Malicious Node Detection and Deletion in Energy Efficient Wireless Sensor Networks

Gowri P
Research Scholar
Department of Compute Science
Bharathiar University

Geetha K
Assistant Professor
Department of Compute Science
Bharathiar University

Abstract

Due to the malicious activities of nodes such as behavioral change of node and malicious activities, Wireless Sensor network may face a critical issue. Scale free wireless sensor network are important because they tolerate random attacks very well. However they can be vulnerable to malicious attacks, which particularly target certain important nodes. To address this problem, both routing and secured communication protocols should be enforced to provide full protection for every node in a communication network. This paper is going to explore the activities of sensor of sensor node architecture. The performances of existing path identification approaches, however, degrade rapidly in large scale networks with lossy links. This paper presents intelligent route identification scheme (IRIS), a robust path evaluation method against poor performance of node construction works. Proposed system can be implemented even when the hacking or node failure occurs in sensor networks. The Robot Detection mechanism is used to detect the malicious nodes and remove the malicious nodes in the network. This proposed mechanism is provide efficient data transmission.

Keywords: Wireless Sensor Networks, IRIS, X-Hop Neighbors

I. INTRODUCTION

A. *Wireless Sensor Networks*

WSN having a spatially data transmission distributed autonomous sensors to monitor physical or environmental conditions, such as sound, temperature, pressure, etc. and to cooperatively pass their data through the network to a main location. The modern computer networks are bi-directional, also enabling control of wireless sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The design and development of wireless sensor networks was invented by military applications such as battlefield surveillance; today, such type of networks are used in many industrial applications and consumer applications, such as industrial process monitoring and control, machine health monitoring. The WSN is built of transmission nodes from a few to several hundreds or even thousands; there each node is connected to one sensor. Each such sensor network node has typically several parts: a radio transmission transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for making communication with the sensors and an energy source, usually a battery or an embedded form of energy harvesting type.

A wireless sensor node might vary in size from that of a shoebox down to the size of a 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 a few to hundreds of dollars, depending on the difficulty of the individual sensor nodes. Network size and cost restrictions of wireless sensor nodes result in corresponding constraints on resources such as energy, computational speed, memory, and communications bandwidth. The network topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh topology network. The propagation technique between the hops of the network can be routing or flooding. The WSN is built of transmission nodes from a few to several hundreds or even thousands, where each node is connected to one wireless sensor.

Each such sensor network node has typically different parts: a radio data transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interconnecting with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A wireless sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning motes of genuine microscopic dimensions have yet to be created.

The cost of wireless sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual network sensor nodes. Size and cost constraints on sensor nodes result in particular constraints on resources such as energy, memory, computational speed and communications bandwidth. The network topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

1) X-Hop Neighbors

The neighborhood of a vertex v in a graph G is the induced sub graph of G containing of all vertices adjacent to v. For example, the image shows a graph of 6 vertices and 7 edges. Vertex 5 is adjacent to vertices 1, 2, and 4 but it is not adjacent to 3 and 6. The neighborhood of vertex 5 is the graph with three vertices, 1, 2, and 4, and one edge connecting vertices 1 and 2.

The neighborhood node is often denoted $N_G(v)$ or (when the graph is unambiguous) N(v). The same neighborhood node notation may also be used to refer to sets of adjacent vertices rather than the corresponding induced sub graphs. The neighborhood node described above does not include v itself, and is more specifically the open neighborhood node of v; it is also possible to define a neighborhood in which v itself is included, called the closed neighborhood and denoted by $N_G[v]$. When stated without any qualification, a neighborhood is assumed to be open.

Neighborhoods may be used to state graphs in computer algorithms, via the adjacency list and adjacency matrix representations. Neighborhoods are also used in the networking clustering coefficient of a graph, which is a measure of the average density of its neighborhoods. In addition, many important classes of graphs may be defined by properties of their neighborhoods, or by symmetries that relate neighborhoods to each other. In network communication Black holes refer to places in the network where incoming or outgoing traffic is silently discarded without informing the source that the data did not reach its intended recipient.

2) Black Hole Filtering

Black hole filtering refers specifically to dropping data packets at the transmission routing level, usually using a routing protocol to implement the filtering on several routers at once, often dynamically to respond quickly to distributed denial-of-service attacks.
A DNS-based Black hole List (DNSBL) or Real-time Black hole List (RBL) is a list of IP addresses published via the Internet Domain Name System (DNS) either as a zone file that can be used by DNS server software, or as a live DNS zone that can be queried in real-time. DNSBLs are most frequently used to publish the addresses of computers or networks linked to spamming; most mail server software can be configured and setup to reject or flag messages which have been sent from a site listed on one or more such lists. The term "Black hole List" is sometimes changed with the term "blacklist" and "block list".

A DNSBL is a software mechanism, rather than a list or policy. There are dozens of DNSBLs in existence, which use a wide array of criteria for listing and delisting of particular node addresses. These include listing the addresses of zombie computers or other machines being used to send spam messages, listing the addresses of ISPs who willingly host spammers, or listing addresses which have sent spam to a honey pot system.

Since the development of the first DNSBL in 1997, the operation and policies of these lists have been frequently controversial, both in Internet and occasionally in lawsuits. Many email systems operators and users consider DNSBLs a valuable communication tool to share the information about sources of spam nodes, but others use some prominent Internet activists have objected to them as a form of censorship.

Extra, a small number of DNSBL operators have been the target of lawsuits filed by spammers seeking to have the lists shut down altogether. Some firewalls discard all ICMP packets, including the ones needed for Path MTU discovery to work correctly. This causes TCP connections from/to/through hosts with a lower MTU to hang.

3) Worm Hole Attacks

Wormhole flow control, also called wormhole routing is a system of simple flow control in computer networking based on known fixed links. It is a subset of flow control methods called Flit-Buffer Flow Control. Switching is a term than routing, as "routing" defines the route or path taken to reach from source to destination.

The wormhole technique does not dictate the route to the destination but decides when the packet moves forward from a router. Cut-through switching, commonly referred as "virtual cut-through," operates in a similar manner, the major difference being that cut-through flow control allocates buffers and channel bandwidth on a packet level, while wormhole flow control does this on the flit level. In most respects, wormhole technique is very similar to ATM or MPLS forwarding, with the exception that the cell does not have to be queued. Wormhole switching is referred as cut-through switching. Large network packets are divided into small pieces called FLITs (flow control digits).

The first flit, called the header flit, holds information about this packet's route (namely the destination address) and sets up the routing behavior for all subsequent flits associated with the packet. The head flit is by zero or more body flits which contain the actual payload of data. The final flit, called the tail flit, performs some bookkeeping activities to close the connection between the two nodes. One thing special about wormhole flow control is the implementation of virtual channels.

B. Problem Definition

In Wireless sensor network data transmission there may be the chance for the malicious attack sometimes. Due to the malicious activities of nodes wireless sensor network faces the critical problems like behavioral change of node and malicious activities. This malicious attacks leads to reduce the network performance and the transmission is not efficient. So the proposed system has to identify the malicious attack, and then has to detect and delete the malicious attacked node in that particular network.

C. Motivation

The motivation is to detect and remove the malicious nodes. This process is done by using robotic detection mechanism. This method first detects the malicious nodes and gathers the missing information by neighboring nodes. And then remove the malicious nodes from the network.

II. MALICIOUS NODE DETECTION AND DELETION

A. WSN'SK-Angle Object Coverage Problem

There are some main issues in sensor networks is coverage problem, which express how well a fields is tracked by sensors. The versions of these issues such as area, object, barrier, and hole coverage problems. To define a new k-angle object coverage issue in a wireless sensor network. Every sensor networks can covers a limit dangle and range only, but sensor networks can rotate to any type of direction freely to cover a particular angle. A set of given sensors and a set of objects at known locations, the goal is to use the lowest number of sensors to k-angle-cover the largest number of objects such that each object is monitored by at least k sensors satisfying some angle constraint.

To solve the new k-angle object coverage problem in wireless sensor networks and centralized and distributed models based on two contribution functions. The contribution function fixes sensors which can add the largest overall contributions first while the second function fixes sensors that can add the largest numbers of higher angle-covered objects.

B. Worst and Best-Case Coverage in Wireless Sensor Networks

Wireless ad hoc sensor networks have latest emerged as a premier research area. Wireless ad hoc sensor networks have long life economic potential, ability to transform the needs of the lives, and it will pose many new system building challenges. Sensor networks also pose a number of recent conceptual and optimization problems. The fundamental problems of wireless ad hoc sensors are namely, coverage. Sensor coverage, in general, answers the questions about the quality of service that can be delivered by a particular sensor network. Here briefly discuss about the coverage problem from several view and formally define the worst case and best-case coverage in a sensor network. By adding computational geometry and graph theoretic models, specifically the Voronoi diagram and graph algorithms, sensor coverage terms in wireless ad hoc sensor networks.

An optimal polynomial time algorithm which uses graph theoretic and computational geometry constructs was developed for solving for best and worst-case coverage. Experimental implementation results show some applications of the theoretic coverage formulations and algorithms specifically for solving for Maximal Breach Maximal Support.

C. On The Path Coverage Properties of Random Sensor Networks

There are two-dimensional spatial coverage processes in wireless sensor network, the points the operational areas that are sensed. Randomly deployed wireless sensor networks, typically, the wireless network coverage of two-dimensional areas are getting analyzed. However, the most of the sensor network applications, e.g., the sensing process on paths, tracking of moving objects, rather than in areas of interest such as application in mind. The analyze the coverage process induced on a one-dimensional path by a wireless sensor network that is modeled as a two-dimensional Boolean model. In the analysis, the sensor locations form a spatial Poisson process of density and the sensing regions are circles of random radii.

The first task to obtain a law for the fraction of a path that is k-sensed, that is sensed by sensors. Asymptotic routing path-sensing results are counted under the same limiting regimes as those required for asymptotic coverage by a Boolean model. Poisson sensor networks in regard to its ability to track a path in the field. Obtain the asymptotic and finite set of network statistics. That is the fraction of a path that is 1-sensed is the same as the fraction of an area that is 1-sensed.

D. Networks for Efficient Query Execution

The essential work of a sensor type network is spatial query execution, where a query collects sensor data within a particular geographic region. Spatial query execution can be exploited to minimize the communication cost incurred in execution of such queries. Any reduction in communication cost would result in an efficient use of the battery energy, which is limited in sensors. There is one type of approach is to reduce the communication cost of a query is to self-organize the network, in response to a query, into a network structure that involves only a tiny subset of the sensors efficient for query processing. The query is then activated using only the sensors in the constructed network topology. The self-organization technique is extra boostup for queries that run sufficiently long to the communication cost incurred in self-organization. Methods to exploit the redundancy in the sensor network by selecting a small subset of sensors that is sufficient to process a given query.

The centralized approximation algorithm in which provably gives near-optimal solution which have provided. In addition, the selected distributed algorithms (distributed approximation and distributed Priority) are also empirically shown to deliver a near-optimal solution. Via extensive simulations, have shown that worked techniques result in substantial energy savings in a wireless sensor network. This technique can also be used to calculate multiple disjoint connected sensors covers in the manner of distributed type.

E. Centralized & Clustered K-Coverage Protocols for WSN

An important functionality of sensor networks are Sensing the coverage. Anyhow, it is also well known that coverage alone in Wireless Sensor Networks is not sufficient, and network connectivity should also be mention for the correct operation of Wireless Sensor Networks. In this proposed work, address the problem of k-coverage in WSNs such that in each scheduling round, every location in a monitored field is surrounded by at least k active sensors while all the active sensors are being connected. Exactly study of the sensors duty explaining about the generating k-coverage configurations in WSNs.

There are multiple types of models available in k-coverage. First, the model of the k-coverage problem in WSN is considered. Second, the model of this problem have to derive a sufficient condition of the sensor spatial density for complete k-coverage of a field and also provide a relationship between the transmission communication and sensing ranges of sensors to maintain both k-coverage of a field and connectivity among all the active sensors.

Third, there are four types of configuration protocols needs to propose to solve the issue of k-coverage in WSNs. characterized k-coverage of a field based on a geometric analysis of the intersection of sensing disks of k sensors and also computed a bound on the sensor spatial density required to k-cover a field. Second, have to prove that k-coverage implies connectivity. Third, proposed pseudodistributed (T-CRACCk and D-CRACCk), centralized (CERACCk), and totally distributed (DIRACCk) protocols to solve the k-coverage problem in WSNs. The simulation implementation results show that DIRACCk is more energy-efficient than CCP with respect to the number of active sensors required for k-coverage and network operational lifetime.

III. METHODOLOGY

Holes detection and healing (HEAL) are the types of available comprehensive solution in the existing system that has a very low complexity and avoid some drawbacks. A distributed virtual forces-based local healing approach based on the hole healing area, in which the forces will be effective. The design and evaluation of HEAL, a distributed, localized and comprehensive two-phase protocol, that can effectively estimate and enhance the area coverage in a mobile WSN. Hole and border detection algorithm is distributed and lightweight, and thus more suited to the energy constrained WSNs.

A. Drawbacks

- A lot of complex techniques are involved
- More time taken for processing
- Not check coverage and connectivity of each node to the neighboring node.

B. Proposed Approach

Robot detection algorithm is implemented in proposed system. This algorithm used for continuous transmission to the neighbor node in the various paths. Each and every node presented in the network can check coverage and connectivity mean distance between the nodes only use same frequency match for available neighboring nodes. There are many holes are occurring like coverage, worm hole, trust hole, block data hole and multiple processing simultaneously performs at the same time. The hole is attack involved for data transmission from the sender node to the particular receiver node to heal that attacks. Robot detection technique contributes frequently in entire network to detect automatically any holes occurred in the process.

C. Benefits

Minimum no of techniques are used to detect the holes.
Less time taken for processing
Check each node coverage and connectivity to the neighbor nodes.

1) Design Factors

A BitTorrent tracker is a special type of server, one of that works in the data communication between peers using the BitTorrent protocol. In a peer-to-peer file sharing a software client on an end-user system requests a file, and portions of the requested file residing on peer machines are sent to the client, and then reassembled into a full copy of the particular requested file. This server named as tracker server keeps track of where file contents copies reside on peer machines, that are available at time of the client request, and helps coordinate efficient data transmission and reassembly of the copied file.

This source systems which have already downloading a file to communicate with the tracker frequently to negotiate faster file communication with new peers, and It will provide network performance; however, after initializing peer-to-peer file download is started, peer-to-peer communication can continue and also without the connection to a tracker. Since the creation of this distributed hash table (DHT) method which is used Bit Torrent trackers "Tracker less" torrents. These trackers have recently become redundant; however, they are still often included and contributed with torrents to improve the speed of peer discovery.

One of the available options for this HTTP based tracker communication protocol is the flag of "compact". This flag expresses that the tracker can compact the response by encoding technique of IPv4 addresses as a set of 4 bytes (32 bits). IPv6 though are 128 bits long, and as such, the flag “compact" breaks IPv6 support. Trackers that are support for IPv6 clients thus currently ignore the compact flag. There is No current alternative is available for IPv6.

2) Protocol Explanation

Here used LEACH protocol for routing. Low-energy adaptive clustering hierarchy ("LEACH") is a TDMA-based MAC protocol which is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). The goal of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the life time of a wireless sensor network. LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full power all the time would waste energy.

Nodes that have been cluster heads cannot become cluster heads again for P rounds, where P is the desired percentage of cluster heads. Thereafter, each node has a 1/P probability of becoming a cluster head again. At the end of each round, each node that is not a cluster head selects the closest cluster head and joins that cluster. The cluster head then creates a schedule for each node in its cluster to transmit its data.

All nodes that are not cluster heads only communicate with the cluster head in a TDMA fashion, according to the schedule created by the cluster head.

They do so using the minimum energy needed to reach the cluster head, and only need to keep their radios on during their time slot. LEACH also uses CDMA Properties of this algorithm include:

- Cluster based
- Random cluster head selection each round with rotation.
- Cluster head selection based on sensor having highest energy
- Cluster membership adaptive
- Data aggregation at cluster head
- Cluster head communicate with sink or user
- Communication done with cluster head via TDMA
- Threshold value

IV. EXPRIMENTAL RESULTS & DISCUSSION

The Performance has been analyzed Hole attack rate, Throughput, Energy consumption, Efficiency, Network lifetime, Packet delivery ratio and Time delay. Throughput or network throughput is the number of operations per second and the rate of successful message delivery over a communication channel. Energy consumption Wireless sensor networks are a novel technology recent emerging from embedded system, sensor technology and wireless type networks. The fast deployment, self-organization and fault tolerance characteristics of wireless sensor networks may make them a very promising and sensitive technique for military applications, environmental and health applications.

Communication Efficiency is the ability to avoid wasting materials, energy, efforts, money, and time in doing something or in giving a desired result. In a more general sense, it is the ability for doing the things well, successfully, and without waste. In mathematical or scientific terms, it is a measure of the extent to which input is well used for an intended task or function. Overall Network Lifetime: Nodes presented in the network are steady to processing state start to end process have best optimal output is overall network lifetime. The reliability of the wireless sensor network can be increased by using distributed control architecture.

Time Delay: Network delay is an important design work and performance characteristic of a computer network or telecommunications network. The delay of a network specifies how long it considers for a bit of data bits to travel across the network from one node or one point to another. It is measured in multiples or fractions of seconds. Time delay=End Time - Start Time. The simulation tool used here is Network Simulator 2 and the following parameters are used;

Physical Protocol	*IEEE 802.11b*
GT	*1*
GR	*1*
L	*1.0*
Frequency	*2.42e9*
Bandwidth	*11Mb*
Data Rate	*11Mb*
Max Packet Queue	*50*
CP Threshold	*10.0e-12*
CS Threshold	*5.82e-09*

Transmission delay is the amount of time required to push all the communication data packet's bits into the wire.

A. Packet Delivery Ratio

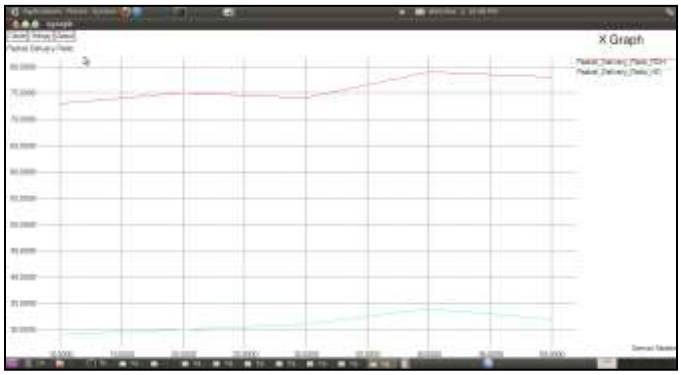

Fig. 4.1: Packet Delivery Ratio

B. Network Hole Attack Ratio

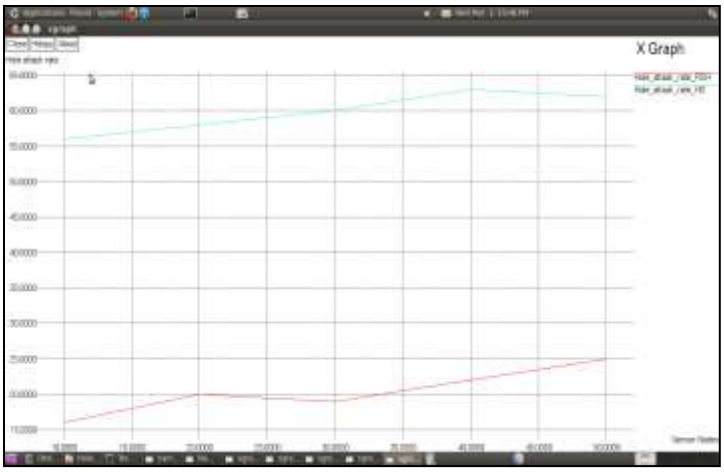

Fig. 4.2: Network Hole Attack Ratio

The throughput of a communication system may be affected by various aspects, including the restrictions of underlying analog physical medium, available processing power of the system components, and behavior of the end user. When different types protocol overheads are taken into account, useful rate of the transferred data can be significantly lower than the maximum achievable throughput; the useful part is usually called to as good put.

Packet delivery Ratio is the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination formula is

$$\sum \text{Number of packet receive} / \sum \text{Number of packet send}$$

C. Time Delay

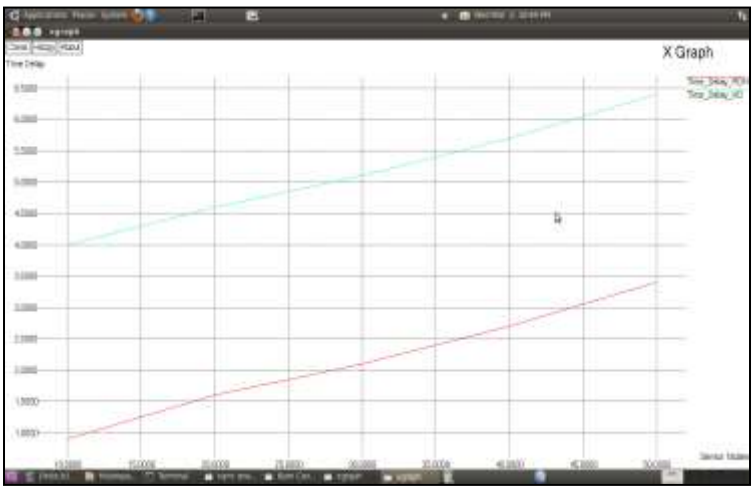

Fig. 4.3: Time Delay

V. CONCLUSION & FUTURE ENHANCEMENT

The malicious attack activities of data transmission nodes reacts the behavioral change of node and malicious activities, Because of this Wireless Sensor network may involves critical issue. Scale free wireless sensor networks are important because they tolerate random attacks very well. Malicious attacks, which particularly target certain important nodes. To address this problem, both routing and secured communication protocols should be enforced to provide full protection for every node in a communication network.

This proposed system is used to detect the malicious attack node and remove the attacked node from the data transmission network by using the method named as robot detection mechanism and the network performance are analyzed using Xgraph to measure about the network performance such as network life time delay, ,energy consumption, throughput, packet delivery ratio etc. Future Enhancements of this work may involve the following;

For the future work, the further development may the future work of this current work for fast transmission in large scale data communication networks and can test in the real world experiments with all required setup.

REFERENCES

[1] C. Ma, J. He, H. H. Chen, and Z. Tang, "Coverage overlapping problems in applications of IEEE 802.15.4 wireless sensor networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2013, pp. 4364–4369.
[2] F. Dai and J. Wu, "On constructing k-connected k-dominating set in wireless ad hoc and sensor networks," J. Parallel Distrib. Comput.,vol. 66, no. 7, pp. 947–958, 2006.
[3] L. C. Shiu, C. Y. Lee, and C. S. Yang, "The divide-and-conquer deployment algorithm based on triangles for wireless sensor networks," IEEE Sensors J., vol. 11, no. 3, pp. 781–790, Mar. 2011.
[4] Y. C. Tseng, P. Y. Chen, and W. T. Chen, "k-Angle object coverage problem in a wireless sensor network," IEEE Sensors J., vol. 12, no. 12, pp. 3408–3416, Dec. 2012.
[5] S. Megerian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, "Worst and best-case coverage in sensor networks," IEEE Trans. Mobile Comput., vol. 4, no. 1, pp. 84–92, Jan./Feb. 2005.
[6] S. S. Ram, D. Manjunath, S. K. Iyer, and D. Yogeshwaran, "On the path coverage properties of random sensor networks," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 494–506, May 2007.
[7] H. Gupta, Z. Zhou, S. R. Das, and Q. Gu, "Connected sensor cover: Self-organization of sensor networks for efficient query execution," IEEE/ACM Trans. Netw., vol. 14, no. 1, pp. 55–67, Feb. 2006.
[8] G. Xing, X. Wang, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration for energy conservation in sensor networks," ACM Trans. Sensors Netw., vol. 1, no. 1, pp. 36–72, 2005.
[9] L. Liu, B. Hu, and L. Li, "Energy conservation algorithms for maintaining coverage and connectivity in wireless sensor networks," IET Commun., vol. 4, no. 7, pp. 786–800, 2010.
[10] H. M. Ammari, and S. K. Das, "Centralized and clustered k-coverage protocols for wireless sensor networks," IEEE Trans. Comput., vol. 61, no. 1, pp. 118–133, Jan. 2012.
[11] A. Ahmad, K. Latif, N. Javaid, and A. Khan, "Density controlled divide-and-rule scheme for energy efficient routing in wireless sensor networks," in Proc. 26th Annu. IEEE Canadian Conf. CCECE, 2013, pp. 1–4.
[12] J. Wu and N. Sun, "Optimum sensor density in distortion-tolerant wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 6, pp. 2056–2064, Jun. 2012.
[13] X. Bai, Z. Yun, D. Xuan, and T. H. Lai, "Optimal patterns for fourconnectivity and full coverage in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 3, pp. 435–448, Mar. 2010.
[14] B. C_arbunar, A. Grama, J. Vitek, and O. C_arbunar, "Redundancy and coverage detection in sensor networks," ACM Trans. Sensors Netw., vol. 2, no. 1, pp. 94–128, 2006.
[15] C. Zhang, X. Bai, J. Teng, and D. Xuan, "Constructing low-connectivity and full-coverage three dimensional sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 7, pp. 984–993, Sep. 2010.
[16] Z. Yun, X. Bai, D. Xuan, and T. H. Lai, "Optimal deployment patterns for full coverage and k-connectivity (k _ 6) wireless sensor networks," IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 934–947, Jun. 2010.
[17] H. Zhang and J. C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks," J. Ad Hoc Sensors Wireless Netw., vol. 1, pp. 89–124, 2005.
[18] S. Yang, M. Li, and J. Wu, "Scan-based movement-assisted sensor deployment methods in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 8, pp. 1108–1121, Aug. 2007.
[19] A. Tahbaz-Salehi, and A. Jadbabaie, "Distributed coverage verification in sensor networks without location information," IEEE Trans. Autom. Control, vol. 55, no. 8, pp. 1837–1849, Aug. 2010.