Effect of 3D Wormholes Attack in Performance Analysis of Wireless Sensor Network for Cellular, Grid and Random Topologies

S.Umamaheswari
Associate Professor,
Department of ECE,
Kumaraguru College of Technology,
Coimbatore, Tamilnadu
Email id: umarajaphd@gmail.com

R.Mahalakshmi
Professor and Head,
Department of EEE,
Sri Krishna College of Technology,
Coimbatore, Tamilnadu

Abstract— Wireless sensor networks (WSN) are usually originated for gathering records from insecure surroundings. Nearly all security protocols for WSN believe that the opponent can do entirely management over a sensing element node by manner of direct physical access. The looks of sensing element networks joined of the most technology within the future has exposed varied challenges to researchers. Wireless sensor networks are composed of huge variety of small sensing element nodes, running singly and in various cases with none access to renewable energy resources. Additionally security being basic to the acceptance and the use of sensing element networks for various applications, conjointly completely different set of challenges in sensing element networks square measure existed. In this paper, specialization will be on security of Wireless Sensor Networks for various topologies with 3D wormhole attack.

Keywords: *Wireless sensor network, 2D and 3D wormhole attack, cellular, grid, random topology*

*****

I. Introduction

Sensor networks by distributed wireless technology area unit employed in various applications. Caused by resource restriction a number of WSN applications work while not security that belittled Quality of Service (QoS). In WSN, a mass of wireless sensors area unit joined along via RF communication links. The standard of operating properly of the nodes in WSN application consists of comprehension, gathering and distributing info within the network. Energy could be a main issue because the sensors area unit generally little. Additionally wireless with restricted memory and quality of operation properly given the actual fact that the batteries have a restricted governing power [1]. Differing kinds of (Denial of Service) DoS attacks will have an effect on a network or node. If attacked node continues to exchange info or ideas with its neighbors and it cause diminish all its power then the node declares as a dead node that is worst cases [2]. Jam could be a well-known attack on physical layer of wireless network. Jam interferes with the radio frequencies getting used by the nodes of a network. Associate aggressor consecutive transmits over the wireless network refusing the underlying waterproof protocol. Jam will interrupt the network spectacular if one frequency is employed throughout the network. Additionally jam will cause excessive energy consumption at a node by injecting impertinent packets. The receiver’s nodes can moreover consume energy by obtaining those packets [4].Xu, Trappe, Zhang associated Wood in 2005 projected [5] four totally different kind of jam attack that may be utilized by an aggressor to prevent the operation of a wireless network. However every model affects on the causing and receiving capability of a wireless node and its excellence were evaluated. it absolutely was remarked that no single system of measures like carrier sensing time and signal strength is adequate for faithfully police investigation the conduct of a transmitter, which victimization packet delivery cannot acknowledge whether or not poor link service was owing to the quality of nodes or jam whereas it's going to be efficacious in mark as totally different between jam-pawn ked situations and full. Meddling is another attack on physical layer. In this attack, nodes area unit prone to meddling or physical hurt [6].

Attacks also can be created on the link layer. Associate in nursing offender might premeditatedly violate the communication protocol, and often send messages in an endeavor to cause collisions. This sort of collisions would wish the retransmission of any packet influenced by the collision. By means that of this method it'd be doable for Associate in nursing individual to consume simply a sensing element node’s power provide by forcing oversupply retransmissions [3].

A sensing element node might get good thing about multi hop mistreatment merely refusing to route messages at the network layer. this might be dead often or on an irregular basis with world wide web result being that any neighbor United Nations agency marks a route through the malevolent node a minimum of are incapable of exchange messages with, a part of the network [3, 7].

Entry by force or while not permission in network layer is sorted into 2 categories: passive and active attacks. A passive trespass doesn't interrupt the functioning of the network; however the antagonist to find info eavesdrops on the traffic flowing across the network while not modifying the info.
It’s terribly tough to observe passive attack in sight of the very fact that a passive attack doesn't influence the functioning of the network. On the opposite facet, associate assaulter will attack knowledge packets inflicting imperfect communication, though it assists with alternative nodes to

create legal routes between senders and receivers. As an example wormhole attacks [8], Blackhole attacks [9], Byzantine attacks [10], DDoS attacks [11] and routing attacks [12, 13] are active attacks.

Furthermore the transport layer is at risk of attack, as within the case of flooding. Flooding is one thing straightforward like causation several association requests to a vulnerable node. During this scenario, sender should be allotted to manage the association request. Eventually a node's resources are going to be exhausted, so rendering the node useless [3].

In this paper examining has been done for three different network topologies with wormhole attack to observe, which deployment of sensing nodes suit best to energy consumption in receive mode and idle mode? We implemented our simulations 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 our 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

Most current wireless sensing element networks analysis assume that the sensors area unit deployed on a two-dimensional (2D) plane. This is often an honest approximation for applications wherever sensors area unit deployed on earth surface and wherever the peak of the network is smaller than transmission radius of a node. In these networks, the peak of the network is negligible as compared to the length and also the breadth. However, this 2nd assumption is profaned in underwater, region and area applications wherever height of the network will be important and nodes area unit distributed over a three-dimensional (3D) area. Though such networks might not exist at the moment, there are a unit works ongoing that may build 3D networks more and more common within the close to future. the difficulty of coverage and property in 3D networks has been self-addressed in [14]. that employment assumes that nodes will be placed anyplace with any capricious exactness in an exceedingly 3D area and solves the matter of finding best placement of nodes specified full coverage of a 3D area is achieved with minimum variety of nodes.

Reducing the amount of active nodes directly contributes to the extension of network lifespan. However, maintaining full property needs that the utmost distance between the active nodes of any 2 first-tier neighboring cells cannot exceed the transmission radius (i.e., communication range). Since active node are often settled anyplace within a cell, the utmost distance between 2 furthest points of 2 first-tier neighboring cells should be but or up to the transmission radius.

As mentioned in [14], proving optimality in several 3D issues is amazingly troublesome, despite the fact that proofs for similar issues in 2nd may be found simply. whereas deploying wireless device network for mission crucial applications, the designers focus specially on 2 totally different aspects, these area unit the look of the reliable wireless device networks and their management when the readying [15].

With the passing years, varied techniques [16- 18] and algorithms [19, 20] are projected to expeditiously style and deploy nodes in wireless sensing element networks particularly for best performance. These techniques and algorithms give higher results, sensible solutions and satisfying performance to the wireless sensing element networks. However, simulation primarily based performance and analysis of network topologies for wireless sensing element network are hardly investigated. In industrial environments for achieving prime quality of service, current approaches of node placement in wireless sensing element networks are supported designers' expertise.

The performance of IEEE 802.15.4 in an exceedingly star network is simulated and studied in [21]. During this study a network with forty nine sensing nodes is deployed to judge packet latency and nodes energy. The performance of the topology is allotted by generating variable quantity of background traffic. Another study to research the performance of a star network is conducted in [15]. During this analysis 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 aren't extensively investigated by the researchers. During this paper we have a tendency to analyze 3 network topologies with 3D wormhole attack on the performance metrics of repeat request packets received, energy consumption in receive and idle mode and share of time in receive and idle mode.

III. PROPOSED SCHEME

In proposed scheme three topologies namely cellular, grid and random topology are considered with increasing nodes in each simulation. In each topology the performance is analyzed with 3D wormhole attacks.

A. Cellular Topology

The cellular topology for wireless sensor network is shown in figure.1 (a,b&c).In the figure1a BS represents the wireless sensor nodes. Apart from the centre of the cell, the nodes also placed in the corners of the cell. The 3D wormholes are not placed exactly in the center or corner. The 3D wormholes are placed in arbitrary locations.

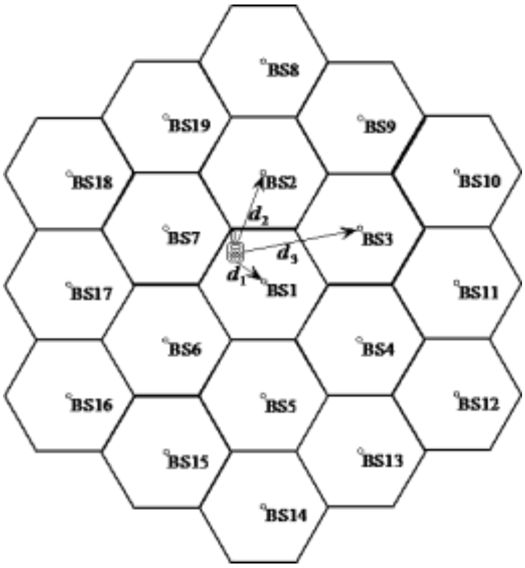

Fig.1a.Cellular Topology for Wireless Sensor Network

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.

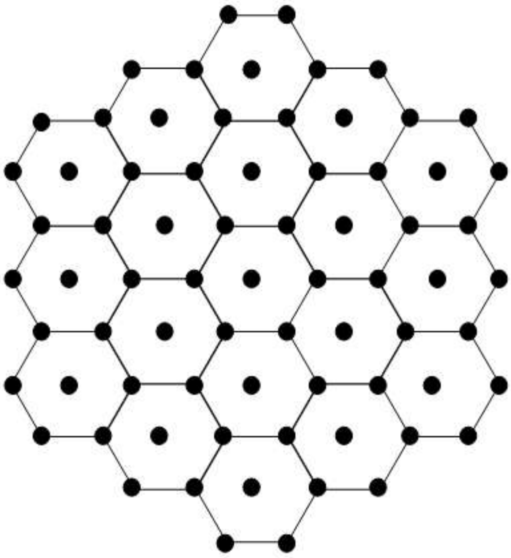

Fig.1b. Cellular Topology for Wireless Sensor Network with nodes placement at the centre and edges of the cell.

The figure 1c shows the cellular topology which forms triangular topology when the nodes are placed at the centre of each cell.

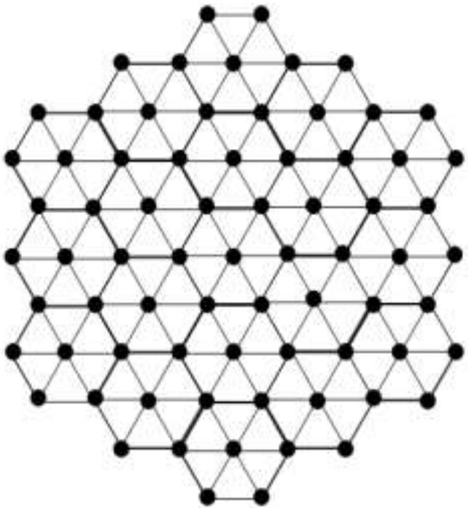

Fig 1c. Cellular Topology for Wireless Sensor Network which forms triangular topology.

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].

The figure 1b shows the cellular topology with node placements at the centre and edges of each cell which finally forms 7 tiers.

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 |.

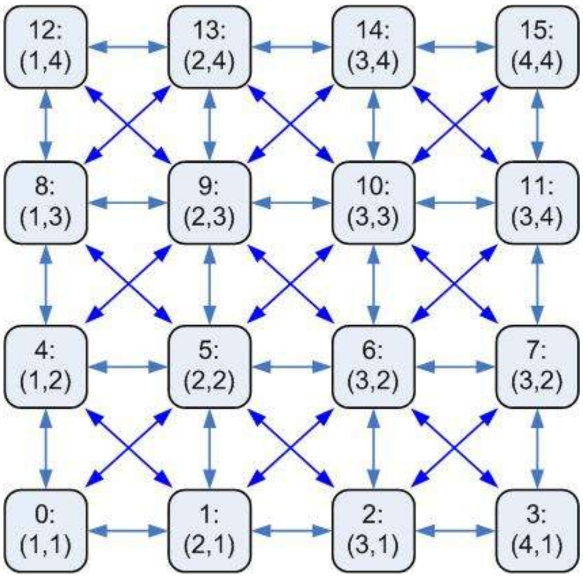

Fig.2.Grid Topology for Wireless Sensor Network

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 worm holes are placed in arbitrary locations.

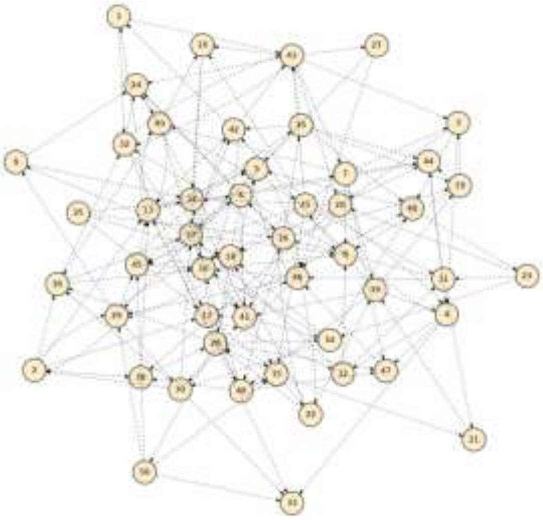

Fig.3.Random Topology for Wireless Sensor Network

Given a fixed number of nodes and a probability p, then each edge between two vertices will be constructed independently with probability p. The pseudocode 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]

```
for all $0 \leq i , j \leq n-1$
        do $A_{i,j} \leftarrow 0$
for all $0 \leq i , j \leq n -1$
        do if $p \leq$ getRandom()
            then $A_{i,j} \leftarrow 1$
return A
```

IV. SIMULATION SETUP

The main objective of our study is to research and compare the performance of cellular, grid and random WSN topologies with 3D wormhole attack. In earlier work solely 2 dimensional coordinates area unit thought-about for the position of wormhole. However during this analysis work 3 dimensional coordinates area unit thought-about for the position of wormholes. The performance of those network topologies area unit measured on the bases of metrics that is principally contains of repeat request packets received, energy consumption in receive and idle mode and proportion of time in receive and idle mode. This section presents a detail description of the network surroundings, simulation models and parameters and used performance metrics. In this research work QualNet is used as network simulator to perform our simulations. QualNet simulator is one in every of the simplest tools obtainable within the market to simulate massive, heterogeneous networks and distributed applications.

The figure 4(a&b),5(a&b) and 6(a&b) shows the cellular ,grid and random topology simulation models for wireless sensor networks with 2D and 3D wormholes respectively.

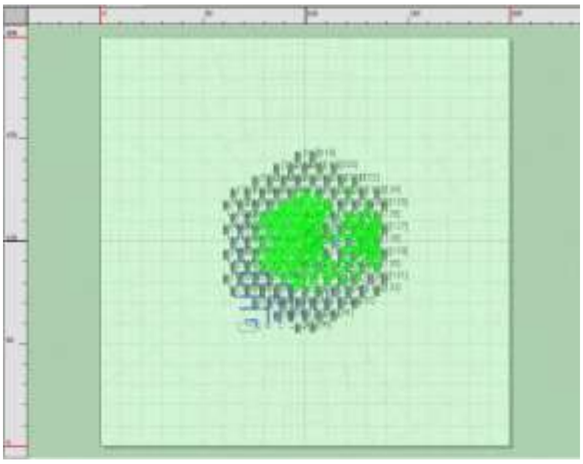

Fig.4a.Cellular Topology simulation model of Wireless sensor Network with 2D wormholes

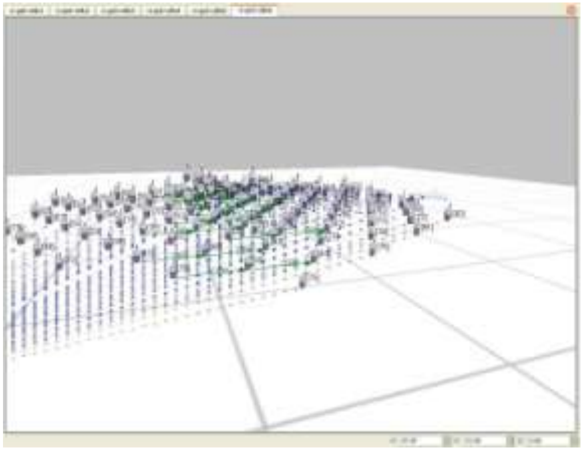

Fig.4b.Cellular Topology simulation model of Wireless sensor Network with 3D wormholes

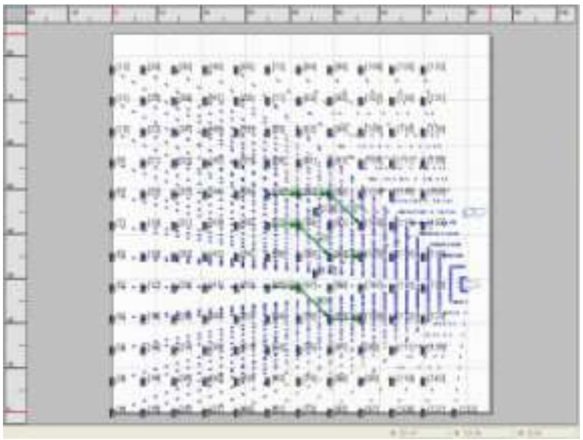

Fig.5a.Grid Topology simulation model of Wireless sensor Network with 2D wormholes

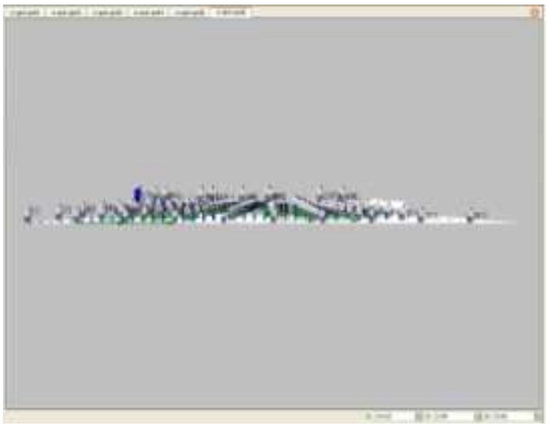

Fig.5b.Grid Topology simulation model of Wireless sensor Network with 3D wormholes

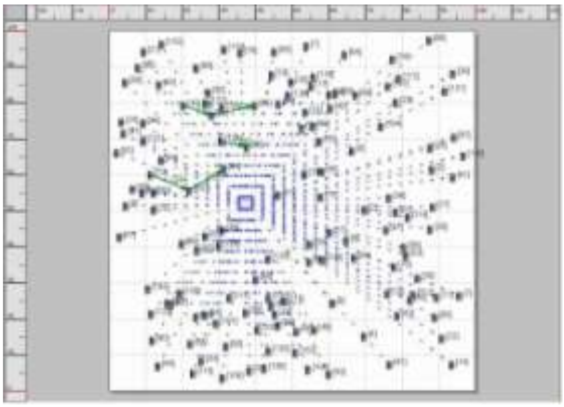

Fig.6a.Random Topology simulation model of Wireless sensor Network 2D wormholes

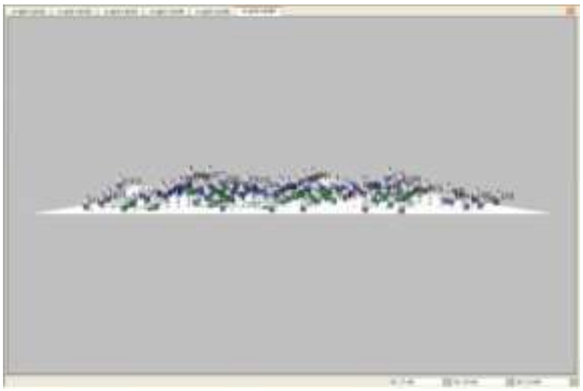

Fig.6b.Random Topology simulation model of Wireless sensor Network 3D wormholes

In cellular topology the simulation is applied for seven cycles. within the initial cycle single cell with seven nodes, one node within the centre and remaining six nodes square measure placed within the corners of the polygon cell. For the second cycle the seven cell cluster is taken into account however within the outer cells solely the nodes placed within the centre of the every cell is taken into account. The nodes placed within the corners square measure thought-about for third cycle simulation. Likewise the nodes square measure inflated for remaining cycles. The nodes in every cycle square measure seven, 13, 31,43,73,91 and 133 severally.

For grid and random topology the same numbers of nodes are considered for simulation to maintain uniformity among topologies. The simulation also carried out for the topologies with 2D and 3D wormhole attack. The numbers of wormholes also considered in every cycles of simulation of topologies are uniform.

V.SIMULATION RESULTS AND DISCUSSION

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

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.

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
Worm Hole mode	Threshold mode with 75
Worm hole 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 7th cycle and variable for remaining
Height for 3D wormholes	3m
Topology	Cellular, Grid and Random

The figure 7(a,b&c) shows the analysis of RREQ packets received by the nodes in the network for cellular, grid and random topology without wormhole attack ,with 2D and 3D wormhole attack respectively.

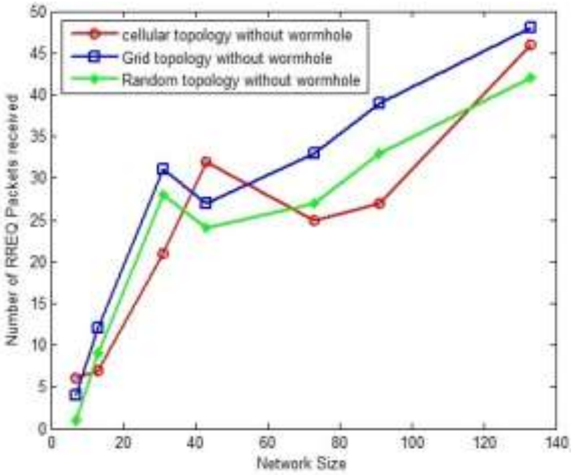

Fig.7a.Analysis of RREQ packets received for cellular, grid and random topology without wormhole attack

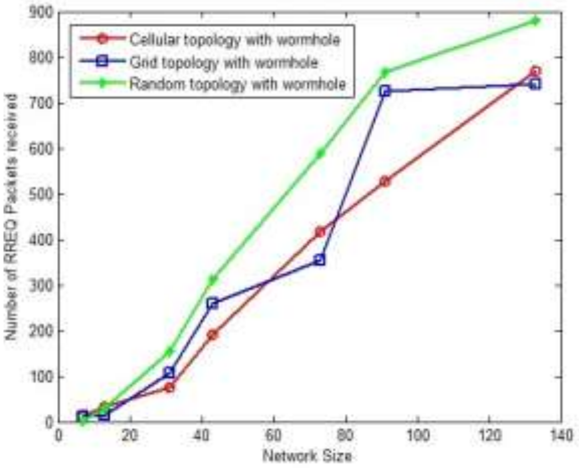

Fig.7b.Analysis of RREQ packets received for cellular, grid and random topology with 2D wormhole attack

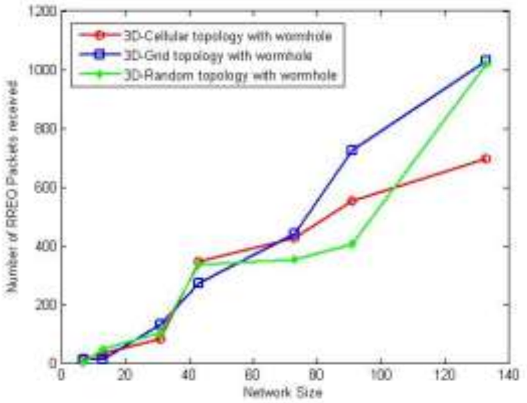

Fig.7c.Analysis of RREQ packets received for cellular, grid and random topology with 3D wormhole attack

From the above figures 7a & 7b it is observed that the cellular topology provides better results when compared to grid and random topologies even subjected to wormhole attack.

When the network is subjected to 3D wormhole attack cellular topology provides better results even when the network size is more. Even though the distance increases because of 3D position of wormholes number of RREQ packets increases in grid and random topologies. But in case of cellular topology the number of RREQ packets received decreases when compared to 2D wormhole attack.

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

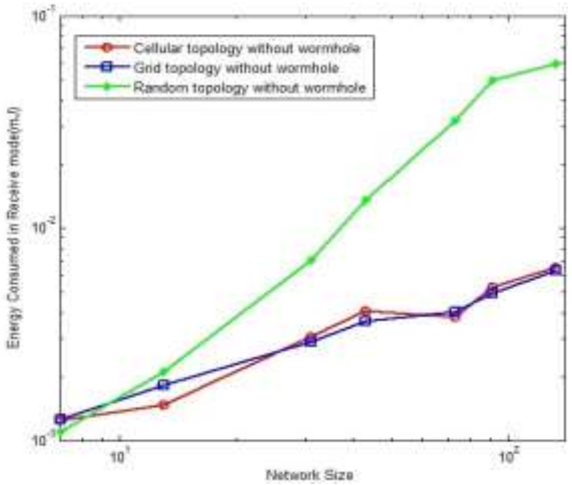

Fig.8a.Analysis of energy consumption in receive mode for cellular, grid and random topology without wormhole attack

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.

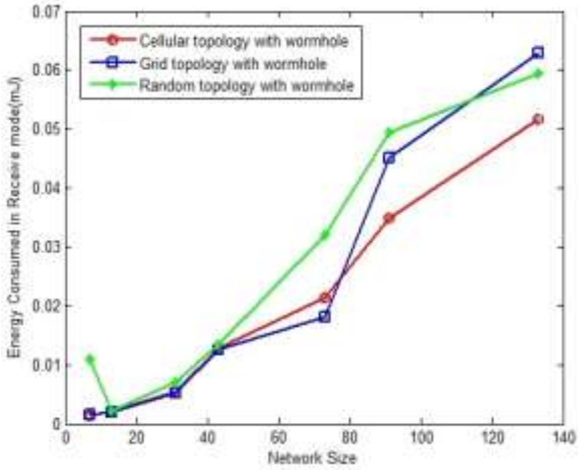

Fig.8b.Analysis of energy consumption in receive mode for cellular, grid and random topology with 2D wormhole attack

The figure 8c shows the analysis of energy consumption in receive mode for cellular, grid and random topology with 3D wormhole attack. From the results it is evident that cellular topology with 3D wormhole attack in receive mode is 27.62 % and 36.6 % lesser than grid and random topologies respectively. Energy consumption for cellular topology with 3D wormhole attack is 5.2% lesser than Energy consumption for cellular topology with 2D wormhole attack.

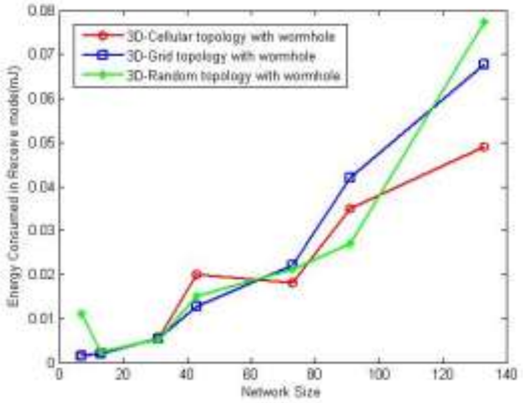

Fig.8c.Analysis of energy consumption in receive mode for cellular, grid and random topology with 3D wormhole attack

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.

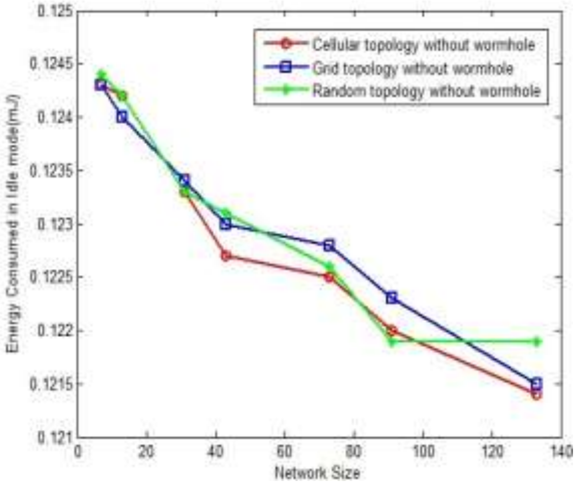

Fig.9a.Analysis of energy consumption in idle mode for cellular, grid and random topology without wormhole attack

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%.

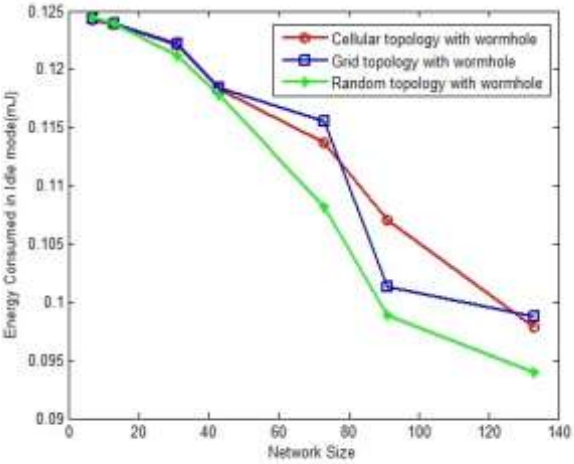

Fig.9b.Analysis of energy consumption in idle mode for cellular, grid and random topology with wormhole attack

The figure 9c shows the analysis of energy consumption in idle mode for cellular, grid and random topology with 3D wormhole attack. From the results it is apparent that cellular topology with 3D wormhole attack in idlel mode is 3.37 % and 2.47 % lesser than grid and random topologies respectively. Energy consumption for cellular topology with 3D wormhole attack is 3.3% lesser than Energy consumption for cellular topology with 2D wormhole attack.

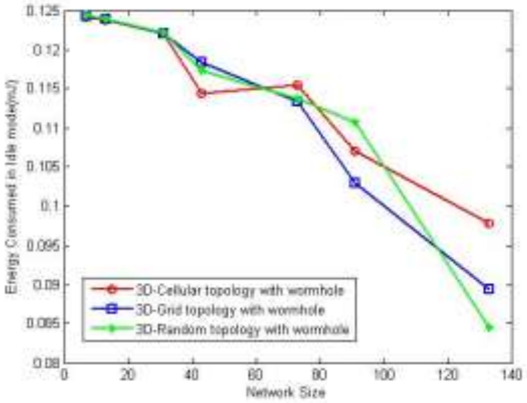

Fig.9c.Analysis of energy consumption in idle mode for cellular, grid and random topology with 3D wormhole attack

The figure 10(a, b &c) and 11(a, b &c) 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.

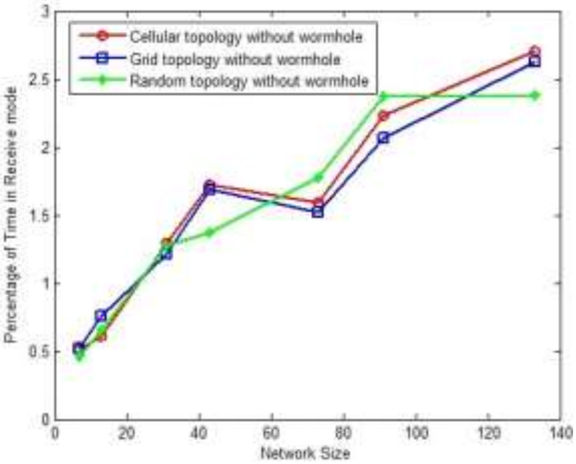

Fig.10a.Analysis of percentage of time the node is in receive mode for cellular, grid and random topology without wormhole attack

The following figure shows the analysis of percentage of time the node is in receive 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.

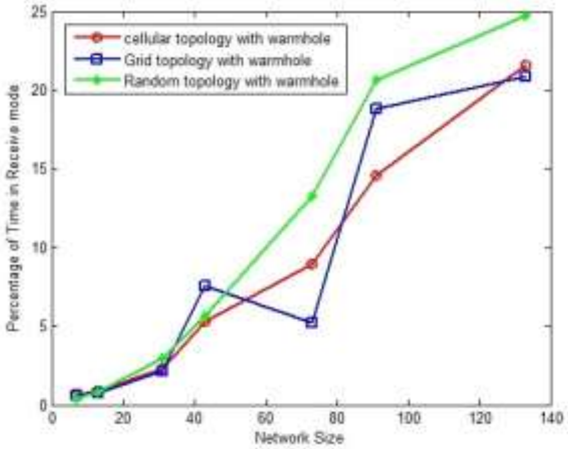

Fig.10b.Analysis of percentage of time the node is in receive mode for cellular, grid and random topology with wormhole attack

The figure 10c shows the analysis of percentage of time the node is in receive mode for cellular, grid and random topology with 3D wormhole attack. The nodes in cellular topology spends 27.5% and 36.44% lesser time in receive mode when compared to the nodes in grid and random topologies respectively. Time consumption for cellular topology with 3D wormhole attack in receive mode is 5% lesser than time consumption for cellular topology with 2D wormhole attack in receive mode.

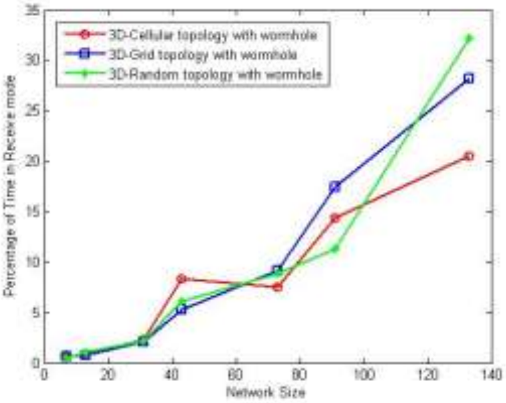

Fig.10c.Analysis of percentage of time the node is in receive mode for cellular, grid and random topology with 3D wormhole attack

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.

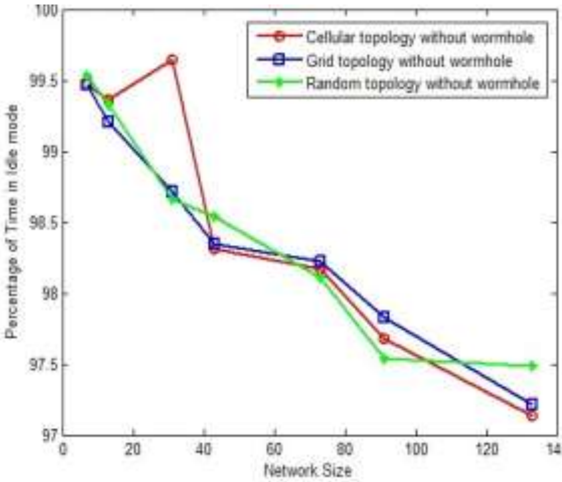

Fig.11a.Analysis of percentage of time the node is in idle mode for cellular, grid and random topology without wormhole attack

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.

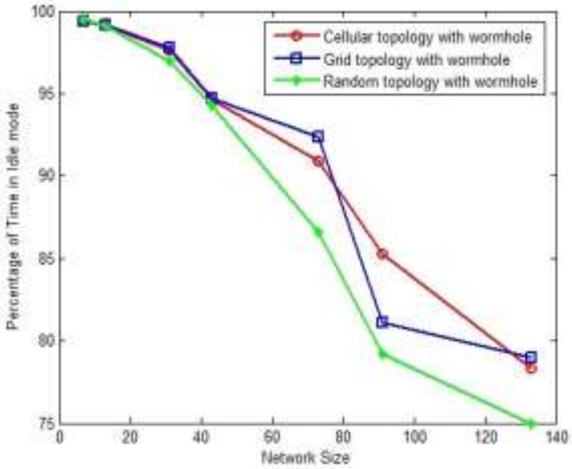

Fig.11b.Analysis of percentage of time the node is in idle mode for cellular, grid and random topology with wormhole attack

The figure 11c shows the analysis of percentage of time the node is in idle mode for cellular, grid and random topology with 3D wormhole attack. The nodes in cellular topology spend 11.11% and 17.34% more time in idle mode when compared to the nodes in grid and random topologies respectively. Time consumption for cellular topology with 3D wormhole attack in idle mode is 1.35% lesser than time consumption for cellular topology with 2D wormhole attack in idle mode.

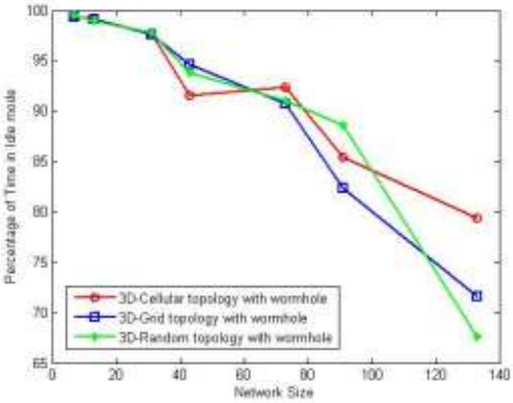

Fig.11c.Analysis of percentage of time the node is in idle mode for cellular, grid and random topology with 3D wormhole attack

VI CONCLUSION AND FUTURE WORK

In this paper the 3 totally different network topologies with 2D and 3D wormhole attack is examined to watch, that preparation of sensing nodes suit best to energy consumption in receive mode and idle mode. The simulations square measure administrated by deploying sensing nodes in 3 totally different network topologies cellular, grid and random. From the simulation results it's observed that the cellular topology provides promising results compared to grid and random topologies with the presence of 2D and 3D wormhole attacks. The cellular topology with nodes at the centre of cells form triangular topology and with wormholes at the peak of 3metres form pyramids. The current work solely deals with static nodes.

In future the analysis is going to be extended for mobility models for 2D and 3D wormholes.

References

1. R. Muraleedharan and L. A. Osadciw, "Balancing the performance of a sensor network using an ant system," 2003.
2. R. Muraleedharan and L. A. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system," SPIE Defence and Security, Orlando, 2006.
3. J. P. Walters, et al., "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, p. 367, 2007.
4. H.-J. Kim, et al., "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., "The feasibility of launching and detecting jamming attacks in wireless networks," 2005, pp. 46-57.
6. P. B. Jeon, "A pheromone-aided multipath QoS routing protocol and its applications in MANETs," Citeseer, 2006.
7. A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, pp. 54-62, 2002.
8. Y. C. Hu, et al., "Packet leashes: a defense against wormhole attacks in wireless networks," 2003, pp. 1976-1986 vol. 3.
9. H. Deng, et al., "Routing security in wireless ad hoc networks,"Communications Magazine, IEEE, vol. 40, pp. 70-75, 2002.
10. B. Awerbuch, et al., "An on-demand secure routing protocol resilient to byzantine failures," 2002, pp. 21-30.
11. W. Enck, et al., "Exploiting open functionality in SMS-capable cellular networks," 2005, pp. 393-404.
12. Y. C. Hu, et al., "Rushing attacks and defense in wireless ad hoc network routing protocols," 2003, pp. 30-40.
13. Y. C. Hu, et al., "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," Ad Hoc Networks, vol. 1, pp. 175-192, 2003.
14. S. M. Nazrul Alam and Zygmunt Haas, Coverage and Connectivity in Three-Dimensional Networks, In Proc of ACM MobiCom, 2006.
15. Guinard, M. S. Aslam, D. Pusceddu, S. Rea, A. McGibney and D. Pesch, ”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, 2011.
16. S. Geethapriya and A. Jawahar, ”Performance Evaluation of Hybrid Topology Control in WSN”, International conference on Communication and Signal Processing, pp. 9-13, India, 2013.
17. J. T. Wand, J. D. Xu and H. Q. Liang, ”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, 2009.
18. F. Medhat, R. A. Ramadan and I. Talkhan, ”Smart Clustering for Multimodal WSNs”, 7th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), pp. 367-372,Canada, 2012.
19. X. Yingxi, G. Xiang, S. Zeyu and L. Chuanfeng, ”WSN Node Localization Algorithm Design Based on RSSI Technology”, 5th International Conference on Intelligent Computation Technology and Automation (ICICTA), pp. 556-559, China, 2012.
20. C. K. Singh, A. Kumar and P.M. Ameer, ”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 August 2008.
21. B. Bougard, F. Catthoor, D.C. Daly, A. Chandrakasan and W.Dehaene, ”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, March 2005.

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 Nehu 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.