*International Journal of Engineering Inventions*
*e-ISSN: 2278-7461, p-ISSN: 2319-6491*
*Volume 6, Issue 1 [Jan. 2017] PP: 61-68*

# PHY-MAC Layer Configuration Based Energy Efficiency for Improving the Quality of Service in Mobile Ad-Hoc Network

S.R.Raja Associate Professor, Dr.K.Alagarsamy
*MCA Dept. K.L.N.College of Engineering, Madurai,Tmailnadu,India*
*Reader In Computer Science, Madurai Kamaraj University, Madurai, Tamilnadu,India*

**Abstract:** Mobile adhoc networks are one of the rapidly growing wireless networks. The number of mobile nodes, data transmission among the nodes and the mobility speed of the networks are increasing day by day. Due to scalability, the routing protocols cannot change its behavior in terms improving the quality of service. The existing routing protocols are facing lot of problems in terms of scalability and mobility. In order to solve these kind of problems Physical and MAC layers of the existing routing protocols are configured to concentrate on providing better quality of service during data transmission in the network. Slot allocation, Priority-Queue management and garbage collection are the three different tasks are carried in the proposed approach which can help to increase the QoS in the wireless network. This approach is simulated in NS2 software and the results are verified for investigating the QoS.

***Keywords:*** *MANET, Wireless Networks, QoS, AODV, MAC-Layer.*

## I BACKGROUND STUDY

The wireless sensor network (WSN) has a set of compact and automated devicescalled sensing nodes such as Berkeley MICA Mote [1, 2], SmartDust [3-5], andCotsDust [6] . It is a computational device consisting of memory, battery, processor,transceiver, and a sensing device. It can be distributed across an area and has the ability tocommunicate among them,thus forming an adhoc network. The information collectedby the sensor network are processed and stored by a special node called sink node.If two nodes are not in their transmission range,they will undergo multiple hops forcommunication. Environmental monitoring, infrastructure management, public safety,medical, home and office security, transportation, and battlefield surveillance are some of theapplications envisaged for sensor networks. Due to their criticality, these applications havethe probability to be attacked. In this work, we centered on two types of attacks: HELLOflood attacks [7] and wormhole attacks [8].When the nodes want to announce their presenceand proximity to their neighbors, they use HELLO messages in many protocols. Acountermeasure for wormhole attacks in ad hoc network [8] has been proposed by Hu,Perrig, and Johnson. They also introduced the concept of a packet leash which is a piece ofadditional information added to standard packets in order to restrict its maximum allowedtravel distance.

Mobile Ad Hoc Network (MANET) is the Ad Hoc network consisted of mobiledevices which are a self-configuring and self-organized network without fixed infrastructure [9].In MANET, any node can join and leave the network whenever they want. Only the neighbornodes can receive the information of the sender node. It lead that nodes play both the role ofuser and router. MANETs have good robustness because there are no center nodes.An anonymous on-demand routing protocol called MASK, one of the IDS which wasdeveloped by Yanchao Zhang, Wei Liu and Wenjing Lout from department of Electrical andComputer Engineering of University of Florida. The aim of the MASK is to operate againsttraffic analysis attacks.A pairing-based cryptography is used as the cryptographic foundation in MASK. Theanonymity of MASK consist of two parts-One is anonymous MAC-Layer communicationswhile the other is anonymous network-layer communications [10].The anonymous MAC-layer communications is about how to achieve anonymous single-hop MAC-layercommunications through an anonymous neighborhood authentication protocol [11]. It isrudimentary according to anonymous neighborhood authentication and anonymous MACframe exchange.

## II PROBLEM STATEMENT

In this paper initially the class of vulnerabilities drained the energy of the sensor devices while they are in active mode else it is in sleep mode to save energy. Using content based slot allocation in MAC protocols, make the sensor devices in sleep mode as much as possible. A malicious user who knows about MAC protocol can exploit the environment. In this research, it is analyzed that the functionality of the all the types of MAC protocol [T-MAC [12], S-MAC [13], -MAC, ESR-MAC, from that analysis, design and describe a new mechanism for MAC-layer, to reduce the resource consumption for WSN. This research is motivated to design, implement and evaluate a novelty suite for low-overhead, cross-layer and platform independent which can mitigate the resource-consumption attacks. The clustered malicious suite incorporates a low overhead, no-replay

mechanism, a rate-allocated-contention-slot mechanism, and detecting traffic jam and mitigation to identify the sensors is in wakeup mode. All these mechanisms are combined together to improve mitigation and prevention of any kind of malicious activity in WSNs.

## III EXISTING APPROACH

In this paper the requests of WSN environment is examined, and proposed A THREE STAGE SECURITY - [**TSS**] mechanism [3], which has three stages where in the first stage energy utilization is diminished by circular path clustering based routing and allocating a random key for each nodes in the network. In the second stage of TSS mechanism verifies and validates the nodes for authentication based communication among the nodes. In the third stage of TSS, using ECC encryption strategy, secured data is passed among the nodes in the network. But the efficacy of the TSS approach is not applicable for scalability.

## IV PROPOSED WORK

The proposed method DASA is accompanied in three steps. **Step-1** involves in analyzing the MAC protocols for scheduling and security provision. Designing and implementing an analytical model of this provision is showing the efficiency and effectiveness of the MAC protocol of WSN. **Step-2** is involved in developing a mechanism using Jain's ten-step performance evaluation method [5]. Finally, **Step-3** involved in testing and validating the denial-of-sleep mitigation mechanisms. This paper is motivated to improve the effectiveness of the network in terms of a network-lifetime, by mitigating any attacks.

This paper is motivated, to improve the **effectiveness** of the network in terms of a network-lifetime, by mitigating and eliminating denial-of-sleep attacks. Reducing the **low overhead** by limiting the request and reply among sensor nodes, where it increases the throughput of the network. To deploy our mechanism functionalities into the existing MAC protocol, there will be a **minimum modification** is applied. The mechanism is developed in such a manner and in such a platform, where this mechanism becomes a **platform independent** one for any existing WSN protocols. The **configured MAC** protocol is added with features which can prevent, mitigate and eliminate denial-of-sleep attacks. This feature can accommodate various MAC protocol vulnerabilities. One of the main objectives of this paper is to develop a mechanism based on a MAC protocol which can be applied to anti-denial-of-sleep mechanism in any existing as well as in future protocols during the compile time. Table-1 shows all the metrics used for designing the malicious mitigation mechanism. These metrics are quantitative which includes network lifetime, network throughput and memory overhead.

| **Design Criteria** | **Goal** |
|---|---|
| *Effectiveness* | *Maintain network lifetime of* 90% *or better while under attack as compared to a network not under attack.* |
| *Low overhead* | 1. *Use an average of less than* 5% *total memory per node.* |
| | 2. *Reduce network lifetime by* 5% *or less while not under attack* |
| | 3. *Cause* 2% *or less reduction in network throughput while not under attack.* |
| | 4. *Minimize processor overhead through efficient coding and by avoiding floating point calculations.* |
| *Minimum modification to existing protocols* | 1. *Protocols function normally when not under attack.* |
| | 2. *Allow application compilation with or without added denial − of − sleep mitigation mechanisms.* |
| *Platform independence* | *Show effectiveness on multiple platforms through simulation and implementation.* |
| *MAC protocol independence* | *Demonstrate effectiveness on* $S-MAC, T-MAC, B-MAC,$ |
| *Automatic reaction to attack* | *React to attacks based on all of the vulnerabilities* |
| *User configurability* | *Allow user to easily modify which denial − of − sleep mitigation components are used and to modify component parameters in configuration file.* |

**Table-1:** System Design Goals and Metrics

**Analysis of MAC**

**S-MAC**

S-MAC utilizes a fixed number and size of duty cycle. The sleep mode utilizes the deployed radios the remaining time and node lifetime is increased significantly. Nodes in the S-MAC are organizing themselves by using the synchronization messages within a time interval. The nearest

nodes overhear the sync messages and synchronize its schedules with the other nodes and 90% of the sleep time saves more energy of the node, is depicted in Figure-1.

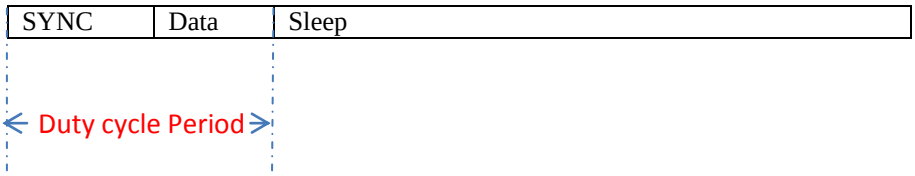


**Figure-1**: S-MAC Frame Structure

T-MAC

T-MAC is an improved version of S-MAC and it is concentrating on the traffic only during the time of duty period for improving the energy efficiency. The following Figure-2 depicts the message transmission and receiving. T-MAC also follows the SYNC message used in S-MAC. The stipulated awake period with the adaptive timeout technique allows all the nodes to sleep at the time of most traffic. During the time of node awake, each node can sense the activities in the wireless channel and resets the time to sleep for the timeout value. If there is no traffic is observed, then the time to sleep is expired and the node goes to sleep mode. T-MAC follows RTS-CTC mechanism based message passing and it can be represented as:

$$TA = 1.5 \times (T_{CW} + T_{RTS} + T_{SIFS})$$

Where, $T_{CW}$ denotes the duration of the contention slot allocation, $T_{RTS}$ denotes the time to send RTS and $T_{SIFS}$ is the minimum inter-frame space.

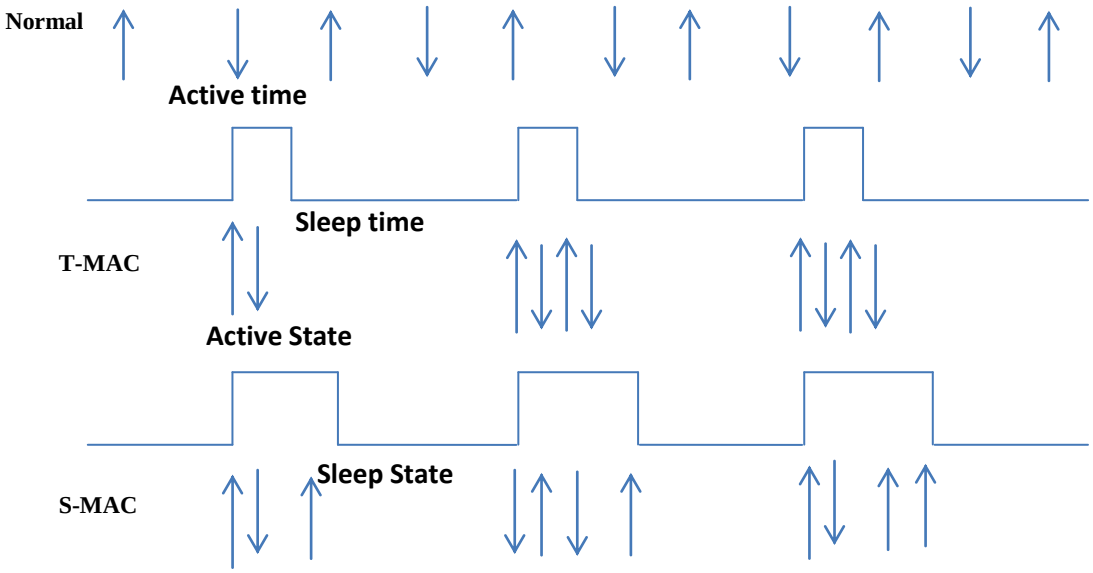


**Figure-2:** T-MAC adaptive Timeout

**G-MAC**

One of the energy efficient MAC protocol is G-MAC which can do transmissions within a cluster. The Figure-3 shows the structure of the G-MAC and it is divided into two periods such as collection period and contention period. At the time of collection period all the nodes within a cluster sends a FRTS-[Future RTS] message to the gateway node. At the time of contention period all the nodes from all the clusters exchange their message in the form of RTS/CTS/DATA/ACK. End of the contention period, the CH or the gateway node sends a GTIM message to all the nodes in the cluster for cluster synchronization, then all the nodes can exchange the data. All the nodes can interchange their data in their contention period. According to the present resource level and volunteer behavior the gateway node is selected in a periodic manner. G-MAC is having capability to eliminate the GTIM message overhears. G-MAC is slow but can improve the network lifetime more than 3 times than T-MAC [12].

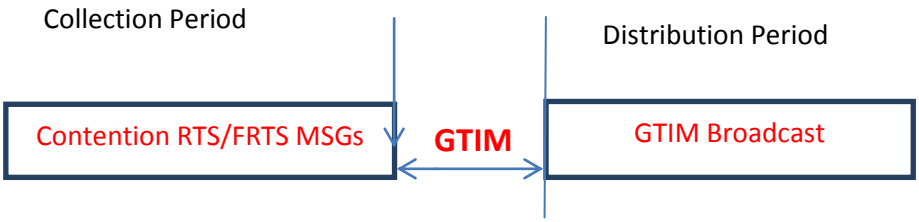


**Figure-3:** G-MAC Frame Structure

**Proposed MAC-PHY**

The MAC protocols explained above shows the quality of service in terms of energy efficiency WSN and all are belongs to current version systems released under TinyOS.

In the MAC layer, unnecessary collisions should be avoided because retransmissions require additional power consumption and further increase packet delay. MAC protocols based on RTS/CTS, such as [14], have been proposed to alleviate these problems. However, as the number of mobile terminals increases, more energy will be consumed for channel contention and network performance will degrade quickly. Additionally, as explained in the following, RTS/CTS-based protocols do not completely solve the hidden terminal and exposed terminal problems.

By utilizing the RTS/CTS mechanism and common MAC-PHY layer advancements the data transmission is scheduled, slotted and executed. According to the signal strength the carrier sensing unit carries the data. Network allocation vector is used for framing the data packet followed by IEEE 802.11 standard the data will be transmitted from one system to other system. Since it follows a stipulated time interval for data transmission the latency of the network is reduced as much as possible. In this paper MAC-PHY layers are configured as cooperative and utilized scheduling algorithm with priority queue with weight.

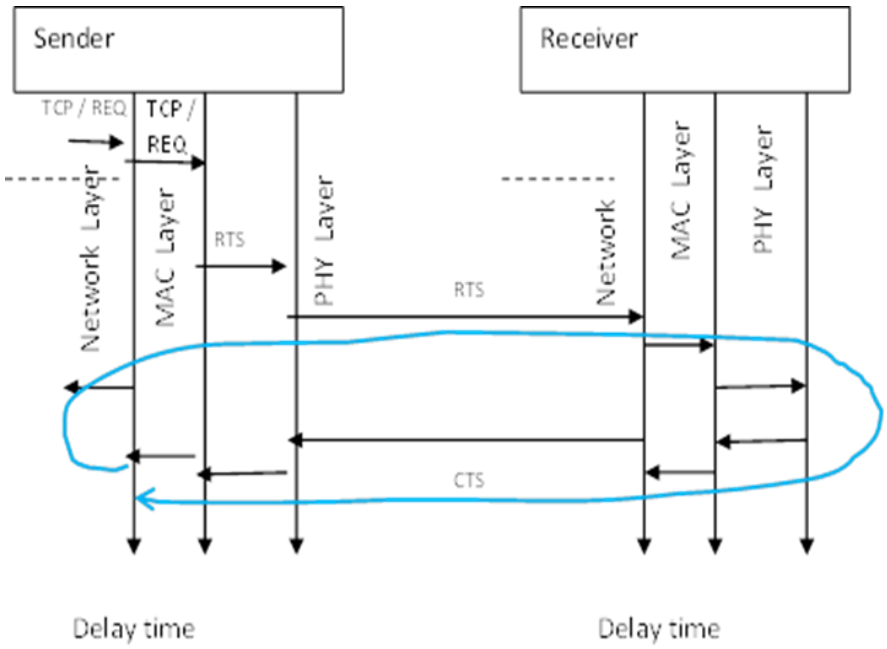


**Figure-4:** RTS/CTS Functional Architecture

After a round of REQ-RES-ACK process a route is discovered using the available AODV routing protocol with configured MAC and PHY layers. This RTS-CTS mechanism eliminates the time delay, avoid congestion and clear the traffic by scheduling the packets, slot allocation for more number of users and assign priority for data queue. After successful data transmission or one round completion the entire buffer, queue, registers and memory used of the network process are stored in trace and cleared by calling the garbage collector in the existing OS. It leads to overriding the existing content and avoid time taken in the entire process.

## V SIMULATION RESULTS AND DISCUSSION

The parameters used in our simulation are shown in Table-2. The simulation flow follows the MAC and PHY layer based configuration. In the simulation, node deployment, the data packet transmission from

source node to destination route all information are controlled by MAC and PHY layer for scheduling and allocating slot for different number of users. Also it is assumed that this MAC-PHY layer configuration is applied in to the existing AODV routing protocol to increase the efficiency of AODV routing protocol for WSN.

**Table-2:** Simulation Parameter Settings in NS2

| | |
|---|---|
| Area | 1200 x 1200 |
| Nodes | 10, 20, 30, 40, 50, 100 |
| Packet Size | 50 |
| Transmission Protocol | AODV |
| Application Traffic | CBR – TCP - UDP |
| Simulation Time | 50 ms |
| Queue Type | Drop-Tail |
| Propagation Model | Two Ray Ground |
| Antenna Model | Omni Antenna |
| Routing Protocol | AODV |
| Initial Energy | 100 |

The entire functionality of the proposed approach MAC-PHY layer configuration are configured and programmed in Network Simualtor-2 software and experimented. In order to verify the performance the number of rounds and the number of nodes deployed in the network are changed from 100 to 500 nodes in round 1 to 5 respectively.

The efficiency and the performance of the proposed approach are verified by computing the energy consumption level, throughput, and delay and packet delivery ratio. The performance can be verified by comparing the results with different number of nodes and with existing TSS [14] algorithm. In terms of energy consumption, each node needs some amount of energy for various kinds of network operations. Even it needs some energy for alive in the network. In this simulation the energy consumption is computed in each round for different number of nodes and the obtained result is shown in Figure-5. From this figure, it is clear and noticed that the proposed MAC-PHY approach obtained less energy consumption than the existing TSS approach because of MAC layer based slot allocation and scheduling operations. PHY layer directly controls the data packet without collision and it increases the energy level of a node in the network. Since, it is understood that the proposed MAC-PHY layer approach is better for increasing the QoS in terms of energy in WSN.

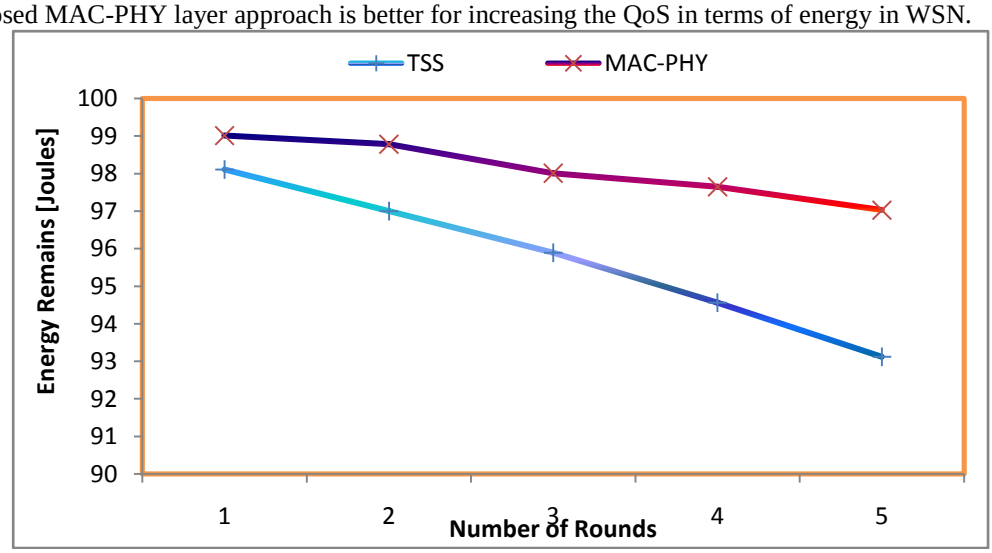


**Figure-5:** Comparison of Energy Consumption

In terms of throughput, the total number data packets transmited within a stipualted interval of time or within a round of network operation is calcualted and verified. The obtained results is shown in Figure-6. When the number of nodes increased the amount of throughput is also increased. Fromt this figure it is noticed that the propsoed MAC-PHY obtained more throughput than the existing TSS approach. It is calculated in each round of operation and given. In each round the MAC-PHY approach is proved as a better approach than TSS. In all the rounds the amount of througput obtained by both aprpaoches are gradually increased according to the number of nodes increased.

In terms of delay the time taken by the proposed approach and the existing approaches are calculated in the simulation and the obtained results are shown in Figure-7. From this figure it is very clear and noticed that

the proposed MAC-PHY approach takes lesser time than the existing TSS approach. Also it is noticed that the delay increases according to more amount of network operations is also increases. In each round according the number of nodes is increased gradually whereas the delay is also increased. When number of nodes increased is automatically increases the amount of network operations. From figure-7, MAC-PHY approach proved that it is efficient in terms of delay than the TSS.

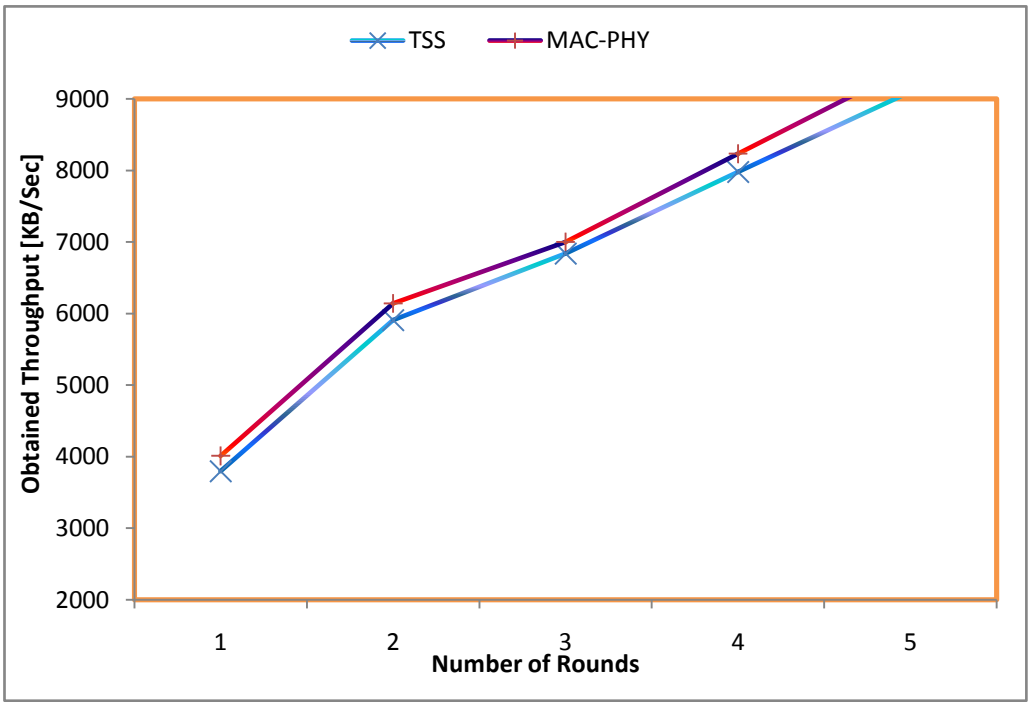


**Figure-6:**Number of Rounds versus Throughput

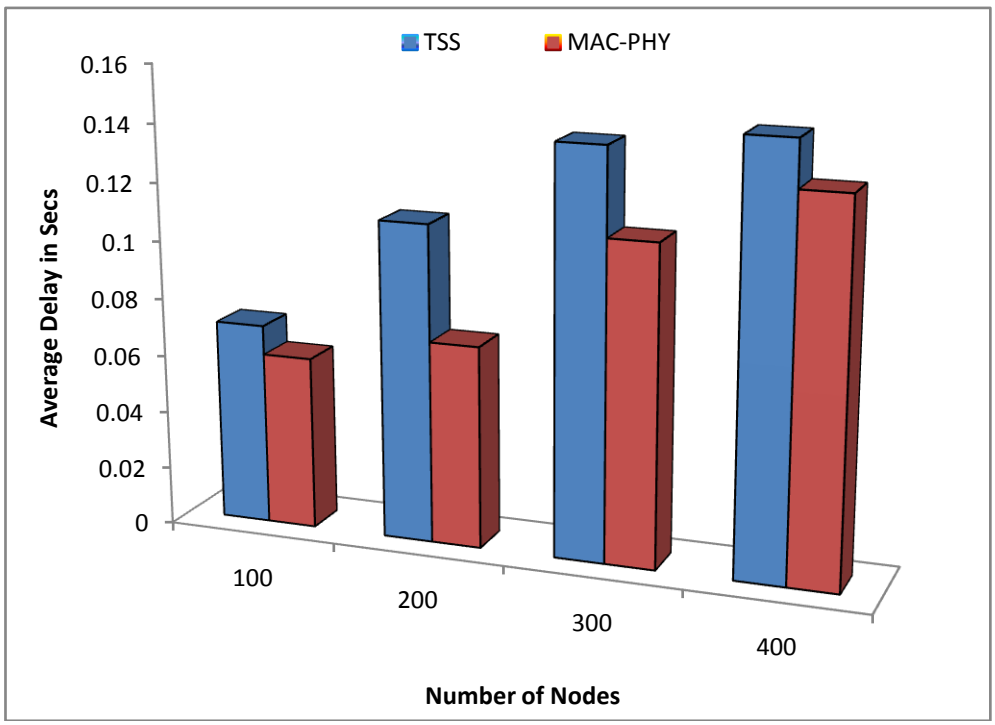


**Figure-7:**Number of Node versus Delay

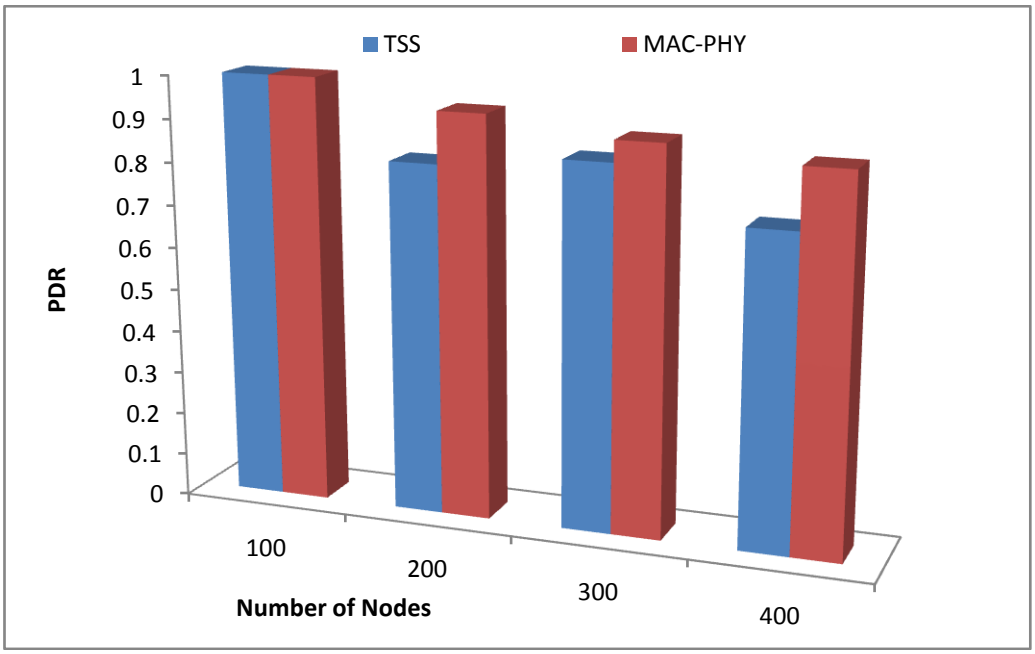


**Figure-8:** Network Size vs. PDR

Similarly the packet delivery ratio is calculated and shown in Figure-8. The packet delivery ratio is depends on the throughput and number of nodes. But the PDR differs from throughput whereas it defines the number of data packets successfully received at the destination side. When number of node increases the PDR decreases due to overload, overhear and more number of paths. In this paper the obtained PDR is gradually and slowly decreases due to data packets. From the experiment it is clear that the obtained PDR using MAC-PHY approach is higher than the TSS approach. Hence it is decided that the proposed MAC-PHY approach is better and efficient than the TSS.

From the above Figure-5 to Figure-8 it is proved and concluded that the proposed MAC-PHY layer based approach is better in term of QoS in AODV routing protocol.

## VI CONCLUSION

The main objective of this paper is to increase the ability of ADOV routing protocol in terms of Quality of Service parameters. To do this, here it is focused on configuring the MAC-PHY layer as cooperative layers to save the energy by controlling collision and other data jamming in a WSN. Both layers are concentrating on different services like scheduling, slot allocation, congestion controlling, and priority assignment and concentrating on data packets. This layer based approach is simulated and experimented for verifying the obtained results. From the results it is clear and concluded that the proposed approach is better than the existing approach in terms of quality of service.

## REFERENCES

[1]. J. Hill and D. Culler. A wireless embedded sensor architecture for system-level optimization. Technical report, University of California, Berkeley, 2001.

[2]. Berkeley MICA mote. http://webs.cs.berkeley.edu/tos/hardware/hardware.html, 2003.

[3]. J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next century challenges: Mobile networking for “smart dust”. In *International Conference on Mobile Computing and Networking (MOBICOM)*, pages 271–278, 1999.

[4]. J. M. Kahn, R. H. Katz, and K. S. J. Pister. Emerging challenges: Mobile networking for “smart dust”. *Journal of Communications and Networks*, 2(3):188–196, September 2000.

[5]. B. Warneke, M. Last, B. Liebowitz, and K. S. J. Pister. Smart dust: Communicating with a cubic-millimeter computer. *Computer*, 34(1):44–51, 2001.

[6]. S. Hollar. COTS Dust. Master’s thesis, University of California, Berkeley, December 2000.

[7]. C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *First IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003.

[8]. Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, April 2003.

[9]. K Thomas and S Büettrich. "Wireless mesh networking." posted at Wireless DevCenter on Jan 22 (2004), pp. 1-9.
[10]. Z Yanchao, W Liu, and WLou. "Anonymous communications in mobile ad hoc networks." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 3. IEEE, (2005).
[11]. Z Yanchao, W Liu, and Wenjing Lou. "Anonymous communications in mobile ad hoc networks." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 3. IEEE, (2005).
[12]. T. Zheng, S. Radhakrishnan, and V. Sarangan, "PMAC: An adaptive energy efficient MAC protocol for Wireless Sensor Networks," IEEE *IPDPS*, 2004.
[13]. Jaejoon Cho, Sungho Kim, Heungwoo Nam, SunshinAn, "An Energy-Efficient Mechanism using CLMAC Protocol for Wireless Sensor Networks", Networking and Services – IEEE conference – 2007.
[14]. Muthumayil K, Manikandan S, Rajamani V, "TSS: A Secure Clustered Energy Efficient Algorithm for Wireless Sensor Networks", International Journal of Advanced Engineering Technology, VII/Issue I/Jan.-March.,2016/427-433.