Three Dimensional Intrusion Objects Detection under Randomized Scheduling Algorithm in Sensor Networks

Yanping Zhang[+], Yang Xiao[+], Kui Wu[++], Xiaojiang Du[*], and Bo Sun[%]
[+]*Department of Computer Science, University of Alabama, Tuscaloosa, AL 35487, USA*
[++]*Department of Computer Science, University of Victoria, Victoria, BC, Canada*
[*]*Department of Computer Science, North Dakota State University, Fargo, ND 58105, USA*
[%]*Department of Computer Science, Lamar University, Beaumont, TX 77710, USA*
Emails: yzhang@cs.ua.edu,{yangxiao, wkui, dxj}@ieee.org, bsun@my.lamar.edu

Abstract

Wireless sensor networks are widely used for monitoring applications. The monitored area and the intrusion object are mostly three dimensional. In this paper, we are particularly interested in a sensor network used for monitoring a field to detect intrusion objects such as submarine in some sea area, or goods on shelves in warehouse. In these applications, sensors float in different depth of water or on different height of shelves in three dimensional situations. Since sensor nodes have limited energy supply, sensor networks may be configured to put some sensor nodes in sleep mode to save energy. This is a special case of a randomized scheduling algorithm. In this paper, we study the performance of several randomized scheduling algorithms in terms of intrusion coverage intensity when an intrusion object is considered to occupy a three dimensional space. We study the impact of the size of intrusion object on the sensor network's configuration.

1. Introduction

Composed of a large number of multifunctional sensor nodes, wireless sensor networks (WSNs) have become an important technology combining sensor technology, embedded computing, distributed information processing, and wireless communication technology all together [25], [26]. WSNs have broad applications [27], such as medical monitoring, environment pollution monitoring, forest fire monitoring, target tracking, combat field reconnaissance, military command and control, and so on.

Generally, data collection is the basic requirement in all the applications of WSNs, since data is critical for the network to perform analysis and take actions. To collect data well, network coverage and connectivity are deterministic factors. Meanwhile there are several important constraints for WSNs, such as limitation of energy, memory, and computation. Therefore, it is necessary to construct the networks under the constraints. Energy is vital for many applications in WSNs as it is always hard to recharge the deployed nodes with limited energy. Great efforts have been devoted to minimizing the energy consumption and extending the lifetime of the network. One common way is to put some sensor nodes in sleep mode to save energy and wake them up under some strategies. In this paper, we also introduce the randomized scheduling algorithm [9-11] into our study, which aims to save energy consumption in sensor networks.

Although energy efficiency is the essential requirement for WSNs, it should not be achieved at the cost of reducing network coverage which is usually a major metric in measuring Quality of Service (QoS) of sensor networks [23]. As sensor nodes are usually densely deployed, there is high spatial redundancy in WSNs. Therefore, energy efficiency and high sensing coverage can be achieved simultaneously by exploiting the spatial redundancy among sensor nodes. Many research efforts have been devoted to sensor scheduling algorithms that turn off redundant sensors for energy saving [1]-[5], [7]-[8]. Since maintaining location information and time synchronization introduces extra energy and computational overhead, some scheduling schemes [1], [7], [9], [19] work without the availability of location information or the existence of precise time synchronization. In [16], the authors propose several sensing scheduling protocols and analyze the performance of object detection and network lifetime with a different framework from ours. Recently, the joint problem of coverage and connectivity is considered [9], [15], [18], [22]. In [18], the authors consider a network with sensor nodes deployed strictly in grids. The joint problem in more general sensor networks where the sensor nodes are

978-0-7695-3457-2/08 $25.00 © 2008 IEEE
DOI 10.1109/MSN.2008.34

deployed at random is investigated in [9], [22]. Similar work was done in [21] in which the authors also present a Coverage Configuration Protocol (CCP) that can provide fully coverage of a convex region.

In [9-11], and [24], we have studied the randomized coverage algorithm, which is also called k-set randomized scheduling algorithm. Let S denote the set including all the sensor nodes deployed in a WSN. Each sensor node is randomly assigned to one of k disjoint subsets (S_j; $j = 1, 2, ..., k$), which work alternatively. In other words, at any time, only one set of sensor nodes are working, and the rest of sensor nodes sleep. Network lifetime is the elapsed time during which the network functions well. Network coverage intensity is the ratio of the time when a point in the field of the sensor network is covered by at least one active sensor node to the total time [10-11], [24].

In our previous studies [9-11] and [24], we considered the cases where the intrusion object is modeled as a point. In reality, an intrusion object is much more complex. For example, in underwater sensor network, sensors may be deployed to detect enemy's submarines or other intrusion underwater robots. Therefore, we need to consider the underwater environment to be three dimensional. Another example is warehouse monitoring, in which, sensors are deployed on shelves to monitor goods in the warehouse. The sensing area in fact is three dimensional and the monitored area and objects always occupies a three-dimensional space. Therefore, in many applications, three dimensional considerations are more realistic. Meanwhile sensing area of a sensor should be also considered to be a three-dimensional space, that is a spherality, with radius r which is also sensor's sensing radius.

In this paper, we study the intrusion detection intensity with objects considered to be three dimensional. We also study how the sizes of the intrusion objects influence the sensor network's configuration.

2. 3D Intrusion Object with space

We assume that the intrusion object is considered to be three dimensional (3D) with size o, which denoting the space occupied by the intrusion object. Of course, the intrusion object's size is difficult to predict beforehand. However, studying it can help to set up a sensor network's configuration. For example, in a 3D underwater area, sensor network deployed to detect enemy's submarine or underwater equipment, intrusion objects' sizes are totally different. This section studies the influence of sizes of the intrusion objects on a sensor network's configuration, e.g., the number of deployed sensors. Intuitively, the smaller the intrusion objects, the more sensors are needed to be deployed. In this paper, we assume that sensors are randomly distributed in a three dimensional space.

In this paper, we assume that a sensor node can monitor the activities within a sphere area. This sensing model may not exactly match specific real-world sensor devices whose sensing range is subject to the orientation and aperture of sensors. For ease of analysis, however, we need to select a simple model to approximate the sensing area of a node. Furthermore, this sensing model is implementable because a sensor node can physically carry several sensors, with each monitoring a different direction.

2.1. Intrusion Detection Intensity

In (1), let r, a, and k denote the size of sensing area of each sensor, the size of the whole sensing field, and the number of the disjointed subsets, respectively. Firstly, we consider the intrusion detection intensity of two different shaped objects which are spherical and cuboid. We assume the sensing area of a sensor is also a ball, and the sensing radius of a sensor is $\sqrt[3]{3r/(4\pi)}$. Let o denote the size of intrusion object, which is the space occupied by the object. If the object is spherical shaped, its radius is $\sqrt[3]{3o/(4\pi)}$. If the object is cuboid, we denote its length, width, and height as b, b, and o/(bc), respectively. A sensor does not overlap an intrusion object if the sensor is far away ($>\sqrt[3]{3r/(4\pi)}$) from the boundary of the intrusion object. The probability that a sensor detects a spherical intrusion object or a cuboid-shaped intrusion object is expressed as follows:

$$
\begin{aligned}
p_1 &= \Pr(\text{a sensor detects an intrusion object}) \\
&= \Pr(\text{a sensor area overlaps the body of obejct}) \\
&= \begin{cases} \dfrac{4\pi}{3a}\left(\sqrt[3]{3r/(4\pi)} + \sqrt[3]{3o/(4\pi)}\right)^3, \text{spherical} \\ \dfrac{1}{a}[o + 2(bc + o/b + o/c)\sqrt[3]{3r/(4\pi)} + r \\ +(b + c + o/(bc))\pi\left(\sqrt[3]{3r/(4\pi)}\right)^2], \text{cuboid} \end{cases} \qquad (1) \\
&= \begin{cases} \dfrac{1}{a}(\sqrt[3]{r} + \sqrt[3]{o})^3, \text{spherical} \\ \dfrac{1}{a}[o + 2(bc + o/b + o/c)\sqrt[3]{3r/(4\pi)} + r \\ +(b + c + o/(bc))\sqrt[3]{9\pi r^2/16}], \text{cuboid} \end{cases}
\end{aligned}
$$

Meanwhile, we define intrusion detection intensity V_n as follows:

$$V_n = 1 - \left[1 - p_1/k\right]^n \quad (2)$$

From (2), we know that the intrusion detection intensity is the probability that a given area at a given time is detected by at least one active sensor.

2.2. Sensor Network Deployment

We now study the required number of sensors or the required number of subsets to achieve certain degree of intrusion detection intensity when the intrusion object occupies a space. For example, the monitored area may be airspace or water area; the object may be an airplane or submarine. Sensors are randomly deployed in the monitored area. They might be some smart dust that floats in the air to detect some feature information of its object, or some underwater sensors that keep monitoring some underwater vehicles. The following two questions need to be answered in order to investigate the influence of sizes of the intrusion objects on a sensor network's configuration, e.g., the number of sensors deployed.

- Question A: given intrusion detection intensity and the intrusion object size [(o (and b, c)], what is the minimum number of sensors to achieve the intrusion detection intensity?
- Question B: given intrusion detection intensity and the intrusion object size [o (and b, c)], what is the maximum k value to achieve the intrusion detection intensity?

From (2), we can have the following results:

Lemma 1*: Given a required intrusion detection intensity* V_{n-req} *, the minimum number of sensors to achieve* V_{n-req} *is at least*

$$n \geq \frac{\ln(1 - V_{n-req})}{\ln(1 - p_1/k)}. \quad (3)$$

The above result answers Question A.

Lemma 2*: Given a required intrusion detection intensity* V_{n-req} *, the maximum number of subsets to achieve* V_{n-req} *is*

$$k \leq \frac{p_1}{\left(1 - \left(1 - V_{n-req}\right)^{1/n}\right)}. \quad (4)$$

The above result answers Question B.

3. Performance Evaluation

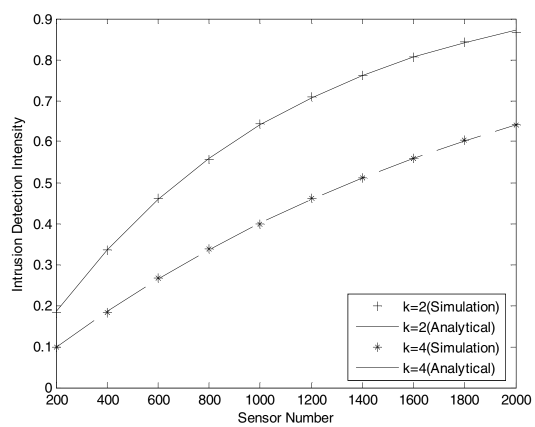
In this section, we study the performance of detection probability and intrusion detection intensity via both simulations and analytical results. All the results considered both the spherical intrusion objects and cuboid intrusion objects.

3.1. Intrusion Detection Intensity

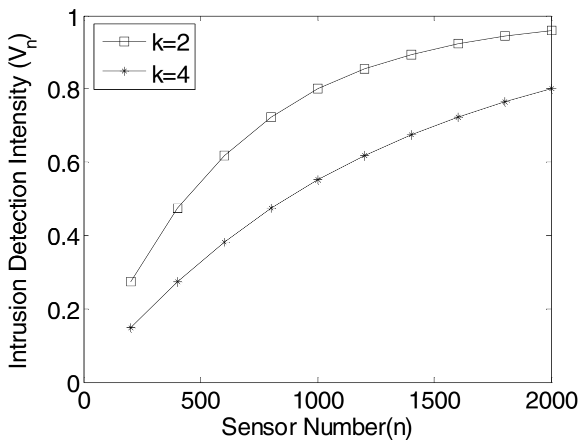
We study the performance of intrusion detection intensity versus number of sensor nodes, number of subsets, and object size.

Fig. 1 shows the performance of intrusion detection intensity vs. the number of sensor nodes for different number of subsets (*k=2* and *k=4*), where *a= 1000000*, *r=500*, and *o* (object size) = *100*. Fig. 1a shows the performance with a spherical intrusion object. Both the analytical results and simulation results are studied and from the figure we observe that the intrusion detection intensity increases as the number of nodes increases. A larger k is corresponding to smaller intrusion detection intensity. From (2), we know that a large n will lead to big intrusion detection intensity, and when n goes to infinity, the detection intensity runs to 1. In Fig. 1a, the analytical results match the simulation results nicely Fig. 1b shows the similar performance of intrusion detection intensity with cuboid intrusion object (*o=100, c=15, b=5*).

Fig. 2 shows the performance of intrusion detection intensity vs. number of subsets for different number of sensor nodes (*n=5000* and *n=3000*), where *a= 1000000*, *r=500*, and *o* (object size) = *100*. Fig. 2a shows the performance with a spherical intrusion object and from the figure we observe that the intrusion detection intensity decreases as the number of subsets increases. When *k* goes to infinity, the intrusion detection intensity runs to *0*. From (3), we know intrusion detection intensity is a decreasing function of *k*, and a larger n is corresponding to larger detection intensity. Fig. 2b shows the similar performance of intrusion detection intensity with cuboid intrusion object (*o=100, c=15, b=5*). Normally, we may not divide the sensors into so many subsets. However, for deeply understanding of subsets (*k*), we take a broad range to see its impacts.



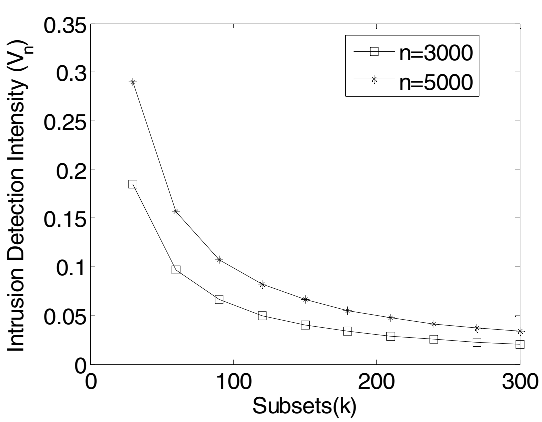
(a) Vn vs. number of sensor nodes: spherical object



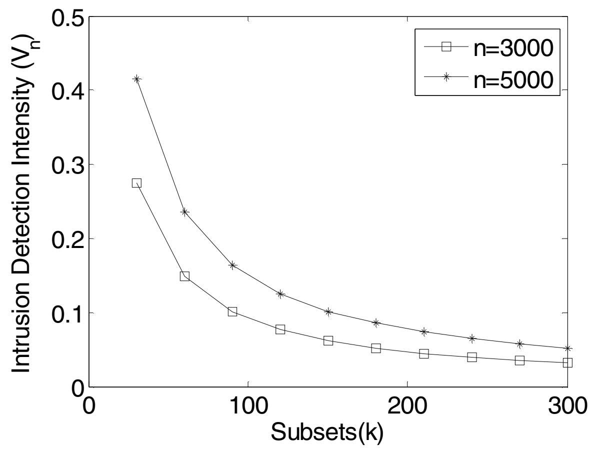
(b) Vn vs. number of sensor nodes: cuboid object

Fig. 1 Intrusion detection intensity vs. number of sensor nodes

Fig. 3 shows the performance of intrusion detection intensity vs. object size for different number of subsets (*k=2* and *k=4*), where *n=1000*, *a= 1000000* and *r=500*. Figs. 3a and 3b show the performance with a spherical intrusion object and with a cuboid intrusion object (with one pair of sides fixed at *5*, *15* and the third side varying), respectively. Both figures show the similar performance of intrusion detection intensity. By intuition, the intrusion detection intensity increases as the intrusion object size increases, and this is also illustrated in the figures. A larger *k* makes the detection intensity smaller.

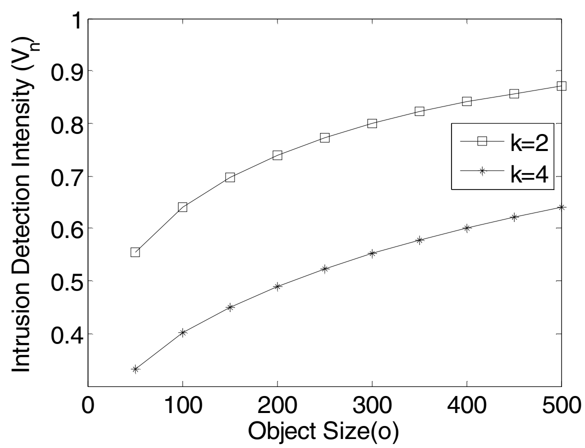


(a) Vn vs. number of subsets: spherical object

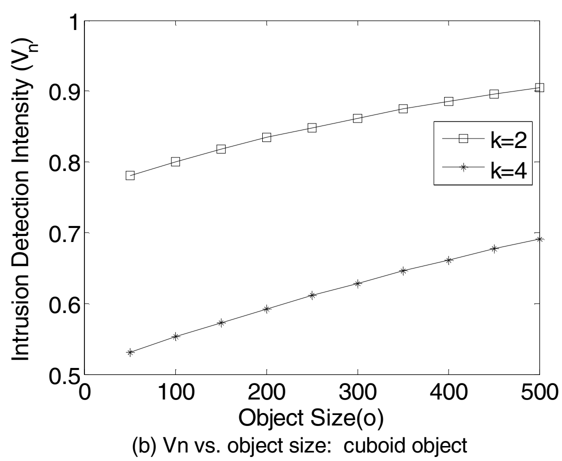


(b) Vn vs. number of subsets: cuboid object

Fig. 2 Intrusion detection intensity vs. number of subsets



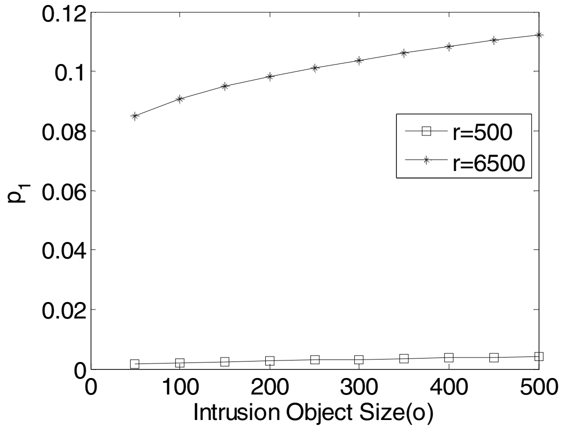
(a) Vn vs. number of object size: spherical object



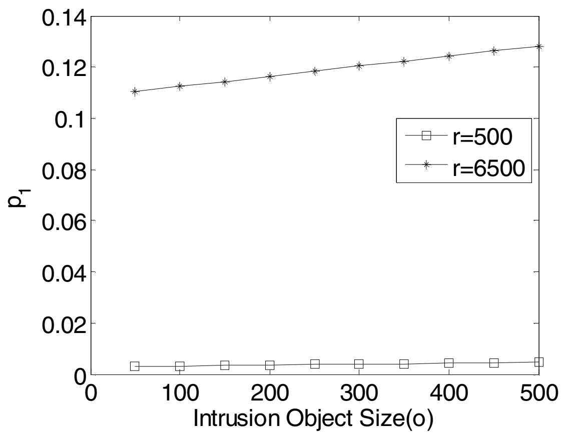
(b) Vn vs. object size: cuboid object

Fig. 3 Intrusion detection intensity vs. object size

3.2. Detection Probability



(a) p_1 vs. intrusion object size: spherical object

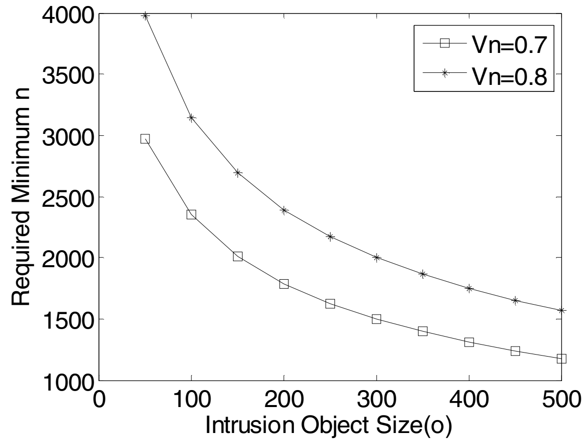


(b) p_1 vs. intrusion object size: cuboid object

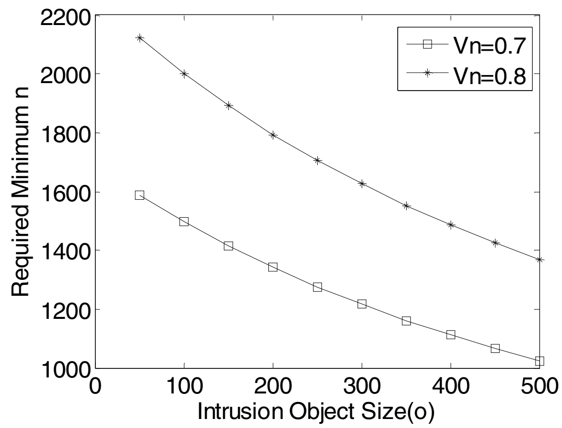
Fig. 4 Detection probability vs. intrusion objects size.

Fig. 4 shows the detection probability vs. the size of intrusion object with different sensing area of each sensor, where *a= 1000000*. Fig. 4a shows the performance with spherical intrusion object and Fig. 4b shows the performance with cuboid object (with one pair of sides fixed at *5*, *15* and the third side varying). As illustrated in the figures, the detection probability increases as the size of the intrusion objects increases, and a larger r is corresponding to a larger detection probability. This is also consistent with our intuition.

3.3. Sensor Network Deployment



(a) Required minimum n vs. object size: spherical object

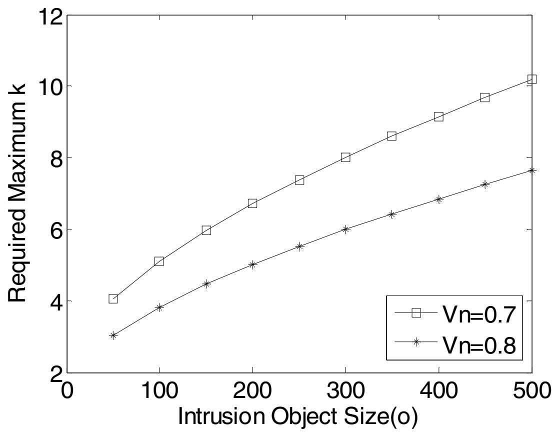


(b) Required minimum n vs. object size: rectangle object

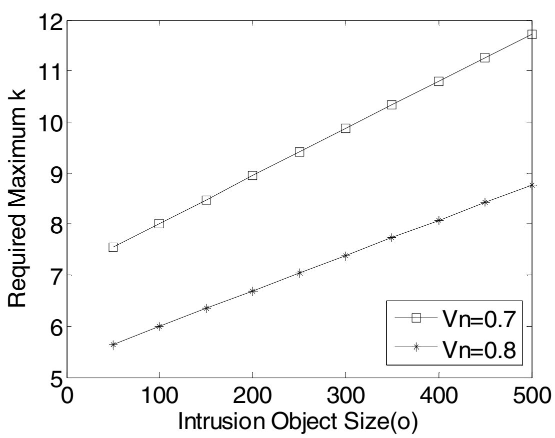
Fig. 5 Required minimum n vs. object size

Fig. 5a shows the required minimum number of sensor nodes for a given intrusion detection intensity vs. intrusion object size with a spherical intrusion object, where *a= 1000000*, *r =500*, and *k = 4*. As illustrated in the figure, the required minimum number of sensor nodes decreases as the value of intrusion object size increases. Larger intrusion detection intensity needs more sensor nodes. Fig. 5b shows the similar result with Fig. 5a while the intrusion object is a cuboid one. The figures answer Question A in the above.

Fig. 6a shows the required maximum k value (i.e., the number of subsets) for a given detection intensity vs. object size with a spherical intrusion object, where *a= 1000000*, *r = 500*, and *n=3000*. As illustrated in the figure, the required maximum number of subsets increases as the value of intrusion object size increases. A larger intrusion detection intensity needs a smaller k. Fig. 6b shows the similar result with Fig. 6a while the intrusion object is a cuboid one. The figures answer Question B in the above.



(a) Required maximum k vs. object size: spherical object



(b) Required maximum k vs. object size: rectangle object

Fig. 6 Required maximum k vs. intrusion object size

4. Conclusion

Energy saving and network lifetime are important topics for wireless sensor networks, and the k-set randomized scheduling algorithm extends the lifetime of the network. In this paper, we evaluated the performance of the randomized scheduling algorithms with an intrusion object occupying a three dimensional space. We studied intrusion detection intensity via both simulations and analytical results. We also studied the influence of sizes of the intrusion objects on a sensor network's configuration, which can help to set up a sensor network's configuration. For intrusion object detection, the detection probability is determined by the object size, the number of sensors, sensing radius, the number of subsets, as well as the size of the monitored region.

5. Acknowledgement

This work was supported in part by 1) the US National Science Foundation (NSF) under the grants CNS-0716211, CNS-0737325, CNS-0829827, CNS-0721907, CNS-0709268, and DUE-0633445, 2) Army Research Office under grants W911NF-07-1-0250 and W911NF-08-1-0334, as well as 3) the Texas Advanced Research Program under grant 003581-0006-2006.

6. References

[1] Z. Abrams, A. Goel, and S. Plotkin, "Set k-cover algorithms for energyefficient monitoring in WSNs," Proc. of IPSN 2004.

[2] C. Hsin and M. Liu, "Network coverage using low duty-cycled sensors:Random & coordinated sleep algorithm," Proc. of IPSN 2004.

[3] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava,"Coverage problems in wireless ad-hoc sensor networks," Proc. of IEEE INFOCOM 2001.

[4] D. Tian and D. Georganas, "A coverage-preserving node scheduling scheme for large WSNs," Proc. of WSNA 2002.

[5] K. Wu, Y. Gao, F. Li, and Y. Xiao, "Lightweight deployment-aware scheduling for WSNs," ACM/Springer Mobile Networks and Applications (MONET), Special Issue on Energy Constraints and Lifetime Performance in WSNs, vol. 10, no. 6, pp. 837-852, December 2005.

[6] T. Yan, T. He, and J. Stankovic, "Differentiated surveillance for sensor networks," Proc. of ACM SenSys 2003.

[7] F. Ye, G. Zhong, J. Cheng, S. Lu, and L. Zhang, "Peas: A robust energy conserving protocol for long-lived sensor networks," Proc. Of ICNP 2002.

[8] L. Wang and Y. Xiao, "A Survey of Energy-Efficient Scheduling Mechanisms in Sensor Networks," ACM/Springer Mobile Networks and Applications (MONET), Vol. 11, No. 5, Oct. 2006, pp. 723 - 740.

[9] C. Liu, K. Wu, Y. Xiao, and B. Sun, "Random Coverage with Guaranteed Connectivity: Joint Scheduling for WSNs," IEEE Transactions on Parallel and Distributed Systems, Vol. 17, No. 6, June 2006, pp. 562-575.

[10] Y. Xiao, H. Chen, K. Wu, C. Liu, and B. Sun, "Maximizing Network Life Time under QoS constraints in WSNs," Proc. of GLOBECOM 2006.

[11] Y. Xiao, H. Chen, K. Wu, and B. Sun, "Modeling Detection Metrics in Randomized Scheduling Algorithm in Wireless Sensor Networks" Proc. of IEEE WCNC 2007.

[12] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: Anenergy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," Proc. of Mobicom 2001.

[13] E. Elson and K. Romer, "WSNs: A new regime for time synchronization," Proc. of First Workshop on Hot Topics in Networks, Princeton, New Jersey, October 2002.

[14] P. Godfrey and D. Ratajczak, "Robust topology management in wireless ad hoc networks," Proc. of IPSN 2004.

[15] H. Gupta, S. Das, and Q. Gu, "Connected sensor cover: Self-organization of sensor networks for efficient query execution," Proc. of MobiHoc 2003.

[16] 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 Transactions on Parallel and Distributed Systems, Vol. 18, No. 3, 2007.

[17] C. Schurgers, V. Tsiatsis, S. Ganeriwal, and M. Strivastava, “Topology management for sensor networks: Exploiting latency and density,” Proc. of MobiHoc 2002.

[18] S. Shakkottai, R. Srikant, and N. Shroff, “Unreliable sensor grids: Coverage, connectivity and diameter,” Proc. of INFOCOM 2003.

[19] S. Slijepcevic and M. Potkonjak, “Power efficient organization of WSNs,” Proc. ICC 2001.

[20] S. Tilak, N. Abu-Ghazaleh, and H. W., “Infrastructure tradeoffs for sensor networks,” Proc. WSNA’02.

[21] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, “Integrated coverage and connectivity configuration in WSNs,” Proc.of Sensys 2003.

[22] H. Zhang and J. Hou, “Maintaining coverage and connectivity in large sensor networks,” Proc.of WTASA 2004.

[23] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp.102.114, August 2002.

[24] Y. Xiao, Y. Zhang, X. Sun, and H. Chen, “Asymptotic Coverage and Detection in Randomized Scheduling Algorithm in Wireless Sensor Networks,” Proc. of IEEE ICC 2007.

[25] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks”, IEEE Communications Magazine, pp. 102 – 114, August 2002.

[26] D. Culler, D. Estrin, and M. Srivastava, “Overview of Sensor Networks”, IEEE Computer magazine, pp. 41−49, August 2004.

[27] M. Ilyas and I. Mahgoub, “Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems”, CRC Press, 2004.