A Survey on Recent Trends in Wireless Sensor Networks

S.Kannadhasan, R.Balaganesh and G.Srividhya

ABSTRACT------**Wireless Sensor Networks have promise a large variety of applications. They are often deployed in potentially adverse or even hostile environments. Intrusion detection systems make available a necessary layer of in-depth fortification for wired networks. Miniature research has been performed about intrusion detection in the areas of wireless sensor networks. Energy efficiency in wireless sensor network [WSN] is the highly important role for the researchers. Clustering is the important factors for real time applications .We present the challenge of constructing intrusion detection systems for wireless sensor networks and survey the intrusion detection techniques, and indicate important future research directions.**

Keywords: Clustering, Issues of WSN, Attacks, Load Balancing, Sensor Technology

I. INTRODUCTION

A wireless sensor node (WSN) is a one type of sensor technology to monitor physical or conservational needs, such as pressure, sound, vibration, temperature, motion and to transmit the data to a sink (base station) through the network. Currently most of the latest networks are bi-directional, enabling to cope up with the activity of the sensors [1]. Military applications like battle field reconnaissance is the main inspiration for wireless sensor networks development, recently this type of distributed networks a read opted in most of remote monitoring applications and industrial measurements application like machine condition monitoring, industrial process monitoring, structural health monitoring, and indoor monitoring.Sensors nodes are characteristically proficient of wireless communication and are considerably obliged in the amount of existing resources such as energy (power), storage (memory) and computation [2]. These obligate make the deployment and operation of WSN significantly distinct from existing wireless networks, and demand the development of resource aware protocols and supervision techniques.

S**. Kannadhasan, R. Balaganesh and G. Srividhya** are PG Scholars, Department of ECE, Velammal College of Engineering and Technology, Madurai, Tamilnadu, India, Emails: kannadhasan.ece@gmail.com, arbala22@gmail.com, srividhyagk1990@ yahoo.co.in

II**. CLUSTERING APPROACH**

Clustering is considered as an effective approach to reduce network overhead and improve scalability. Since sensor networks are based on the dense deployment of disposable and low-cost sensor nodes, destruction of some nodes by hostile action does not affect a military operation as much as the destruction of a traditional sensor, which makes the sensor network concept a better approach for battlefields [3]. The transmission between the two nodes will minimize the other nodes to show the improve throughput and greater than spatial reuse than wireless networks to lack the power controls. Adaptive Transmission Power technique to improve the Network Life Time in Wireless Sensor Networks.

The Clustering Technique using the minimum spanning tree[MST] to detect the shortest path in wireless sensor networks. The data from nearby the cluster heads will be directly transmitted to the sink node. The data from sink nodes to calculate the distance whereas the cluster head will be transmitted through the shortest multihop path. The distance between the cluster head and sink node. The shortest path between each cluster head to the sink node. To find the Predominant node[Maximum number of path].Transmission power techniques is to improve the performance of the network in several aspects [4]. Transmission range in the wireless networks should be change the ranges in each link. The traffic capacity decreases when more nodes are added to increases the interference. Routing graph theory to multiple paths from data sources to a neighbor's node.

In the cluster-based approach sensor nodes in particular WSN are permitted to transmit sensed data towards the base station. In this allows sensor nodes to sense and transmit the sensed information to the cluster-heads directly, instead of routing through its immediate neighbors. When a cluster node fails because of energy depletion we need to choose alternative cluster for that particular region. In periodical time each sensor node in the cluster should possess the next cluster head re-election based on energy to avoid node failure. Unlike previous algorithms, cluster formation precedes before cluster head selection. The spanning tree is 'minimal' to the cluster of each node when the total length of the edges is the minimum necessary to connect all the vertices in the clustering head.

In the newly formed clusters, the each node with the highest energy level is selected as the cluster head and the next higher energy level node is selected as the next CH node.

III. ROUTING PROTOCOL

DTN is fundamentally an opportunistic communication system, where communication links only exist temporarily, rendering it impossible to establish end-to-end connections for data delivery. In such networks, routing is largely based on nodal contact probabilities. The key design issue is how to efficiently maintain, update, and utilize such probabilities. Clustering is considered as an effective approach to reduce network overhead and improve scalability. Various clustering algorithms have been investigated in the context of mobile ad hoc networks. However, none of them can be applied directly to DTN, because they are designed for well-connected networks and require timely information sharing among nodes [5]. A node in real-life tends to visit some locations more frequently than others. If two nodes share the same home location, they have high chance to meet each other. Thus real-life mobility patterns naturally group mobile devices into clusters.

Due to possible errors in the estimation of contact probabilities and unpredictable sequence of the meetings among mobile nodes, many unexpected small size clusters may be formed. To deal with this problem, we employ a merging process that allows a node to join a "better" cluster, where the node has a higher stability as to be discussed in the next section. The merging process is effective to avoid fractional clusters.

IV. LOAD BALANCING

Load balancing is an effective enhancement to the proposed routing protocol. The basic idea is to share traffic load among cluster members in order to reduce the dropping probability due to queue overflow at some nodes. Sharing traffic inside a cluster is reasonable, because nodes in the same cluster have similar mobility pattern, and thus similar ability to deliver data messages [6]. More specifically, it randomly transmits as many messages as possible to any node it meets, until their queues are equally long .

V. CATEGORIES OF SENSOR NODES

5.1 Passive, Omni Directional Sensors: passive sensor nodes sense the environment without manipulating it by active probing. In this case, the energy is needed only to amplify their analog signals. There is no notion of "direction" in measuring the environment.

5.2 Passive, narrow-beam sensors: these sensors are passive and they are concerned about the direction when sensing the environment.

5.3 Active Sensors: these sensors actively probe the environment.

Since a sensor node has limited sensing and computation capacities, communication performance and power, a large number of sensor devices are distributed over an area of interest for collecting information (temperature, humidity, motion detection, etc.). These nodes can communicate with each other for sending or getting information either directly or through other intermediate nodes and thus form a network, so each node in a sensor network acts as a router inside the network [7]. In direct communication routing protocols (single hop), each sensor node communicates directly with a control center called Base Station (BS) and sends gathered information. The base station is fixed and located far away from the sensors. Base station(s) can communicate with the end user either directly or through some existing wired network. The topology of the sensor network changes very frequently. Nodes may not have global identification. Since the distance between the sensor nodes and base station in case of direct communication is large, they consume energy quickly.

VI. TRANSMITTED POWER

Wireless sensor networks (WSNs) provide a new class of computer systems and expand human ability to remotely interact with the physical world. Most of the sensors used so far are point sensors which have disc-shaped sensing and communication areas. Energy-efficient communication is discussed in WSNs. Saving energy is very important in WSNs because of the limited power supply of sensors and the inconvenience to recharge their batteries [8]. Methods are proposed to reduce communication energy by minimizing the total sensor transmission power. That is, instead of transmitting using the maximum possible power, sensors can collaboratively determine and adjust their transmission power to reach minimum total transmission power and define the topology of the WSN by the neighbor relation under certain criteria. This is in contrast to the "traditional" network in which each node transmits using its maximum transmission power and the topology is built implicitly without considering the power issue. Choosing the right transmission power critically affects the system performance in several ways. First, it affects network spatial reuse and hence the traffic carrying capacity. Choosing too large power level results in excessive interference, while choosing too small power level results in a disconnected network. Second, it impacts on the contention for the medium. Collisions can be mitigated as much as possible by choosing the smallest transmission power subject to maintaining network connectivity [9]. The goal is to find distributed methods to let each sensor decide its transmission power by communicating with other sensors to minimize total sensor transmission power while maintaining the connectivity of the network. It is pointed out that it can maintain the network connectivity, but may not minimize the total sensor transmission power. Then it is enhanced to DTCYC algorithm, where the basic idea is to let each sensor remove the largest edge in every cycle involving it as a vertex.

6.1 Power Efficiency in WSNs is generally accomplished in three ways:

- Low duty cycle operation
- Local/In network processing to reduce data volume (and hence transmission time)
- Multihop networking reduces the requirement for long range transmission since signal path loss is an inverse exponent with range of distance. Each node in the sensor network can act as a repeater, thereby reducing the link range coverage required and in turn the transmission power.

VII. ADVANTAGES AND DISADVANTAGES

7.1 Advantages

- Network setups can be done without fixed infrastructure.
- Ideal for the non-reachable places such as across the sea, mountains, rural areas or deep forests.
- Flexible if there is ad hoc situation when additional workstation is required.
- Implementation cost is cheap.

7.2 Disadvantages

- Less secure because hackers can enter the access point and get all the information.
- Lower speed compared to a wired network.
- More complex to configure than a wired network.

VIII. OVERVIEW OF SENSOR TECHNOLOGY

Sensor Nodes are almost invariably constrained in energy supply and radio channel transmission bandwidth, these constraints, in conjunction with a typical deployment of large number of sensor nodes, have posed a plethora of challenges to the design and management of WSNs [9]. Some of the key technologies and standards elements that are relevant to sensor networks are as follows:

8.1 Sensors

- Intrinsic Functionality
- Signal processing
- Compression, forward error correction, encryption
- Control/actuation
- Clustering and in-network computation
- Self assembly

8.2 Wireless Radio Technologies

- Software defined radios
- Transmission range
- Transmission impairments
- Modulation Techniques
- Network Topologies

8.3 Standards

- IEEE 802.1.1a/b/g together with ancillary security protocols
- IEEE 802.15.1 PAN/Bluetooth
- IEEE 802.15.3 Ultra wide band (UWB)
- IEEE 802.15.4 ZIGBEE
- IEEE 802.16 WIMAX
- IEEE 1451.5 (Wireless Sensor Working Group)
- Mobile IP

8.4 Software Applications

- Operating Systems
- Network Software
- Direct database Connectivity software
- Middleware software
- Data Management Software

IX. ISSUES OF WIRELESS SENSOR NETWORKS

9.1 Hardware and Operating System for WSN

Wireless sensor networks are composed of hundreds of thousands of tiny devices called nodes. A sensor node is often abbreviated as a node. A Sensor is a device which senses the information and passes the same on to a mote. Sensors are used to measure the changes to physical environment like pressure, humidity, sound, vibration and changes to the health of person like blood pressure, stress and heart beat [10]. A Mote consists of processor, memory, battery, A/D converter for connecting to a sensor and a radio transmitter for forming an ad hoc network. A Mote and Sensor together form a Sensor Node. There can be different Sensors for different purposes mounted on a Mote. Motes are also sometimes referred to as Smart Dust. A Sensor Node forms a basic unit of the sensor network

9.2. Wireless Radio Communication Characteristics

Performance of wireless sensor networks depends on the quality of wireless communication. But wireless communication in sensor networks is known for its unpredictable nature. Main design issues for communication in WSNs are:

- Low power consumption in sensor networks is needed to enable long operating lifetime by facilitating low duty cycle operation and local signal processing.
- Distributed sensing effectively acts against various environmental obstacles and care should be taken that the signal strength, consequently the effective radio range is not reduced by various factors like reflection, scattering and dispersions.
- Multihop networking may be adapted among sensor nodes to reduce the range of communication link.
- Long range communication is typically point to point and requires high transmission power, with the danger of being eavesdropped. So, short range transmission should be considered to minimize the possibility of being eavesdropped.
- Communication systems should include error control subsystems to detect errors and to correct them.

9.3. Deployment

Deployment means setting up an operational sensor network in a real world environment [11]. Deployment of sensor network is a labor intensive and cumbersome activity as it does not have influence over the quality of wireless communication and also the real world puts strains on sensor nodes by interfering during communications. Sensor nodes can be deployed either by placing one after another in a sensor field or by dropping it from a plane.

9.4 Localization

Sensor localization is a fundamental and crucial issue for network management and operation. In many of the real world scenarios, the sensors are deployed without knowing their positions in advance and also there is no supporting infrastructure available to locate and manage them once they are deployed. Determining the physical location of the sensors after they have been deployed is known as the problem of localization.

9.5 Synchronization

Clock synchronization is an important service in sensor networks. Time Synchronization in a sensor network aims to provide a common timescale for local clocks of nodes in the

network. A global clock in a sensor system will help process and analyze the data correctly and predict future system behavior [12]. Some applications that require global clock synchronization are environment monitoring, navigation guidance, vehicle tracking etc. A clock synchronization service for a sensor network has to meet challenges that are substantially different from those in infrastructure based networks.

9.6 Calibration

Calibration is the process of adjusting the raw sensor readings obtained from the sensors into corrected values by comparing it with some standard values [13]. Manual calibration of sensors in a sensor network is a time consuming and difficult task due to failure of sensor nodes and random noise which makes manual calibration of sensors too expensive.

9.11 Network Layer Issues

Energy efficiency is a very important criterion. Different techniques need to be discovered to eliminate energy inefficiencies that may shorten the lifetime of the network. At the network layer, various methods need to be found out for discovering energy efficient routes and for relaying the data from the sensor nodes to the BS so that the lifetime of a network can be optimized. Routing Protocols should incorporate multi-path design technique. Multi-path is referred to those protocols which set up multiple paths so that a path among them can be used when the primary path fails. Path repair is desired in routing protocols when ever a path break is detected. Fault tolerance is another desirable property for routing protocols. Routing protocols should be able to find a new path at the network layer even if some nodes fail or blocked due to some environmental interference. Sensor networks collect information from the physical environment and are highly data centric [14]. In the network layer in order to maximize energy savings a flexible platform need to be provided for performing routing and data management. The data traffic that is generated will have significant redundancy among individual sensor nodes since multiple sensors may generate same data within the vicinity of a phenomenon. The routing protocol should exploit such redundancy to improve energy and bandwidth utilization. As the nodes are scattered randomly resulting in an ad hoc routing infrastructure, a routing protocol should have the property of multiple wireless hops.

9.12 Quality of Service

Quality of service is the level of service provided by the sensor networks to its users. Quality of Service (QoS) for sensor networks as the optimum number of sensors sending information towards information-collecting sinks or a base station.

9.13 Security

Security in sensor networks is as much an important factor as performance and low energy consumption in many applications. Security in a sensor network is very challenging as WSN is not only being deployed in battlefield applications but also for surveillance, building monitoring, burglar alarms and in critical systems such as airports and hospitals. Since sensor networks are still a developing technology, researchers and developers agree that their efforts should be concentrated in developing and integrating security from the initial phases of sensor applications development; by doing so, they hope to provide a stronger and complete protection against illegal activities and maintain stability of the systems at the same time.

X.ATTACKS ON WIRELESS SENSOR NETWORK

10.1 Introduction

Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols.

Attacks can be classified into two major categories, according to the interruption of communication act, namely

1) Passive attacks
2) Active attacks

From this regard, when it is referred to a passive attack it is said that the attack obtain data exchanged in the network without interrupting the communication [15]. When it is referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication.

Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, Denial of Service (DoS), and message replay.

10.2 Traffic analysis

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.

10.3 Denial-of-service attack (DoS attack) or Distributed Denial-of-Service attack (DDoS attack)

A Denial-of- service attack (DoS attack) or distributed denial of service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users [16]. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high profile web servers such as banks, credit card payment gateways, and even root name servers .

10.4 Replay attack

A replay attack is a breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction. For example, messages from an authorized user who is logging into a network may be captured by an attacker and resent (replayed) the next day. Even though the messages may be encrypted, and the attacker may not know what the actual keys and passwords are, the retransmission of valid log on messages is sufficient to gain access to the network [17]. Also known as a "man-in-the-middle attack", a replay attack can be prevented using strong digital signatures that include time stamps and inclusion of unique information from the previous

transaction such as the value of a constantly incremented sequence number.

10.5 Eavesdropping

Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers. The mobile hosts in mobile ad hoc networks share a wireless medium. The majorities of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be overheard, and fake messages can be injected into network.

10.6 Interference and Jamming

Radio signals can be jammed or interfered with, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications [18]. The most common types of this form of signal jamming are random noise and pulse. Jamming equipment is readily available. In addition, jamming attacks can be mounted from a location remote to the target networks.

10.7 Flooding

Routing message flooding attacks, such as hello flooding, RREQ flooding, acknowledgement flooding, routing table overflow, routing cache poisoning, and routing loop are simple examples of routing attacks targeting the route discovery phase. Proactive routing algorithms, such as DSDV and OLSR, attempt to discover routing information before it is needed, while reactive algorithms, such as DSR and AODV, create routes only when they are needed.

10.8 Data forwarding phase

Some attacks also target data packet forwarding functionality in the network layer. In this scenario the malicious nodes participate cooperatively in the routing protocol routing discovery and maintenance phases, but in the data forwarding phase they do not forward data packets consistently according to the routing table. Malicious nodes simply drop data packets quietly, modify data content, replay, or flood data packets; they can also delay forwarding time-sensitive data packets selectively or inject junk packets.

10.9 Particular routing protocols

There are attacks that target some particular routing protocols. In DSR, the attacker may modify the source route listed in the RREQ or RREP packets. It can delete a node from the list, switch the order, or append a new node into the list. In AODV, the attacker may advertise a route with a smaller instance metric than the actual distance, or advertise a routing update with a large sequence number and invalidate all routing updates from other nodes.

10.10 Wormhole attack

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them [19]. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. This will most likely always be the case when the endpoint of the wormhole is relatively far from a base station. Wormholes can also be used simply to convince two distant nodes that they are neighbors by relaying packets between the two of them. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping. Detection is potentially difficult when used in conjunction with the Sybil attack.

10.11 Rushing attack

Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial of-service attack against all currently proposed on-demand WSN routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne.

10.12 Resource consumption attack

This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

10.13 Location disclosure attack

An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios.

10.14 SYN flooding attack

The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection. For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. The three messages exchanged during the handshake allow both nodes to learn that the other is ready to communicate and to agree on initial sequence numbers for the conversation. During the attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN-ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet [20]. Without receiving the ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed size table while it awaits the acknowledgement of the three-way

handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection.

10.15 Session hijacking

Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target. Hijacking a session over UDP is the same as over TCP, except that UDP attackers do not have to worry about the overhead of managing sequence numbers and other TCP mechanisms. Since UDP is connectionless, edging into a session without being detected is much easier than the TCP session attacks.

10.16 Malicious code attacks

Malicious code, such as viruses, worms, spywares, and Trojan Horses, can attack both operating systems and user applications. These malicious programs usually can spread themselves through the network and cause the computer system and networks to slow down or even damaged.

10.17 Repudiation attacks

Repudiation refers to a denial of participation in all or part of the communication.

10.18 Impersonation attacks

Impersonation attacks are launched by using other node's identity, such as MAC or IP address. Impersonation attacks sometimes are the first step for most attacks, and are used to launch further, more sophisticated attacks.

XI. CONCLUSION

Wireless Sensor Network is the major field in recent trends. WSN which collects information by sensing and though its major issues are discussed. And various types of attacks are also discussed.Major attacks in network layer are Wormhole attack, Denial of Service. The attacks which disrupts the routing, communication facilities and the network's funtioning The eligible sensor nodes are chosen depending on their power levels and association with number of nodes in transmission area. The various types of researches are also discussed in wireless sensor netwoks.

REFERENCES

[1] F.Akyildiz, W.Su, Y.Sankarasubramaniam, E.Cayirci, "Wireless Sensor Networks: a Survey", Computer Networks (Elseveir) 393–422,2002

[2] Chris Karlof, David Wagner "Secure routing in wireless sensor networks:Attacks and Countermeasures", Special issue on sensor network application protocols, 2003

[3] P.papadimitratos and Z.J.Haas,"Secure routing for mobile ad hoc networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002),January, 2002

[4] Majid meghdadi, Suat ozdemir, Inan giller,"A Survey on wormhole based attacks and their counter measures in wireless sensor networks", IETE Technical Review, VOL28, ISSUE2, 2011

[5] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," Conference of the IEEE Computer and Communications Societies (INFOCOM),pp. 1976-1986, 2003.

[6] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," ACM Journal of Wireless Networks(WINET),2005.

[7] Maheshwari R, Gao Jie, Das S R. "Detecting wormhole attacks in wireless networks using connectivity information".IEEE International Conference on Computer Communications. 2007:107-115.

[8] Hu.Y C, Perrig A, Johnson D. "Wormhole attacks in wireless networks". IEEE J.Sel.Areas Communication,2006.

[9] S. Capkun, L. Buttyán, and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," ACM workshop on Security of adhoc and sensor networks (SASN 03), pp.21-32,2003.

[10] Hu Lingxuan, Evans D. "Using directional antennas to prevent wormhole attacks". In Network and distributed network security symposium,2004

[11] Connectivity and Coverage in Hybrid Wireless Sensor Networks using Dynamic Random Geometric Graph Model, Author : Jasmine Norman, Vellore Institute of Technology, Vellore – 14, International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.3, September 2011 .

[12] A New Graph Theory based Routing Protocol for Wireless Sensor Networks, Author : B.Baranidharan, B.Shanthi, SASTRA University, School of Computing, Thanjavur, India, International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.4, December 2011.

[13] Bhupendra Gupta , Srikanth K Iyer , D Manjunath , "Topological Properties Of The One Dimensional Exponential Random Geometric Graph", Random Structures & Algorithms , Volume 32 , Issue 2 , 2008, pp: 181-204

[14] Chen Avin , "Random Geometric Graphs: An Algorithmic Perspective" , Ph,D dissertation, University of California , Los Angeles , 2006

[15] Chi-Fu Huang, Yu-Chee Tseng , "The Coverage Problem in a Wireless Sensor Network" , WSNA'03,September 19, 2003, San Diego, California, USA.

[16] J. Diaz D. Mitsche X. Pierez-Gimienez , "On the Connectivity of Dynamic Random Geometric Graphs, Symposium on Discrete Algorithms" , Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms , 2008, pp 601-610

[17] Josep Diaz, Dieter Mitsche, and Xavier Peirez-Gimeinez , "Large Connectivity for Dynamic Random Geometric Graphs", IEEE Transactions On Mobile Computing, Vol. 8, No. 6, June 2009

[18] Gupta, P.; Kumar, P.R., "Critical Power for Asymptotic Connectivity in Wireless Networks", In Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of W.H. Fleming; McEneaney, W.M., Yin, G.G., Zhang, Q., Eds.; Birkhauser Boston: Cambridge, MA, USA, 1998; 1106–1110.

[19] Gupta, P., Kumar P.R, "The Capacity of Wireless Networks", IEEE Trans. Inform. Theory 2000, 46, 388 404.

[20] Hichem Kenniche , Vlady Ravelomananana , "Random Geometric Graphs as Model of Wireless Sensor Networks" , IEEE , 2010