International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 16181-16196

http://www.ripublication.com

Performance Analysis of Wireless Sensor Networks in Presence of Wormhole Attacks for Various Topologies

S.Umamaheswari[1] and R.Mahalakshmi[2]

1-Associate Professor, Department of ECE, Kumaraguru College of Technology, Coimbatore-641 049. Tamilnadu
2-Professor and Head, Department of EEE, Sri Krishna College of Technology, Coimbatore, Tamilnadu
Corresponding Author`s Email id: umarajaphd@gmail.com,
Mobile number 98427 48465.

Abstract

Wireless sensor networks (WSN) are generally set up for gathering records from insecure environment. Nearly all security protocols for WSN believe that the opponent can achieve entirely control over a sensor node by way of direct physical access. The appearance of sensor networks as one of the main technology in the future has posed various challenges to researchers. Wireless sensor networks are composed of large number of tiny sensor nodes, running separately, and in various cases, with none access to renewable energy resources. In addition, security being fundamental to the acceptance and employ of sensor networks for numerous applications; also different set of challenges in sensor networks are existed. In this paper we will focus on security of Wireless Sensor Network for various topologies with wormhole attack..

Keywords – Security Attack, Cellular topology, Grid topology, random topology, Repeat request, Wireless Sensor Network, wormhole

I. INTRODUCTION

In numerous applications, a sensor network by distributed wireless technology is used. The quality of service (QoS) is reduced because the resource restriction caused some of WSN applications work without security. In WSN, a mass of wireless sensors are linked together via RF communication links. The quality of proper working of the nodes in WSN application consists of comprehension, gathering and distributing information in the network. The sensors are generally tiny which leads to issues in energy. In addition wireless network have restricted memory and also the batteries

have a restricted governing power quality which affects the proper working [1]. Different types of DoS attacks can affect a network or node. If attacked node continues to exchange information or ideas with its neighbors, it diminishes all its power. Hence the node is declared as a dead node which is the worst cases [2].

Jamming is a well-known attack on physical layer of wireless network. Jamming will intermeddle with the radio frequencies being used by the nodes of a network. An attacker consecutively transmits over the wireless network declining the underlying MAC protocol.

If a single frequency is used throughout the network, jamming can interrupt the network impressive. In addition by injecting impertinent packets jamming can cause excessive energy consumption at a node. Moreover the receiver's node will consume energy by getting those packets [4].

Xu, Trappe, Zhang and Wood in 2005 proposed [5] four different type of jamming attack that can be used by an attacker to stop the operation of a wireless network. How each model affects on the sending and receiving capability of a wireless node and its impressiveness were evaluated. It was remarked that no single system measures carrier sensing time and the signal strength is adequate for reliably detecting the conduct of a jammer, and that using packet delivery cannot recognize whether poor link service was due to the mobility of nodes or jamming while it may be efficacious in mark as different between jammed scenarios and congested. Tampering is another attack on physical layer. In this attack, nodes are vulnerable to tampering or physical harm [6].

Attacks can also be made on the link layer. An attacker may premeditatedly violate the communication protocol, and frequently send messages in an attempt to cause collisions. This type of collisions would need the retransmission of any packet influenced by the collision. By means of this technique it would be possible for an adversary to consume easily a sensor node's power supply by forcing oversupply retransmissions [3].

A sensor node may obtain benefit of multi hop by simply refusing to route messages at the network layer. This could be executed frequently or irregularly. The net result being that any neighbor who marks a route through the malevolent node at least will be incapable of exchange messages with, part of the network [3, 7].

Entry by force or without permission in network layer can be grouped into two categories: passive and active attacks. A passive trespass does not interrupt the functioning of the network; but the adversary to discover information, eavesdrops on the traffic flowing across the network without modifying the data. It is very difficult to detect passive attack in view of the fact that a passive attack does not influence the functioning of the network. However, an active attack is unlike a passive attack.

On the other side, imperfect communication can be caused because the attacker can attack data packets, although it assists with other nodes to make legal routes between senders and receivers. For instance the active attacks are, Wormhole attacks [8], Blackhole attacks [9], Byzantine attacks [10], DDoS attacks [11] and routing attacks [12, 13].

Furthermore in the case of flooding the transport layer is vulnerable to attack. Flooding implies sending many connection requests to a vulnerable node. In this

situation, sender must be allocated to manage the connection request. Eventually a node's resources will be exhausted, thus rendering the node useless [3].

In this paper three different network topologies with wormhole attack are examined to observe which deployment of sensing nodes suit best to energy consumption in receive mode and idle mode? Simulation was done by deploying sensing nodes in three different network topologies cellular, grid and random.

This paper is organized as follows. The review of related work is given in Section II. The proposed scheme for three topologies is explained in section III. In Section IV we introduce simulation set up including description of network models parameters and metric to be used to analyze the performance of WSN topologies in presence of wormhole attacks. Simulation results and discussions are presented in Section V. Finally the paper is concluded in Section VI.

II. RELATED WORK

The designers focus specially on two different aspects such as the design of the reliable wireless sensor networks and their management after the deployment when wireless sensor network is used for mission critical applications, [14].

With the passing years, numerous techniques [15-17] and algorithms [18, 19] have been proposed to efficiently design and deploy nodes in wireless sensor networks especially for optimal performance. These techniques and algorithms provide better results, good solutions and satisfying performance to the wireless sensor networks. However, simulation based performance and evaluation of network topologies for wireless sensor network are hardly investigated. In industrial environments for achieving high quality of service, current approaches of node placement in wireless sensor networks are based on designer's experience.

The performance of IEEE 802.15.4 in a star network is simulated and studied in [20]. In this study a network with 49 sensing nodes is deployed to evaluate packet latency and nodes energy. By generating varying amount of background traffic the performance of the star topology is carried out. Another study to analyze the performance of a star network is conducted in [14]. In this research work the performance of the topology is measured with the analysis of average power consumption and packet transmission failure rate.

Unlike random topology, cellular and grid topologies are not extensively investigated by the researchers. In this paper we analyze three network topologies with wormhole attack on the performance metrics of repeat request packets received, energy consumption in receive and idle mode and percentage of time in receive and idle mode.

III. PROPOSED SCHEME

In proposed scheme with increasing nodes in each simulation three topologies namely cellular, grid and random topology are used. In each topology the performance is analyzed with wormhole attacks.

A. Cellular Topology

The cellular topology for wireless sensor network is shown in figure.1.In the figure

BS represents the wireless sensor nodes. Apart from the centre of the cell, the nodes also placed in the corners of the cell. The wormholes are not placed exactly in the center or corner. The wormholes are placed in arbitrary locations.

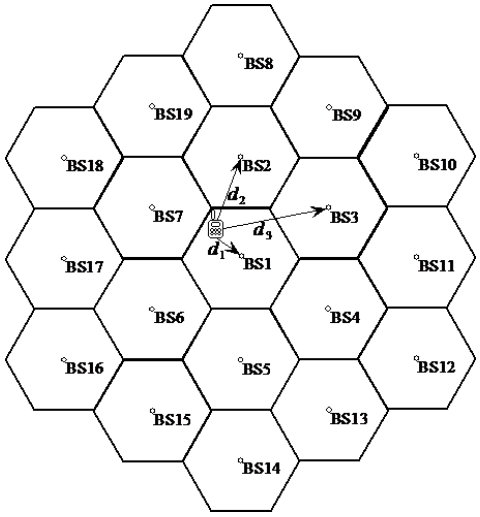

Fig.1.Cellular Topology for Wireless Sensor Network

In the hex world, all points within a distance r of some point form a regular hexagon. In the proposed topology hexagon with centre [100, 100] and radius r=7 is chosen.

Rotation

Using three coordinates, there is an easy trick to rotate a point by 60 degrees around the origin: rotate the coordinates left, and change all the signs:

$$[x, y, z] \rightarrow [-y, -z, -x]$$

(From here it's easy to remove the z-coordinate, as usual, to find:

$$[x, y] \rightarrow [-y, x+y]$$

By applying the trick above repeatedly, we can find similar expressions for points rotated by 120, 180, 240, and 300 degrees.

It is also easy to see immediately whether a point is another point rotated by some multiple of 60. The two points must have the same coordinates (or the same *negative* coordinates), in the same order, but potentially shifted:

We can rotate a point n×60 degrees around any point **c**:

$$R60n(\mathbf{v}–\mathbf{c})+\mathbf{c}$$

Reflection

Reflection about $x = 0$ (y-axis)

- Flip x, keep z, recalculate $y = -x-z$

Reflection about $y = 0$ (x-axis)

- Flip y, keep z, recalculate $x = -y-z$

Reflection about $x+y = 0$ (z-axis)

- Flip both x, y, and z

With suitable translations, we can reflect a point about any line.

For example, to reflect point about the line $x = 1$, we translate the point by $[-1, 0]$, reflect it about the y-axis, and then translate it back by $[1, 0]$.

B. Grid Topology

The figure 2 shows the grid topology for wireless sensor networks. In the figure the number represents the nodes and the values within the brackets show the coordinates in a 2d plane. In the proposed scheme the nodes are separated by 7m vertically and horizontally. As like in cellular topology wormholes are placed in arbitrary locations.

For ease of notation the Cartesian coordinates is used to define node locations. First we describe why a grid topology simplifies the exposition. Since the distance to the nearest node is the same for every node and is equal to the size of the grid, the L1 or Manhattan distance is a meaningful way to measure distances between two nodes. The L1 distance between two nodes ($x1$, $y1$) and ($x2$, $y2$) is given by

$$r = | x1 - x2 | + | y1 - y2 |.$$

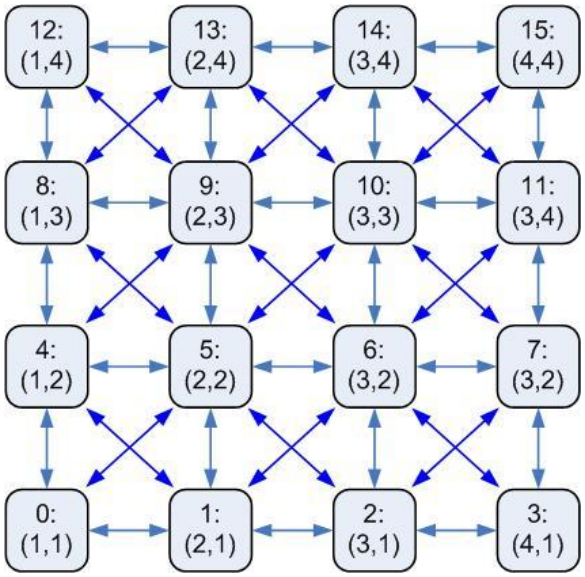

Fig.2.Grid Topology for Wireless Sensor Network

C. Random Topology

The random topology of the wireless sensor network is shown in figure 3.In the figure the circles represent the sensor nodes. In the proposed scheme the nodes are distributed in a two dimensional space uniformly. As like in cellular and grid topology wormholes are placed in arbitrary locations.

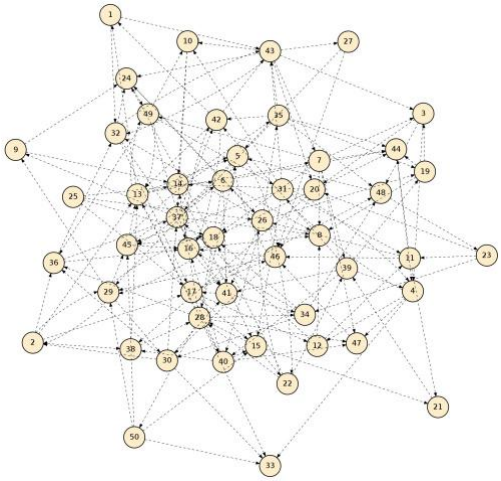

Fig.3.Random Topology for Wireless Sensor Network

Given a fixed number of nodes and a probability p, then each edge between two vertices will be constructed independently with probability p. The pseudo code is presented in Random Graph Algorithm:

Random Graph Algorithm n, p:

A denotes the adjacency matrix of G with n vertices
p denotes the probability that two arbitrary vertices are connected
getRandom() returns uniformly distributed a number over [0; 1]

1. for all $0 \leq i, j \leq n-1$
2. do $A_{i,j} \leftarrow 0$
3. for all $0 \leq i, j \leq n-1$
4. do if $p \leq$ getRandom()

then $A_{i,j} \leftarrow 1$

5. return A

IV. SIMULATION SETUP

The main objective of this study is to analyze and compare the performance of cellular, grid and random WSN topologies with wormhole attack. The performance of these network topologies are measured on the basis of metrics which is mainly

comprised of repeat request packets received, energy consumption in receive and idle mode and percentage of time in receive and idle mode. This section presents a detail description of the network environment, simulation models and parameters and used performance metrics. In this paper, QualNet network simulator is used to perform our simulations. QualNet simulator is one of the best tools available in the market to simulate large, heterogeneous networks and distributed applications.

The figure 4, 5 and 6 shows the cellular, grid and random topology simulation models for wireless sensor networks respectively.

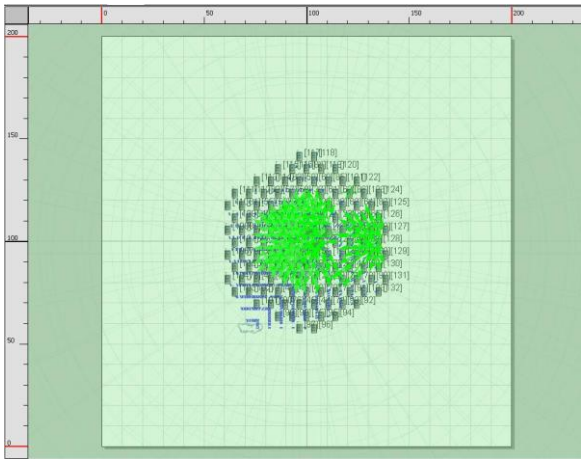

Fig.4.Cellular Topology simulation model of Wireless sensor Network

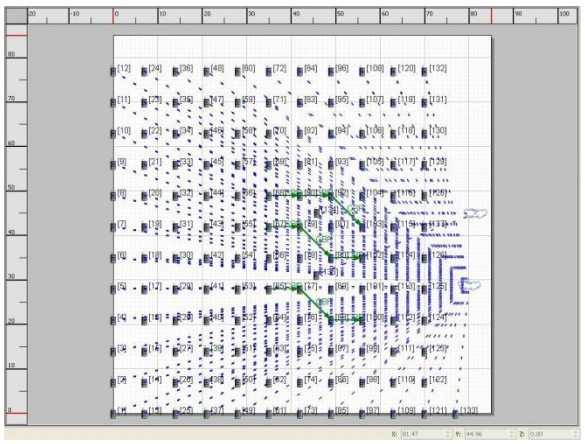

Fig.5.Grid Topology simulation model of Wireless sensor Network

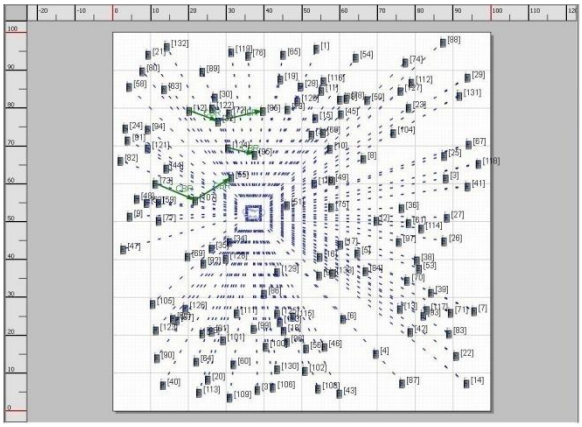

Fig.6.Random Topology simulation model of Wireless sensor Network

In cellular topology for seven cycles the simulation is carried out. In the first cycle single cell with 7 nodes, one node in the centre and remaining 6 nodes are placed in the corners of the hexagon cell. For the second cycle the seven cell cluster is considered but in the outer cells only the nodes placed in the centre of the each cell is considered. The nodes placed in the corners are considered for third cycle simulation. Likewise the nodes are increased for remaining cycles. The nodes in each cycle are 7, 13, 31, 43, 73, 91 and 133 respectively.

For grid and random topology the same numbers of nodes are considered for simulation to maintain uniformity among topologies. The simulation was also carried out for the topologies with wormhole attack. The numbers of wormholes considered in every cycle of simulation of topologies are uniform.

V. SIMULATION RESULTS AND DISCUSSION

To evaluate the effectiveness of the proposed scheme in a wireless sensor network, Qualnet simulator is used for simulation. The simulation configuration and parameters used in this paper is shown in Table 1.

Table 1.Simulation Configuration and Parameters

Parameter	**Value**
Number of Nodes	7, 13, 31, 43, 73, 91 and 133
Transmission Power	3dbm
Energy Model	Mica-Motes
MAC Protocol	CSMA
Wormhole mode	Threshold mode with 75
Wormhole link bandwidth	10000 bits/s
Routing Protocol	AODV
No of Packets	100
Payload Size	128bytes

Simulation Time	30s
Packet Tx Time	25s
Test bed size	200×200 for 7^{th} cycle and variable for remaining
Topology	Cellular, Grid and Random

The effectiveness of the proposed scheme was measured with four different metrics: RREQ packets received, energy consumed in receive mode, energy consumed in idle mode, percentage of time in receive mode and percentage of time in idle mode.

The figure 7(a & b) shows the analysis of RREQ packets received by the nodes in the network for cellular, grid and random topology with and without wormhole attack.

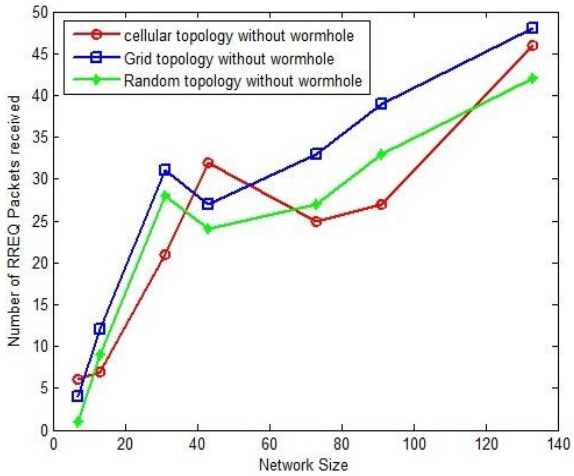

Fig.7a.Analysis of RREQ packets received for cellular, grid and random topology without wormhole attack

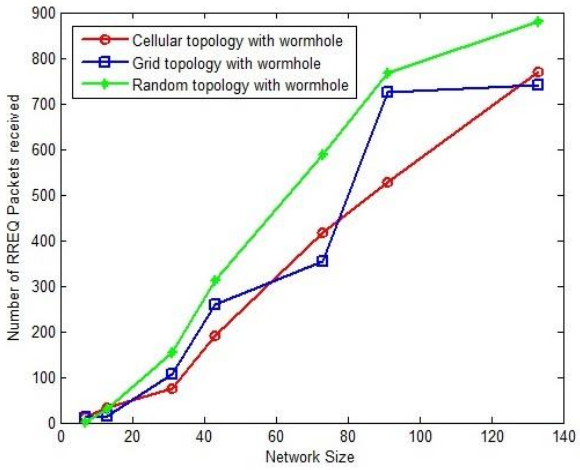

Fig.7b.Analysis of RREQ packets received for cellular, grid and random topology with wormhole attack

From the above figures it is observed that the cellular topology provides better results when compared to grid and random topologies even subjected to wormhole attack.

The energy consumption in receive and idle mode is shown in figure 8(a & b) and 9(a & b) respectively.

The figure 8a shows the analysis of energy consumption in receive mode for all the proposed topologies. It is very much clear that the energy consumption is comparatively low for cellular and grid topologies. But for random topology the energy consumption is more even it is practiced wide.

The analysis of energy consumption in receive mode for cellular, grid and random topology with wormhole attack is shown in figure 8b.From the results it is observed that the energy consumption for cellular topology in receive mode is 9 % and 29 % lesser than grid and random topologies respectively.

In figure 9a the analysis of energy consumption in idle mode for cellular, grid and random topology without wormhole attack is given. The result shows that the energy consumption in idle mode for cellular topology is 0.08% and 0.4% lesser than grid and random topologies respectively.

The following figure 9b shows the energy consumption analysis of cellular, grid and random topology in idle mode with wormhole attack. The energy consumption for cellular topology in idle mode is 8% more than random topology and compared to grid topology is 6%.

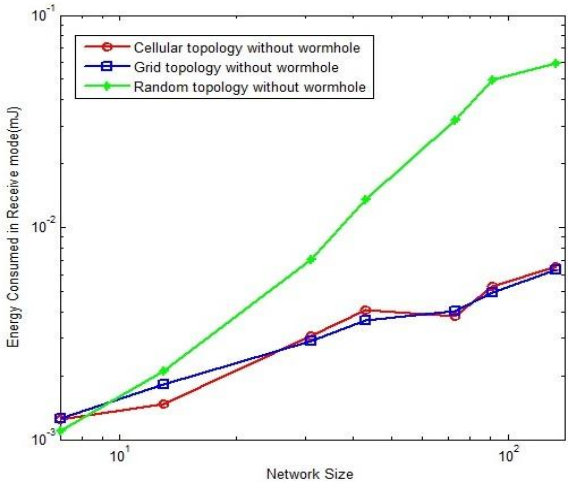

Fig.8a.Analysis of energy consumption in receive mode for cellular, grid and random topology without wormhole attack

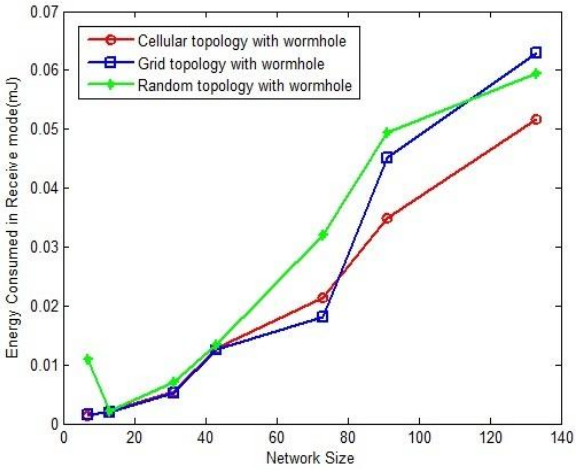

Fig.8b.Analysis of energy consumption in receive mode for cellular, grid and random topology with wormhole attack

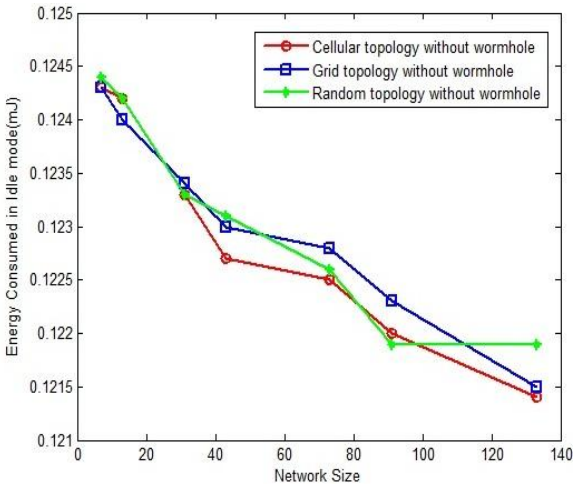

Fig.9a.Analysis of energy consumption in idle mode for cellular, grid and random topology without wormhole attack

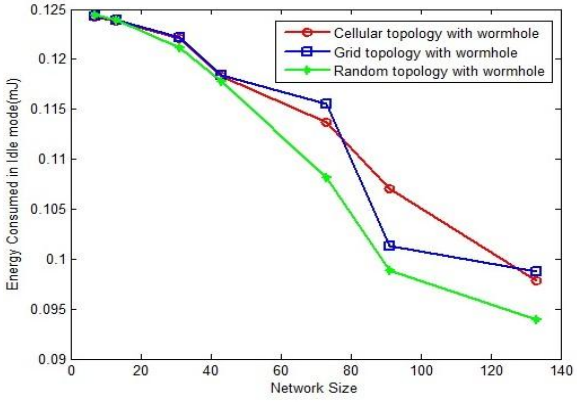

Fig.9b.Analysis of energy consumption in idle mode for cellular, grid and random topology with wormhole attack

The figure 10(a &b) and 11(a &b) shows the analysis of percentage of time the node is in receive and idle mode respectively.

The analysis of percentage of time the node is in receive mode for cellular, grid and random topology without wormhole attack is depicted in figure 10a. The nodes in random topology spend more time when compared to cellular and grid topology. The grid topology spends lesser time in receive mode when compared to cellular topology.

The following figure shows the analysis of percentage of time the node is in idle mode for cellular, grid and random topology with wormhole attack. The nodes in cellular topology spends 30% lesser time in receive mode when compared to the nodes in random topology. But the nodes in grid topology spend 9% time in receive mode when compared to random topology.

The figure 11a represents the analysis of percentage of time the node is in idle mode for cellular, grid and random topology without wormhole attack. The results represents that the percentage of time the node in idle mode for cellular topology with 133 nodes is comparatively smaller than grid and random topology. But for other cycles the nodes in grid topology spends much time in idle mode.

The figure 11b represents the analysis of percentage of time the node is in idle mode for cellular, grid and random topology with wormhole attack. From the figure it is understood that the nodes in cellular topology spends 8% more time than random topology. Whereas the grid topology spends 2.4% more time than random topology.

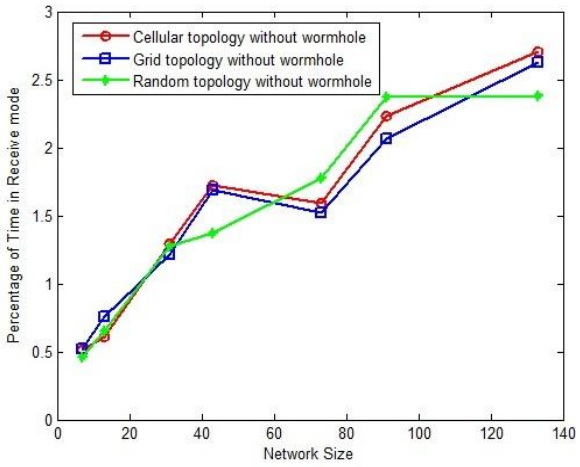

Fig.10a.Analysis of percentage of time the node is in receive mode for cellular, grid and random topology without wormhole attack

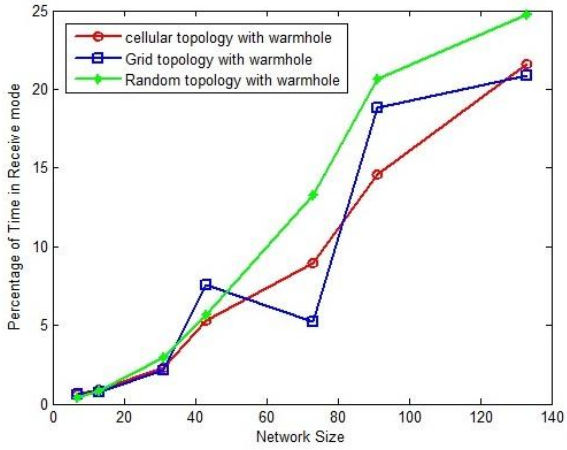

Fig.10b.Analysis of percentage of time the node is in receive mode for cellular, grid and random topology with wormhole attack

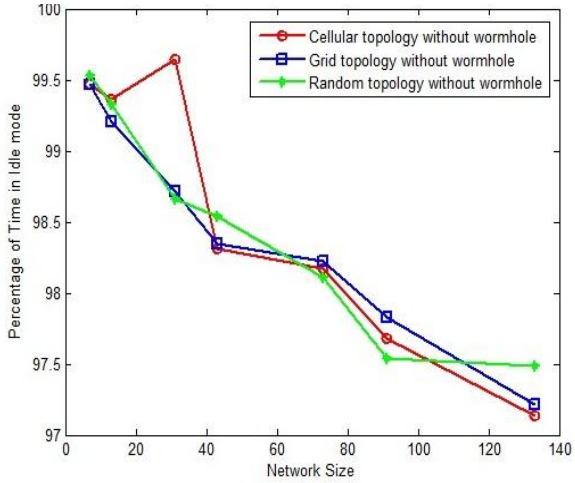

Fig.11a.Analysis of percentage of time the node is in idle mode for cellular, grid and random topology without wormhole attack

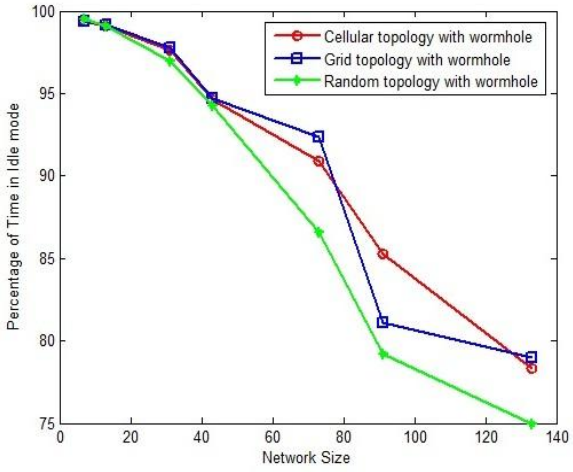

Fig.11b.Analysis of percentage of time the node is in idle mode for cellular, grid and random topology with wormhole attack

VI CONCLUSION AND FUTURE WORK

In this paper the three different network topologies with wormhole attack is examined to observe, which deployment of sensing nodes suit best to energy consumption in receive mode and idle mode?. The simulations are carried out by deploying sensing nodes in three different network topologies cellular, grid and random. From the simulation results it is observed that the cellular topology provides promising results when compared to grid and random topologies in the presence of wormhole attack. The present work only deals with two dimensional locations of the nodes. In future the third dimension for wormholes will be considered and also the analysis will be extended for mobility models for wormholes.

References

[1] R. Muraleedharan and L. A. Osadciw, 2003. "Balancing the performance of a sensor network using an ant system, "

[2] R. Muraleedharan and L. A. Osadciw, 2006. "Jamming attack detection and countermeasures in wireless sensor network using ant system, " *SPIE Defence and Security, Orlando,*

[3] J. P. Walters, *et al.*, 2007 "Wireless sensor network security: A survey, " *Security in distributed, grid, mobile, and pervasive computing*, p. 367.

[4] H.-J. Kim, *et al.*, 2009."A method to support multiple interfaces mobile nodes in PMIPv6 domain, " presented at the Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 2009.

[5] W. Xu, *et al.*, 2005"The feasibility of launching and detecting jamming attacks in wireless networks, ", pp. 46-57.

[6] P. B. Jeon, 2006. "A pheromone-aided multipath QoS routing protocol and its applications in MANETs, " Citeseer,

[7] A. D. Wood and J. A. Stankovic, 2002. "Denial of service in sensor networks, " *Computer*, vol. 35, pp. 54-62,

[8] Y. C. Hu, *et al.*, 2003, "Packet leashes: a defense against wormhole attacks in wireless networks, ", pp. 1976-1986 vol. 3.

[9] H. Deng, *et al.*, 2002."Routing security in wireless ad hoc networks, "*Communications Magazine, IEEE*, vol. 40, pp. 70-75,.

[10] B. Awerbuch, *et al.*, 2002"An on-demand secure routing protocol resilient to byzantine failures, ", pp. 21-30.

[11] W. Enck, *et al.*, 2005 "Exploiting open functionality in SMS-capable cellular networks, ", pp. 393-404.

[12] Y. C. Hu, *et al.*, 2003"Rushing attacks and defense in wireless ad hoc network routing protocols, ", pp. 30-40.

[13] Y. C. Hu, *et al.*, 2003"SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, " *Ad Hoc Networks*, vol. 1, pp. 175-192,

[14] A. Guinard, M. S. Aslam, D. Pusceddu, S. Rea, A. McGibney and D. Pesch, 2011."Design and Deployment Tool for In-Building Wireless Sensor Networks: a Performance Discussion", 7th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, pp. 649-656, Germany,

[15] S. Geethapriya and A. Jawahar, 2013. "Performance Evaluation of Hybrid Topology Control in WSN", International conference on Communication and Signal Processing, pp. 9-13, India,

[16] J. T. Wand, J. D. Xu and H. Q. Liang, 2009."A Density-awareness and Delay-sensitive Data Collecting Scheme for Wireless Sensor Networks", 4th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 475-478, China,

[17] F. Medhat, R. A. Ramadan and I. Talkhan, 2012. "Smart Clustering for Multimodal WSNs", 7th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), pp. 367-372, Canada,

[18] X. Yingxi, G. Xiang, S. Zeyu and L. Chuanfeng, 2012."WSN Node Localization Algorithm Design Based on RSSI Technology", 5th International Conference on Intelligent Computation Technology and Automation (ICICTA), pp. 556-559, China,

[19] C. K. Singh, A. Kumar and P.M. Ameer, August 2008"Performance Evaluation of an IEEE 802.15.4 Sensor Network with a Star Topology", Kluwer Academic Publishers Hingham, MA, USA, Volume 14, Issue 4, pp. 543-568

[20] B. Bougard, F. Catthoor, D.C. Daly, A. Chandrakasan and W.Dehaene, March 2005. "Energy Efficiency of IEEE 802.15.4 Standard in Dense Wireless Microsensor Networks: Modeling and Improvement Perspectives", in Proceedings of Design, automation and test in Europe. IEEE, 2005, Vol.1, pp.196-201,

Authors Biography

Mrs.S.Umamaheswari received the BE degree from Bharathiyar University.Coimbatore, Tamilnadu, India in 1996 and ME degree from Anna University, chennai, Tamilnadu, India in 2005. Currently she is pursuing Ph.D in Information and Communication Engineering under Anna University, India. Now she has been with the Department of Electronics and Communication Engineering at Kumaraguru College of Technology, Coimbatore, Tamilnadu, India as Associate Professor. Her research interests include various topics in Security of Wireless Sensor Networks. He has published many articles and more than fifteen years of teaching and research experience.

Dr.R.Mahalakshmi received the BE and ME degree in Electrical and Electronic Engineering and in Power Systems from Thiagarajar College of Engineering, Madurai, Tamilnadu, India in 1988 and 1989. Currently she is in Sri Krishna College of Technology, Coimbatore, and Tamilnadu, India as Head of the Department of EEE. She received the Ph.D degree in Power Systems from Jawaharlal Nehru Technological University, Hyderabad, Andrapradesh, India in 2010. Her research interests include various topics in Power systems, Power flowing analysis, Flexible AC Transmission systems, and Renewable energy sources.