved by intelligent sensor deployment in WSN. The proposed model deals with four components, a 3D environment within which the WSN should be installed, 3D sensors that are used to detect an intruder, 3D intruder(s) which is (are) predicted to hack WSN, and a target resource that is assumed to be protected by WSN sensors. The 3D environment is represented by a cubic space with predefined dimensions. Sensors, intruders, and targets are presented as sphere centers as shown in Figure 3a. Sensors are heterogonous since each sensor is assumed to be located at a sphere center with a predefined radius that may differ from other sensors radii as shown in Figure 3b. Each sensor covers its entire sphere volume space and is allocated dynamically. Each intruder is also represented as in case of sensors, and its sphere space represents the intrusion space as shown in Figure 3c. Target space is the sphere volume that is required to be protected. The target is hacked by a specific intruder if it is located outside any of sensors coverage spaces, and its distance from the intruder is less than or equal the sum of the intruder sphere and its sphere radii as shown in Figure 3d; otherwise, it is considered to be safe as shown in Figure 3e,f. The steps of the proposed model are described in Algorithm 1 shown below.

Algorithm 1

D_m is the minimum distance
I: Intruder and T: Target
M: The number of intruders
N: The number of sensors
D_{jT}: Intruder/Target distance
D_{TSi}: Nearest Sensor/Target distance
Suppose Dm = 0, F = 0.
I position is random.
T position is random.
Let D_m = X
The nearest sensor from target is in the same direction of intended intruder.
For each Gaussian, uniform, beta, and chi-square
Begin
While (F $\prec$ M)
Begin
For j = 1 TO M
Begin
For i = 1 to N
Begin
If ($D_m \succ D_{iT}$)
$D_m = D_{iT}$
End
S_i = 1 (Flaged)
If (D_{jT} = = D_{TSi})
Print 'Middle State.'
ElseIF $D_{jT} \succ D_{TSi}$
Print 'Save State.'
ElseIF $D_{jT} \prec D_{TSi}$
Print 'Hacking State.'
End
For K = 1 to M
Begin
If (($I_k \cap S_j \neq \Phi$), j=2 to n)
Print 'Detection process is distributed over multi sensors
depending on the overlapped volume spaces.'
End
F = F+1.
End
End

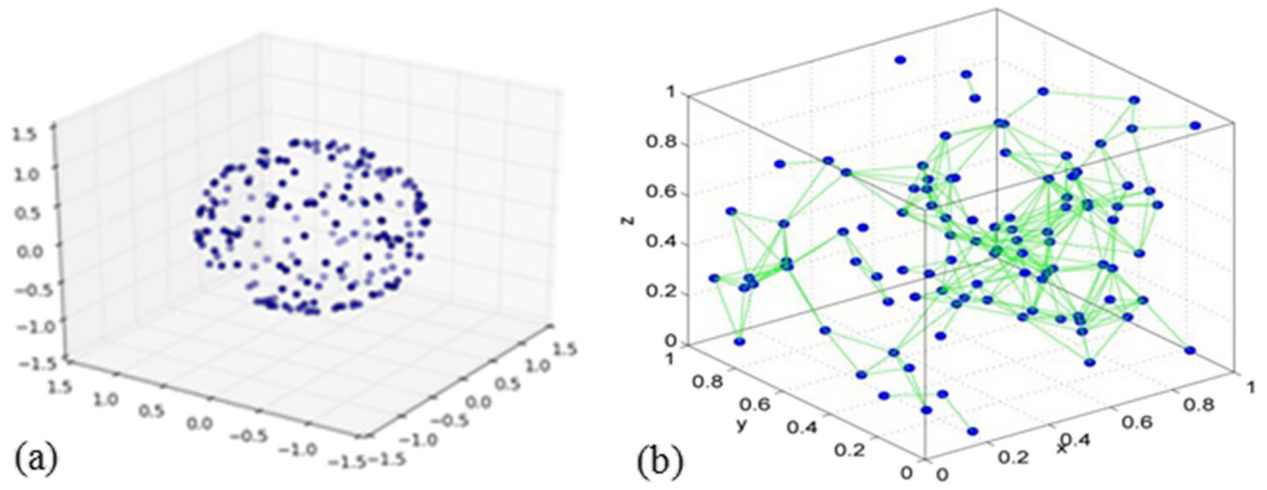

Figure 2 Samples from sensor distribution views. (a) Sensors with uniform distribution in 3D [32]. **(b)** Sensors with normal distribution in 3D [33].

5 Simulation and evaluation

A simulator has been developed to simulate the intrusion detection process with multiple intruders in 3D environment with sensors that are distributed by using various probability distributions. The simulator is also designed to evaluate the proposed model. The evaluation is based on the effect of the used probability distributions on efficiency of WSN and also the network parameters such as packet loss, end-to-end delay, and throughput. The simulation parameters and their values are listed in Table 1.

OPNET 14.5 and NS2 [34,35] are used to simulate a 3D environment that contains ZigBee with its three layers: application, media access control (MAC), and network. In the MAC layer, the 802.15.4 MAC protocol is used in addition to the ZigBee (CSMA/CA) model [34]. The network layer is implemented by the ZigBee network model, which is used in the routing and request handling.

In the simulated environment, each 3D camera is attached to one sensor to reflect the 3D nature. The simulator is built on large scale as shown in Table 1 and includes different numbers of Zigbee end devices, coordinators, and routers. WSN sensors are communicated via infrared media using star topology and distributed using Gaussian, uniform, beta, and chi-square. Configuring WSN model components and selecting the scalable parameters for the entire simulated WSN are accomplished.

5.1 Intruder detection efficiency evaluation

Suppose that the volume space covered by a network sensor is V_s and the volume space covered by intruder is V_i. $P_r(V_i \cap V_s)$ is the coverage spaces intersection probability of an intruder and a sensor. If this probability equals ϕ, then the system is safe and there is a distance between the intruder and its target. So, this probability should be maximized. $P_r(V_i \cap V_s)$ is the worst probability because the intruder is around to reach its target and hack the security system. So, this probability should be minimized. The distance between the target and an intruder and also its velocity are two factors that are used to determine the time consumed by the intruder to hack the target. Knowing this time value enables the security system manager to protect the target against hacking. In the proposed simulation, the values of intruders' velocities and their distances from the target are randomly generated. Equations 11 to 4 are for Gaussian, uniform, beta, and chi-square probability distributions, respectively [29,36,37]. Equation 5 describes how to extract the time from the intruder velocity and the current distance between the intruder and his target [38]. Equation 6 describes the relationship between the intruder and the sensors spheres in the security domain [39].

To evaluate the efficiency of intruder detection process, a simulator with 800 3D sensors covering 3D environment and two 3D intruders is used. The positions of both the target and intruders are created randomly in the simulated environment. The distance between the intruder and the target in addition to the distance between the intruder and the nearest sensor to the target are considered [26].

Two experiments were carried out using this simulated environment. In the first experiment, the values of the distance between the intruder and the target and also the distance between the intruder and the nearest sensor to the target are ignored, in contrast to the second one that considered these values.

Figure 4 shows the simulation results of the first experiment. The results show that Gaussian sensor distribution provides the best average performance for all the numbers of sensors except for 400 sensors. A lower performance is provided in case of using uniform sensor distribution

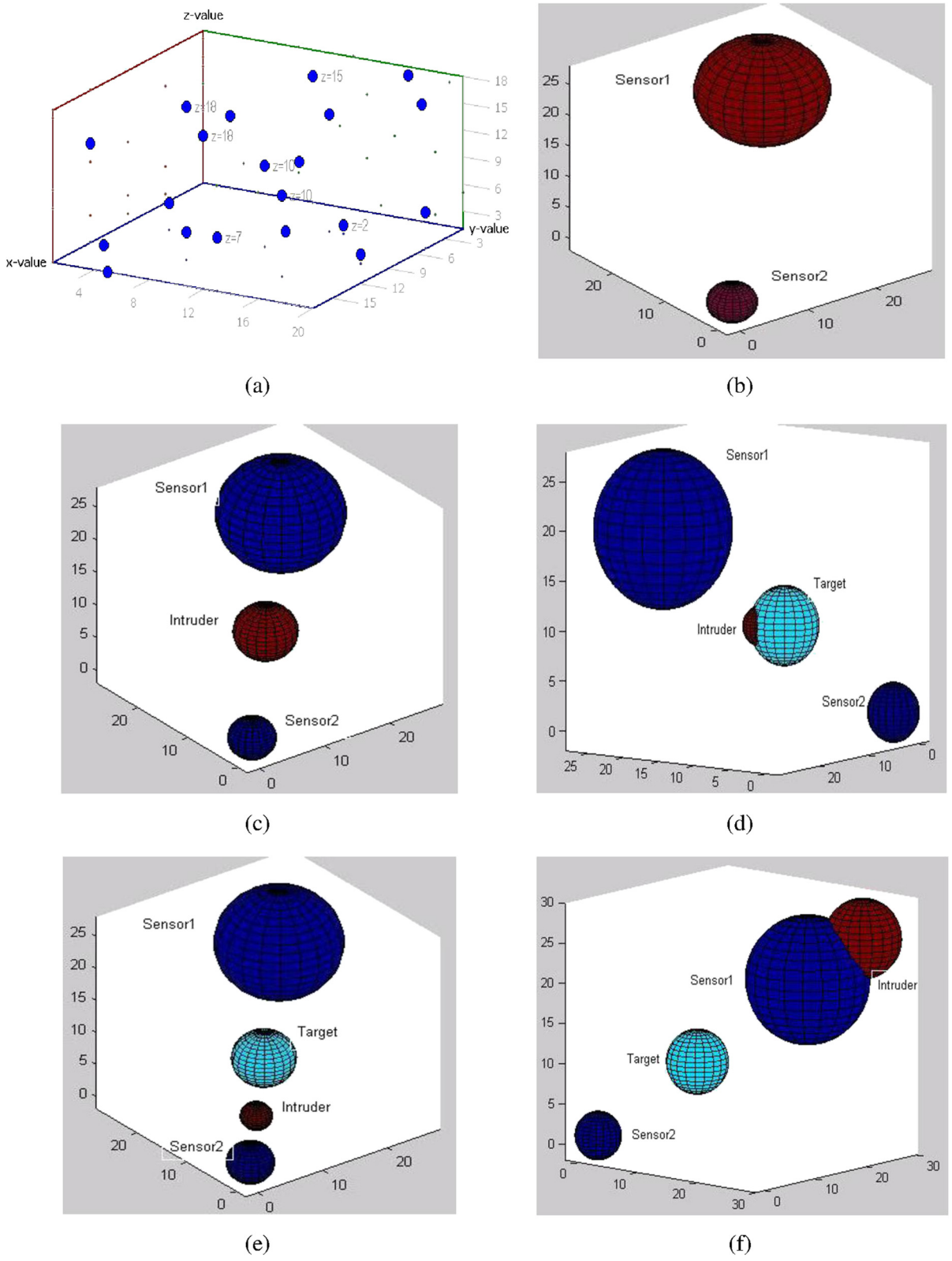

Figure 3 3D environment with sensor distributions and samples of intruder/sensors/target states. (a) 3D environment with sensors spheres centers. **(b)** Two heterogeneous sensors coverage spaces. **(c)** Two heterogeneous sensor and an intruder representation. **(d)** Hacked target. **(e)** Safe target - no intruders detected. **(f)** Safe target - an intruder detected.

Table 1 Simulation parameters and their values

Simulation parameter	Value
Packet size	1,024 Bytes
Destination	Random
Packet inter-arrival time	Constant (1.0)
Simulation time	2 h
Simulation time	2 h
Battery life	3 to 4 h [active sensing] and 1,000+ h [standby]
Start time	Uniform (20, 21)
Transmission range	1 to 100 m
ACK mechanism	Enabled
3D camera	170 (W) × 54 (H) × 49 (D) mm
MAC layer	802.15.4
Transmit power	0.05 mw/m^3
Transmit band	2.4 GHz
Environment space volume	10 × 10 × 10 km^3

especially for 100 and 700 sensors. Beta and chi-square distributions have the lowest average performance values. Figure 5 shows the simulation results of experiment 2. The results show that Gaussian sensors distribution provides the best average performance for all the numbers of sensors. A lower performance is provided in the case of using uniform sensor distribution. Beta and chi-square distributions have the lowest average performance values.

Gaussian [29]

$$f(x,\mu,\sigma) = \frac{1}{\sigma\sqrt{2\Pi}} e^{\frac{(x-\mu)^2}{2\sigma^2}} \tag{1}$$

Uniform [29]

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

Beta [36]

$$f(x,\alpha,\beta) = \frac{1}{B(\alpha,\beta)} x^{\alpha-1}(1-x)^{\beta-1} \tag{3}$$

Chi-square [37]

$$f(x,k) = \begin{cases} \frac{x^{\frac{k}{2}-1} e^{\frac{-\Pi}{2}}}{2^{\frac{k}{2}}\Gamma\left(\frac{k}{2}\right)} & x \geq 0 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

Time extraction [38]

$$T = \frac{D}{V} \tag{5}$$

Spheres intersection [39]

$$\frac{4d^2R^2 - (d^2 - r^2 - R^2)^2}{4d^2} \tag{6}$$

5.2 Evaluation of WSN sensor distribution

It is obvious that if the WSN efficiency is not acceptable, the intruder may be detected but the security system may fail to recover this problem. To complete a test of the proposed model efficiency, the cycle after the intruder detection process should be evaluated. This cycle means that

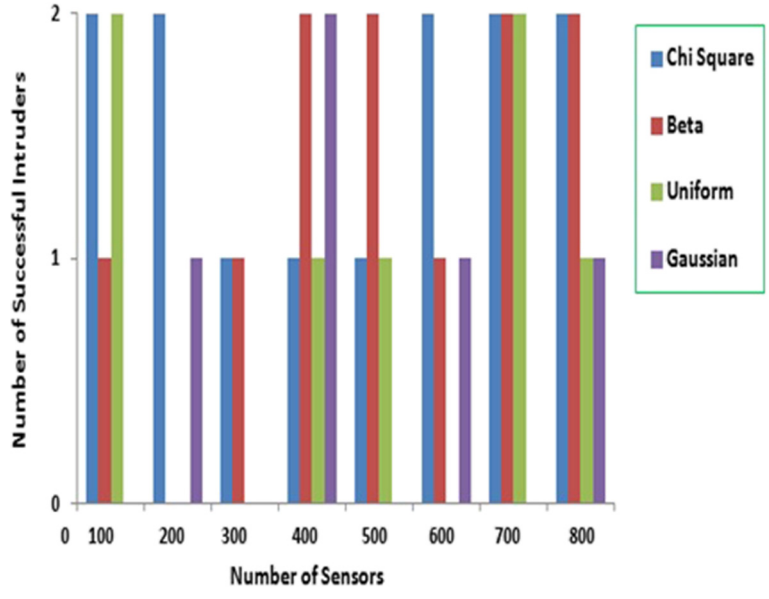

Figure 4 The simulation results of the first experiment. Number of successful intruders for each distribution without considering distance and velocity parameters.

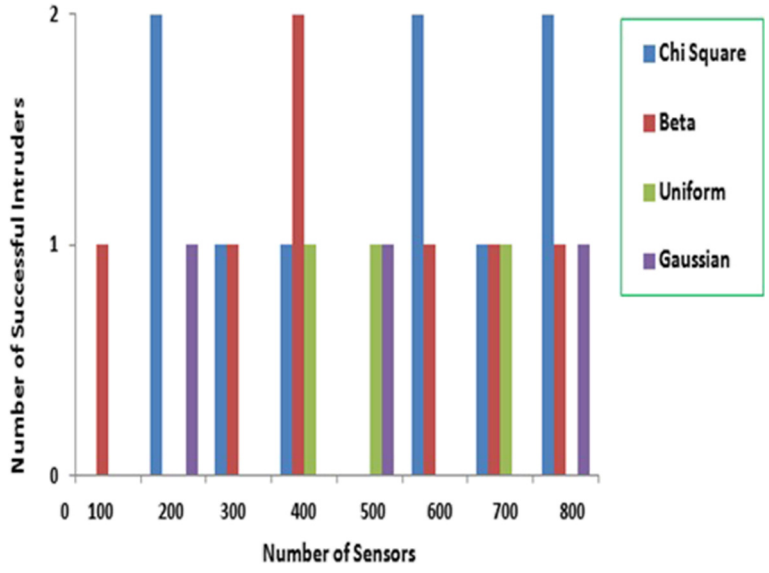

Figure 5 The simulation results of the second experiment. Number of successful intruders for each distribution with considering distance and velocity parameters.

data, which are sent to inform the security manager with intruder, should be transmitted successfully. So, the WSN efficiency should be evaluated. The evaluation parameters are the average number of control bits, the number of hops, the average number of lost packets, the end-to-end delay, the throughput, and the general efficiency. In the following subsections, the simulation environment is constructed and each parameter results is showed and discussed.

5.2.1 Average number of control bits

During simulation execution, trace files containing the number of control bits are created instantly for the number of used sensors. The control bits are the retransmitted bits, the ACK bits and the bits which are used to initiate the sessions between WSN sensors in case of sudden event occurrence such as intruder detection. In general, as the number of management bits decreases, the energy consumption decreases and sensors battery live increases.

Figure 6 shows the transmission control data for different WSNs sensors distributed using Gaussian, uniform, beta, and chi-square. The simulation results indicate that Gaussian WSN has the minimum number of management bits compared with other WSNs in contrast to chi-square WSNs that have the maximum number of control bits.

5.2.2 The number of hops

The routing path is determined by the number of hops, which are used in data transmission. So, the number of transmission hops is an important factor in determining the best routing paths and their alternatives.

Figure 7 shows that the number of hops used in the Gaussian WSN is less than the number of hops used in the other WSNs (uniform, beta, and chi-square). When the number of sensors equals 600, the Gaussian WSN and the uniform WSN have the same number of transmission hops. The hesitations in curve plots are owed to the randomly chosen sources and destinations in the WSNs. In addition, failure of multiple sensor nodes may cause data collision which requires alternative nodes to complete the transmission process that increases the number of hops. Furthermore, when the number of sensors is greater than 300, the plots' values are decreased. This occurs because the data, which are transmitted within the WSN at this number of sensors, use the best routing path. The simulation results indicate that the Gaussian WSN uses the minimum number of hops compared with the other WSNs. In contrast, the beta and the chi-square WSNs have the maximum number of used hops.

5.2.3 The average number of lost packets

In the general networks, it is well known that the transmitted data increases when the number of nodes increases which may cause more packet loss [40]. In WSNs, there is a slight difference; the amount of transmitted data depends on the sensor-acquiring information when urgent events occurred [40]. Also, the number of lost packet affects the network efficiency. So, the number of packet loss should be monitored. Figure 8 shows the average number of lost packets for different WSNs sensors distributed by using Gaussian, uniform, beta, and chi-square distributions. The simulation results indicate

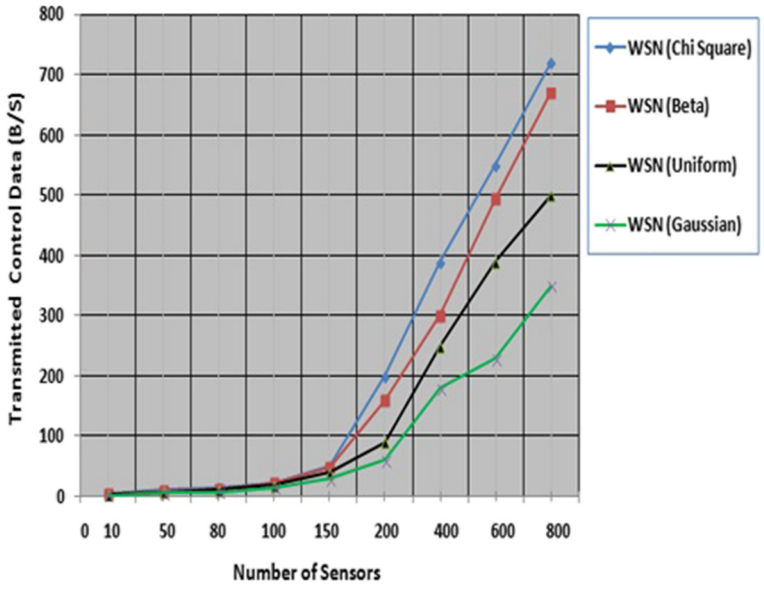

Figure 6 Transmission control data for different WSNs (Gaussian, uniform, beta, and chi-square).

that the number of sensors does not negatively affect the number of lost packets for a medium number of sensor ($\leq$300) for all simulated WSNs. For a large number of sensors ($>$300), the average number of lost packets exponentially increases as the number of sensors increases in case of beta and chi-square WSNs in contrast to Gaussian and uniform WSNs, in which the average number of lost packets increases slowly as the number of sensors increases.

5.2.4 Average end- to-end delay

The end-to-end delay is defined as the total time, which is consumed in packet transmission from source to destination [40]. The end-to-end delay is measured by a time difference between message buffering time at the source and the time of receiving the last bit at the destination. Figure 9 shows the average end-to-end delay for different WSNs sensors distributed by using Gaussian, uniform, beta, and chi-square distributions. The simulation results

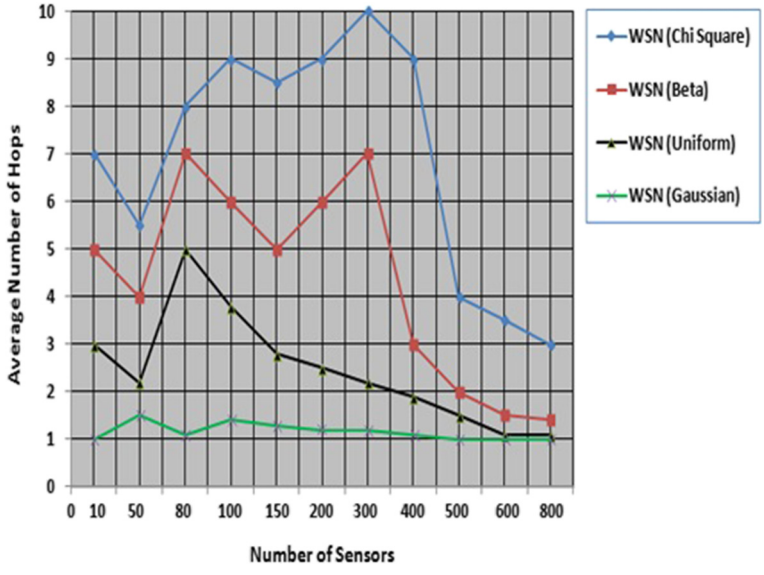

Figure 7 Average number of hops for different WSNs (Gaussian, uniform, beta, and chi-square).

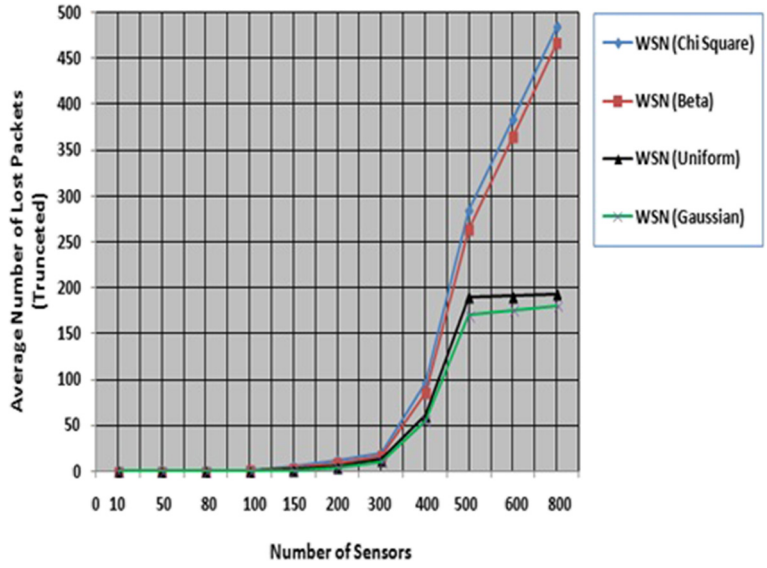

Figure 8 Average number of packet loss for different WSNs (Gaussian, uniform, beta, and chi-square).

indicate that uniform and Gaussian WSNs have the minimum average delay, respectively, compared with the other WSNs. Chi-square and beta WSNs have the maximum delay. The interpretation for these results is that in case of the uniform and the Gaussian WSNs, little number of hops are used to transmit the data from source to destinations; this decreases the total time of hops data handling which leads to less end-to-end delay. On the other hand, the beta and the chi-square WSNs routing paths use more hops to transmit the required data from source to destinations (including sinks) which leads to an increased end-to-end delay.

5.2.5 Throughput

Throughput is defined as the correct transmitted data with a specific quality from source to destination within a time interval [40]. Increased number of sensors used in WSNs makes analysis of QoS parameter an important issue. There are many factors affecting the WSN throughput such as packet loss, end-to-end delay, energy con-

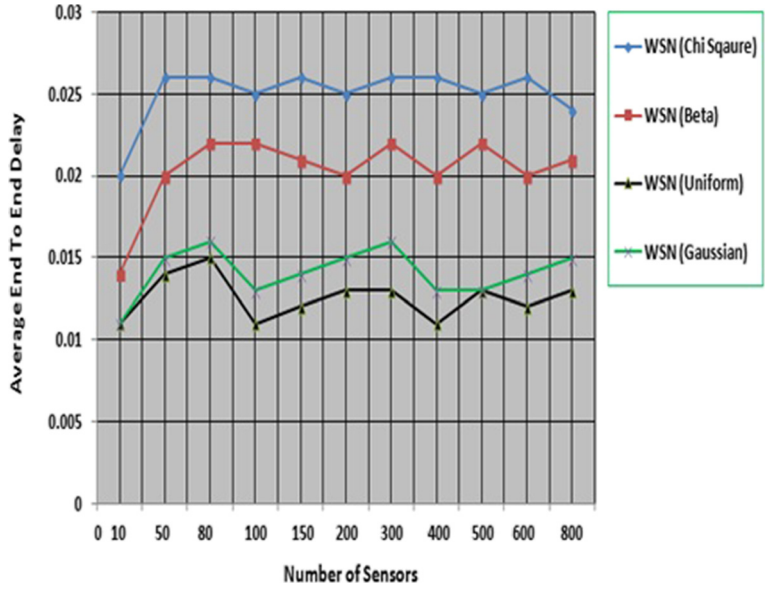

Figure 9 Average end-to-end delay for different WSNs (Gaussian, uniform, beta, and chi-square).

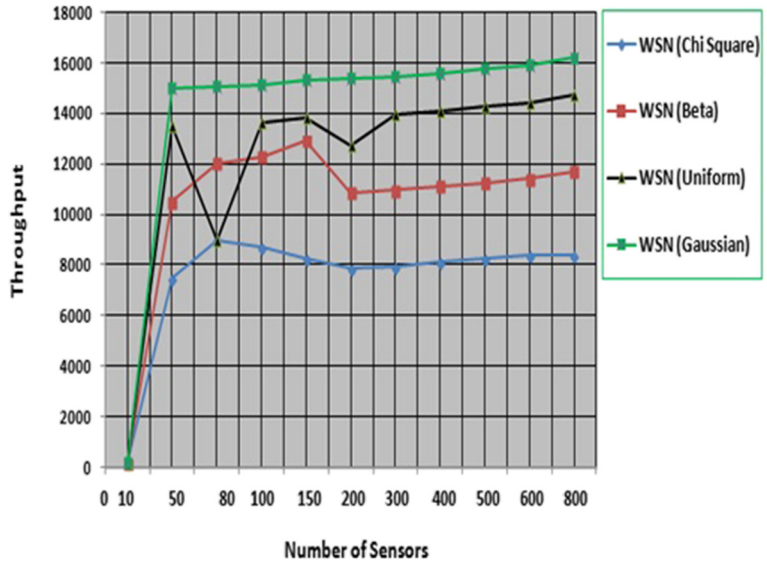

Figure 10 **Throughput for different WSNs (Gaussian, uniform, beta, and chi-square).**

sumption, long distance, and obstacles. Figure 10 shows the throughput for different WSNs sensors distributed by using Gaussian, uniform, beta, and chi-square distributions. The simulation results indicate that Gaussian WSN achieves the maximum throughput, the second highest throughput is achieved by uniform WSN, and beta and chi-square WSNs have the lowest throughput. The interpretation for these results is that Gaussian and uniform WSN have direct sensor communication and high QoS paths. Furthermore, the WSN task may be shared among multiple sensors due to sensor overlaps as a result of less collisions and packet drops. On the other hand, beta and chi-square WSNs have complex paths as a result of higher collisions and packet drops take place as a result of which the throughput is minimum. Also, energy consumption makes some sensors not to provide their services; so other alternative routes should be generated to complete the routing process.

5.2.6 General efficiency

The general efficiency of the entire system is defined by a relationship between the numbers of events which are handled by sensors in one WSN in proportion to other WSNs regarding some parameters such as end-to-end

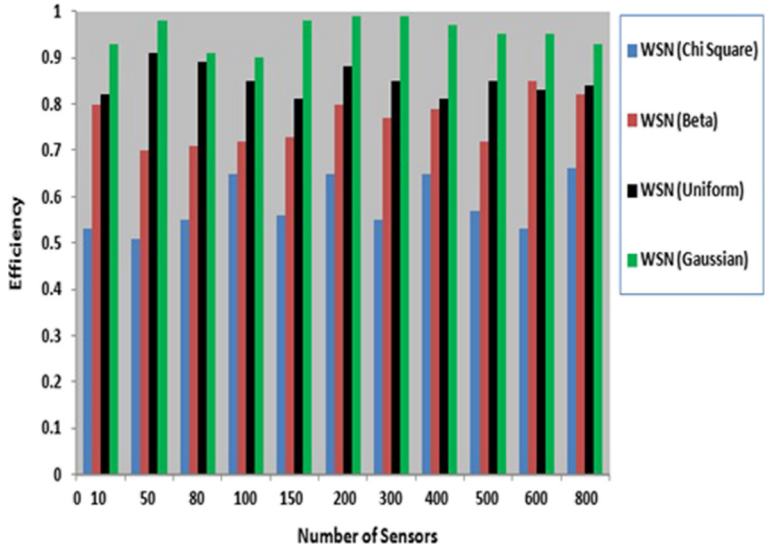

Figure 11 **General efficiency for different WSNs (Gaussian, uniform, beta, and chi-square).**

delay, packet loss, throughput, and path complexity. The simulation results in Figure 11 show that Gaussian WSN has the best efficiency and then uniform WSN. Beta and chi-square WSNs have the lowest efficiency. The general efficiency parameter is considered as cumulative result which summarizes all the previous results. Also, all previous results and final recommendation are summarized in Table 2.

6 Conclusions

In this paper, a new model for WSN intruder detection in 3D environment is proposed. Each element in the security system is represented by a center of various radii spheres. Sensors are distributed in the 3D environment using Gaussian, uniform, beta, and chi-square. The security status (hacked or safe) is determined by three parameters, the intruder/target and nearest sensor/target distances, the intruder velocity, and the relationship between spheres (intruder and sensors). The proposed model handles both detection scenarios, single and multiple. Two approaches of evaluations are presented. The first one concerns with WSN security issue. The second approach concerns with network parameters such as average number of control bits, the number of hops, the average number of lost packets, the end-to-end delay, the throughput, and the general efficiency.

The results showed that Gaussian WSN have the best performance in both evaluation approaches, then uniform WSN. The beta and the chi-square WSNs have the lowest performance. Also, the end-to-end delay is the only parameter where the uniform WSN provides better performance than the Gaussian WSN. Simulation results of the proposed model show that Gaussian sensors distribution in WSN is recommended in 3D environments.

6.1 Future work

Mixed probability distributions of sensors in WSN (i.e., Gaussian/uniform, Gaussian/beta, or more mixtures) should be studied and tested. Accordingly, the results should be compared with those of this paper. This will

Table 2 Results summarization and final recommendation

Distribution	WSN efficiency evaluation		Intruder detection evaluation		Final recommendation
Gaussian	Control data size	HP	Without considering distant	HP	Using Gaussian to distribute the sensors in WSN gives the best performance as regards intruder detection probability and overall WSN efficiency, then uniform, beta, and chi-square
	Number of hops	HP			
	Packet loss HP				
	End-to-end delay	LPR2			
	Throughput	HP	With considering distant	HP	
	General efficiency	HP			
Uniform	Control data size	LPR2	Without considering distant	LPR2	
	Number of hops	LPR2			
	Packet loss	LPR2			
	End-to-end delay	HP			
	Throughput	LPR2	With considering distant	LPR2	
	General efficiency	LPR2			
Beta	Control data size	LPR3	Without considering distant	LPR3	
	Number of hops	LPR3			
	Packet loss	LPR3			
	End-to-end delay	LPR3			
	Throughput	LPR3	With considering distant	LPR3	
	General efficiency	LP			
Chi-square	Control data size	LP	Without considering distant	LP	
	Number of hops	LP			
	Packet loss	LP			
	End-to-end delay	LP			
	Throughput	LP	With considering distant	LP	
	General efficiency	LP			

HP: highest performance. LPR2: lower performance-rank2. LPR3: lower performance-rank3. LP: lowest performance.

provide a standard sensor distribution. Also, the number of sensors, which are used in the simulation environment, should be larger. In addition, a tracer system for an intruder may be added to the proposed model for system security integrity.

Competing interests
The authors declare that they have no competing interests.

Acknowledgements
I would like to pay special thanks and appreciation to the persons who made our research successful.

Author details
[1]Department of Computer Science, College of Science, Menofia University, Shebin El Kom, Gamal Abdelnaser St., 32512, Menofia, Egypt. [2]Department of Computer Science, College of Science, Minia University, Ibrahimia St., 61519, Minia, Egypt. [3]College of Computers and Information Technology, Taif University, Al-Hawyia, 21974, Taif, Saudi Arabia.

Received: 29 July 2014 Accepted: 2 January 2015
Published online: 03 March 2015

References

1. Y Luo, S Morgera, R Sankar, in *proceedings of the 2nd IEEE International Conference on Information Science and Engineering (ICISE)*. A survey on intrusion detection of wireless sensor network (China, 4–6 Dec 2010), pp. 1798-1802
2. Y Akyildiz, S Weilian, Y Sankarasubramaniam, E Cayirci, A survey on wireless sensor networks. IEEE Commun. Mag. **40**(8), 102–114 (2002)
3. K Sohraby, D Minoli, T Znati, Wireless sensor networks: technology, protocols, and applications, 12-68 (2007)
4. J Al-Karaki, A Kamal, E Cayirci, Routing techniques in wireless sensor networks: a survey. IEEE Wireless Commun. **11**(6), 6–28 (2004)
5. S Tilak, N Abu-Ghazaleh, A taxonomy of wireless micro-sensor network models. ACM Mobile Comput. Commun. Rev. **6**(2), 28–36 (2002)
6. A Agah, S Das, K Basu, M Asadi, in *proceedings of the Third IEEE International Symposium on Network Computing and Applications (NCA)*. Intrusion detection in sensor networks: a non-cooperative game approach (USA, January 30 Aug), pp. 343-346
7. A Agah, S Das, K Basu, *A game theory based approach for security in wireless sensor networks*, (USA, Unknown Month 15), pp. 259-263
8. V Giruka, M Singhal, J Royalty, S Varanasi, Security in wireless sensor networks. Wiley Wireless Commun. Mobile Comput. **8**(1), 1–24 (2008)
9. A Arora, P Dutta, S Bapat, V Kulathumani, H Zhang, V Naik, V Mittal, H Cao, M Demirbas, M Gouda, A line in the sand: a wireless sensor network for target detection, classification, and tracking. Int. J. Comput. Telecommun. Networking-Special Issue: Mil. Commun. Syst. Technol. **46**(5), 605–634 (2004)
10. H Solimana, N Hikalb, N Sakrb, A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks. Elsevier Egypt. Inform. J. **13**(3), 225–238 (2012)
11. S Sachan, M Wazid, P Singh, H Goudar, *A cluster based intrusion detection and prevention technique for misdirection attack inside WSN*, (India, May 3), pp. 795-801
12. H Kung, D Vlah, Efficient location tracking using sensor networks. Proceedings of IEEE International Conference on Wireless Communications and Networking (WCNC), 1954-1961 (Unknown Month 20)
13. C Lin, W Peng, Y Tseng, Efficient in-network moving object tracking in wireless sensor networks. IEEE Trans. Mobile Comput. **5**(8), 1044–1056 (2006)
14. Y Albagory, O Said, Performance enhancement of high-altitude platforms wireless sensor networks using concentric circular arrays. Elsevier AEU-Int. J. Electronics Commun. **69**(1), 382–388 (2015)
15. T Yang, D Mu, W Hu, H Zhang, Energy-efficient border intrusion detection using wireless sensors network. Springer EURASIP J. Wireless Commun. Netw. **1**, 1–12 (2014)
16. R Mitchell, I Chen, A survey of intrusion detection in wireless network applications. Elsevier Comput. Commun. J. **42**, 1–23 (2014)
17. C Lin, W Chen, Y Tseng, Efficient in-network moving object tracking in wireless sensor networks. IEEE Trans. Mobile Comput. **5**(8), 1044–1056 (2006)
18. Y Zhang, W Lee, *Intrusion detection in wireless ad-hoc networks*, (USA, November 6), pp. 275-283
19. A Stetsko, T Smolka, V Matyas, Improving intrusion detection systems for wireless sensor networks. Springer Appl. Cryptography Netw. Secur. Lect. Notes Comput. Sci. **8479**, 343–360 (2014)
20. J Kur, V Matyas, A protocol for intrusion detection in location privacy-aware wireless sensor networks. Springer Trust Privacy Secur. Digital Bus. Lecture Notes Comput. Sci. **8647**, 180–190 (2014)
21. Y Wang, Y Leow, J Yin, *Is straight-line path always the best for intrusion detection in wireless sensor networks*, (China, November 8), pp. 564-571
22. Y Wang, W Fu, D Agrawal, *Intrusion detection in Gaussian distributed heterogeneous wireless sensor networks*, (USA, Summer 12), pp. 313-321
23. Y Wang, X Wang, B Wang, D Agrawal, Intrusion detection in homogeneous and heterogeneous wireless sensor networks. IEEE Trans. Mobile Comput. **7**(6), 698–711 (2008)
24. Y Wang, F Li, F Fang, *Poisson versus Gaussian distribution for object tracking in wireless sensor networks*, (China, Unknown Month 22), pp. 1-4
25. B Liu, P Brass, O Dousse, P Nain, D Towsley, *Mobility improves coverage of sensor networks*, (USA, Unknown Month 25), pp. 300-308
26. O Dousse, C Tavoularis, P Thiran, *Delay of intrusion detection in wireless sensor networks*, (Italy, Unknown Month 22), pp. 155-165
27. S Qiong, C Comaniciu, *Efficient cooperative detection for wireless sentinel networks*, (USA, Unknown Month 17), pp. 1-6
28. D Turgut, B Turgut, L Boloni, *Stealthy dissemination in intruder tracking sensor networks*, (Germany, Unknown Month 20), pp. 22-29
29. Y Wang, W Fu, D Agrawal, Gaussian versus uniform distribution for intrusion detection in wireless sensor networks. IEEE Trans. Parallel Distributed Syst. **24**(2), 342–355 (2013)
30. M Chopde, K Ramteke, S Kamble, Probabilistic model for intrusion detection in wireless sensor network. Int. J. Commun. Netw. Secur. (IJCNS). **1**(3), 19–23 (2011)
31. M Mubarak, S Sattar, A Sajitha, Intrusion detection: a probability model for 3D heterogeneous WSN. Int. J. Comput. Appl. **6**(12), 15–20 (2010)
32. C Ortiz, J Puig, C Palau, M Esteve, *Wireless sensor network modeling and simulation*, (Valencia, Spain, Unknown Month 14), pp. 307-312
33. G Marsaglia, Choosing a point from the surface of a sphere. Ann. Math. Stat. **43**(2), 645–646 (1972)
34. R Kaparti, OPNET IT GURU: a tool for networking education. MSCIT Practicum Paper. "http://staff.ustc.edu.cn/~bhua/experiments/ITGAE_Tool_Ntwrk_Ed.pdf" Accessed 3 Mar 2015
35. The network simulator - ns-2. "http://www.isi.edu/nsnam/ns/" Accessed 10 Dec 2014
36. T Xuan, S Choi, I Koo, A novel blind event detection method for wireless sensor networks. Hindawi J. Sensors. **2014**, 1–6 (2014)
37. D Cohen, M Kelly, X Huang, N Srinath, *Trustability based on beta distribution detecting abnormal behaviour nodes in WSN*, (Indonesia, Unknown Month 29), pp. 339-344
38. M Islam, Motion analysis using distance and velocity-time function. Int. J. Sci. Knowl. **2**(1), 1–6 (2013)
39. Sphere-sphere intersection. "http://mathworld.wolfram.com/Sphere-SphereIntersection.html" Accessed 10 Dec 2014
40. I Akyildiz, W Sankarasubramaniam, E Cayirci, Wireless sensor networks: a survey. Elsevier J. Comput. Netw. **38**(4), 393–422 (2002)