Energy Efficient Routing by Taking Willing Status of Node in WSN

[1]Varshitha V, [2]Mrs.Renuka K H

[1]M.Tech, Dept. of CSE, Visvesvaraya Institute of Advance Technology, Bengaluru, India.
[2]Asst. Professor M.Tech, Dept. of MCA, Visvesvaraya Institute of Advance Technology, Bengaluru, India.

***Abstract*: Wireless sensor network is a network used to communicate various wireless sensors through radio link. In WSN the efficient routing willing status (WSN) is used as a proactive routing protocol. The Hello Messages are used in ERWS. The ERWS is extended to the Energy Efficient-ERWS (EE-ERWS). The ERWS is prone to various attacks. The severe attack is the Sleep Deprivation Torture attack. In this paper we are mainly concentrated on the Sleep Deprivation Torture attack. The low energy node is targeted by the Sleep Deprivation Torture attack. The low energy node is taken as the victim by the attacker and moves permanently to the sleep mode. All energy of the node is exhausted by the sleep deprivation attack. These type of attack is also possible at the routing level. The willing property of each nodes is known by the broadcasting Hello messages to all the nodes. So here we are proposing Intrusion Detection System (IDS). The IDS is used to detect the Sleep Deprivation Torture attack. The Network Simulator (NS 2) is used for the simulation for the performance and the existing is compared for the performance.**

***Keywords:* Wireless Sensor Network (WSN); Efficient Routing Willing Status (ERWS); Energy Efficient-ERWS (EE-ERWS); Sleep Deprivation Torture Attack.**

I. INTRODUCTION

A number of cellular sensors called as the wireless sensors are communicated with a central base station through a connection of radio link which is generally called as the wireless sensor networks. Sensor field consists of a large number of tiny sensor detector nodes in WSN [1, 2]. The data can directly transmit to the gateway through detecting using sensor nodes in wireless sensor networks. The tiny sensor nodes are connected through base station. There are two types of routing [3] protocols in WSN. Namely the reactive routing protocol and the proactive routing protocol. The reactive routing protocol is worked by finding the path to transmit the data only if there is transmission of the data. The proactive routing protocol is worked by in advance finding the paths to each and every source and destination. The proactive routing protocol is more advantageous compared to the reactive routing protocol, in advance having all the paths to every nodes. So in the ERWS we are using a proactive routing protocol. The most prominently used in the ERWS is the proactive routing protocol.

The ERWS is enhanced to the Energy Efficient ERWS (EE-ERWS) [5]. In the EE-ERWS the MPR (Multi Point Relay) nodes are used. Each nodes show their willingness property. Based on the willing property of each node the MPR nodes are selected. The willingness property shows the efficiency of the node that is the battery life time of the node. Based on this property the willingness of the node is recognized. Then the node is considered as the MPR node. The MPR node which helps to reduce the flooding of packets, and the network congestion is reduced.

But the unauthorized access is not known by the EE-ERWS. The traditional ERWS is not used other than that the EE-ERWS method is used for the attacks. The EE-ERWS is used to overcome the attacks compared to the traditional ERWS. At the time of routing the Sleep Deprivation Torture attack [4] is also possible. The adversary selects the victim node, and all the energy is exhausted. The node which has the low battery power is selected by the adversary node. After removing all the energy the node goes to permanent sleep mode. In which the node has no energy due to the attack of the adversary node. The attacker node when interacted by the node the lifetime of the node will be linearly reduced. The energy of the node can be drained by the victim in various ways. The attacker gives more tasks to the victim node to drain all its energy. Many researches researched based on the sleep deprivation torture attack, which resulted in many solutions. Among all the solutions one of it is the MAC protocol. MAC protocol [5] shows the single point of failure. The MAC protocol analysis that various types of denial of sleep is possible. The solution which is described by the MAC protocol is not efficient due to the increase of network overhead. One of the solution was also introduced by the Chen C. et al. The fake schedule switch solution was introduced, but it also have a drawback that is the complex installation.

The MAC layer shows that at the level of routing there may be an occurrence of Sleep Deprivation Torture attack. Here in order to avoid the Sleep Deprivation Torture attack we use the Intrusion Detection attack (IDS). There are three types of the IDS [6] namely specification based, anomaly based and signature based. The anomaly based and signature based IDS are the most popular IDS, but there are not used frequently because they generate more false alarms. The specification based is one of the most popularly used IDS because it detects the malicious attacks, and also the problems are avoided.

II. EFFICIENT ROUTING WILLING STATUS

A. *Summary of ERWS:*

ERWS is one of the datagram protocol. The ERWS is specially designed for the mobile ad-hoc networks which uses the table driven link state routing protocol. ERWS is proactive protocol. While broadcasting the messages the overhead occurs by flooding of control packets. The routes are available when needed immediately, using the link state algorithm. In order to avoid flooding we use a multipoint relay (MPR) nodes.

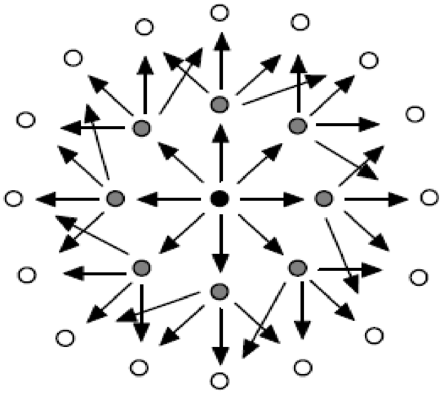


Fig.1: General Transmission Consequence

The MPR nodes overcome flooding. The high energy nodes are made as the MPR nodes. These multi point relay nodes are made to broadcast messages. The 1-hop neighbor nodes are used for the MPR selection. These MPR nodes forward the messages to the 2-hop neighbors of the particular node. By selecting the MPR nodes, the transmission will be easily made to the 2-hop neighbor nodes.

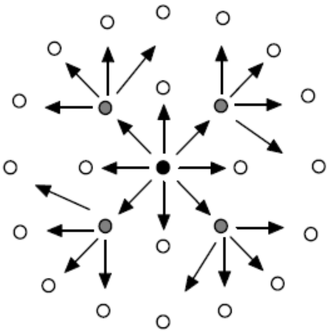


Fig.2: Transmission by MPR Selection

The MPR selection is done in the node set of 1-hop neighbor nodes. The overhead and flooding of control packets is increased due to forwarding messages to all the nodes. So the MPR nodes are selected due to the avoidance of the flooding of control packets. Due to the MPR selection mechanism the network transmission has an advantage of more efficiency. It is more scalable in the usage of the MPR mechanism. Fig 1 shows the general transmission consequence. All the 1-hop neighbor nodes receives the control packets and forwards it.

By the participation of all the nodes in 1-hop neighbor, the duplicate data packets are generated. In order to avoid the duplicate data packets we are using MPR selection of nodes. The general transmission consequence shows the drawback of the traffic overhead. In order to overcome the drawback the MPR forwarding is done. The Fig 2 shows the Transmission by MPR selection. Due to this the traffic overhead is reduced.

B. Message Broadcasting in ERWS:

The ERWS is one which uses the 2 types of control messages. The control messages used by the ERWS is the hello messages and the Topology Control (TC) messages. First the node sendsthe hello messages to all the nodes.

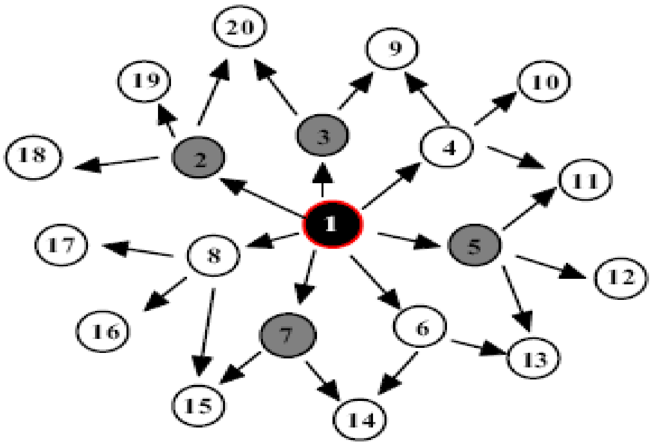


Fig.3: Attack Framework

By sending the hello messages to all the nodes in ERWS, the willing status of each node is reveled. Then by knowing the willing status, the MPR selection is done. Due to the MPR selection, it will be easy to route the packets to the nodes. There are different attributes set for each node. The attributes are like WILL_DEFAULT, WILL_NEVER, and WILL-ALLWAYS. The WILL_DEFAULT attribute indicates the default value of the node.

The neighbor nodes never selects the node as MPR node, when the node has the attribute of WILL_NEVER. The WILL-ALWAYS attribute shows that it is ready for transmission, with willing status always. Now let us consider the Fig 3 as the example. The 1-hop neighbor nodes are the N2, N3, N4, N5, N6, N7, and N8. Now all the 1-hop neighbor nodes receives the hello messages. The 2-hop neighbor nodes are the N9, N10, N11, N12, N13, N14, N15, N16, N17, N18, N19, and N20. After receiving the hello messages, the 1-hop neighbor shows the willing status of each node. Instead of sending packets from all the 1-hop neighbor to the 2-hop neighbor, we use the MPR selection. Because in order to avoid flooding we use the MPR selection. The WILL-ALWAYS nodes are selected as the MPR nodes, the packets are sent to the 2-hop neighbor.

Each MPR nodes contains an MPR selector set. The MPR selector set should be known to the nodes. The MPR nodes should sends the TC messages to all the nodes in the network. The MPR selector set is also sent to all the nodes. By sending TC messages from the MPR node, it comes to know the originator MPR node. When the MPR selector set is empty, then no TC messages will be sent to the node. For example consider Fig. 3 in which the node 1 sends its MPR set through N2. Because N2 is the subset of N1.

III. EE-ERWS

Here the energy is the most essential part in the WSN. The sensor nodes cannot store more power. They do not provide backup, especially in the critical situation, due to its size. The sensor nodes are tiny in size. As the energy is needed as the most prominent one in the WSN. Due to this the route failures are also possible in the networks. So in order to avoid this we are using energy efficiency. This energy efficiency does not only provides us the power. The energy efficiency also measures the performance of the network. It checks the performance through the life-time of the network. Here the energy of each node is displayed.

The willing status is seen by the remaining energy left out in the node. That is the energy used and the energy remaining are calculated. By using these measures the current energy of the node is calculated. A node cannot have some battery power all the time. It may be changing. If the power supply is done to a node simultaneously then, the node can have a good backup, then it can transmit more packets. In this condition the node attribute will be WILL_ALWAYS. If the other node has not connected to the simultaneous power supply and if it does not have a backup. Also no power in the node to transfer packets, then the willingness property will be WILL_NEVER. If the power in the node frequently changes to low, then the willingness property will be WILL_LOW.

There are many researches going on to provide good power to the nodes, in order to provide best communication in WSN. The status of the willingness of the nodes can also be represented by numbers. If the states of a node would be WILL_NEVER, then it is set to integer 0. Likewise the WILL_LOW to 1, WILL_DEFAULT to 3, and WILL_HIGH to 6 and finally WILL_ALWAYS to 7.

C. Attack Scenario:

The ERWS is expanded to the EE_ERWS. The node should select the high energy node to transfer the packets. After sending the hello messages, each node shows its attributes that is the willing status. Some may be willing status high and some may be low. To send a packet the node should select a willing status high node. So that through the high energy, the more packets arte sent simultaneously. This is the procedure of the selection of node in the energy efficient ERWS. But in the case of the attacker he does totally a different process. To elaborate the attack scenario, let us consider fig. 3. Consider that node N1 contains 1-hop and 2-hop neighbor nodes. The 1-hop neighbor nodes of N1 are {N2, N3, N4, N5, N6, N7, N8} and the 2-hop neighbor nodes are the {N9, N10, N11, N12, N13, N14, N15, N16, N17, N18, N19, N20}. Now first the hello messages are transferred to all the nodes from node N1. Then the attribute of each node is known, that is the willingness property of each node is reveled and exchanged with the node. Now in the process of ERWS the node has to select the high energy node. As shown in the fig. 3 consider N3, N5, N7 set of nodes are WILL_LOW. Then N4, N6, N8 are showing the willing status WILL_HIGH. Then the WILL_ALWAYS is shown by N2. But the attacker selects only the willing status low nodes. Then these willing status low nodes are converted to MPR. The attacker uses only the WILL_LOW nodes. The attacker's main aim is to concentrate on the low energy nodes. Then moving the low energy nodes into the permanent sleep mode. All the energy of the node is removed and wasted by giving unwanted work to the node.

IV. PROPOSED SOLUTION IDS

Here we use sensor monitors, to detect the attacks. The sensor monitor is one which is clustered with many number of sensor nodes. Small sensor nodes are grouped from a sensor monitor. In a group of nodes, some set of SMs are used. These SMs are used to detect the attacks. They try to detect the attacks by having communication with the other sensor monitors.

D. Working of IDS:

Here working of the IDS algorithm is described. In order to detect the intruder attacks. The hello messages are sent to all the nodes. The hello messages are never exchanged by the neighbor nodes. After transferring the hello messages the hello table and TC tables are updated.

Algorithm IDS

1. Energy Initialization.
2. HELLO Packet Transmission.
3. Updating HELLO Table and TC Table.
4. 1-hop nodes Energy level displayed.
5. MPR Selection.

6. If Low MPR Selection

a. Low Energy Node Selected

b. Message sent to SM

c. SM Identifying Malicious Node

d. Malicious Node moved to Block List

e. Data Transmission from WILL_YES Node.

7. If High MPR selection

a. High Energy node Selected

b. Data Transmission

8. END

After updating the tables, the willing status of the 1-hop neighbor is displayed. These all high energy nodes are said as the MPR nodes. For a good packet transmission the high energy nodes should be taken. But a node tries to transfer the packets to the low energy nodes. Then these low energy nodes sends message to the SM. The SM receives a message of selection of low energy node for packet transmission. Then the SM doubts for choosing the low energy node. One SM communicates with the other SM. The SM comes to know that it is the attacker. The attacker's main intention is to choose a low energy node. By choosing the low energy node, the attacker moves the node to permanent sleep mode. So the SM after knowing the attacker, stops the node for data transmission. Then the node is moved to the block list. Now the data transmission takes place through willing status yes nodes.

*E. **Working Of SM:***

Here we use 4 sensor monitors. The sensor monitors used namely are the SM1, SM2, SM3, and SM4. Each sensor monitor monitors the number of nodes within its range. The description of sensor monitors are as shown in the fig. 4. The nodes within the range of sensor monitors are monitored by a particular sensor monitor. The 1-hop neighbor nodes of N1 are the N1, N2, N3, N4, N5, N5, N6, N7, and N8. The 2-hop neighbor nodes are the N9, N10, N11, N12, N13, N14, N15, N16, N17, N18, N19 and N20. Now the hello packets are sent to the nodes and willing status of the node is known. The willing status are updated in the hello table. The sensor monitor can access the hello table to see which node has been selected for data transmission and also can know the willing status of each nodes.

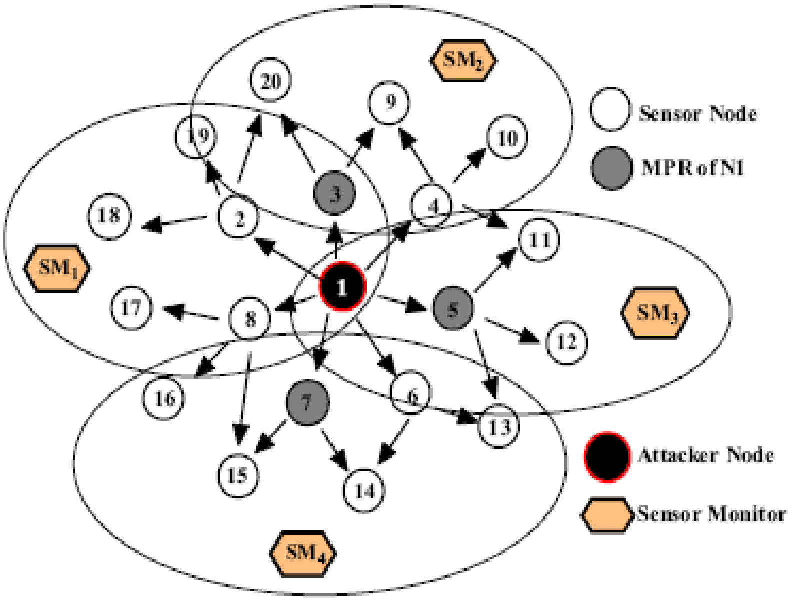
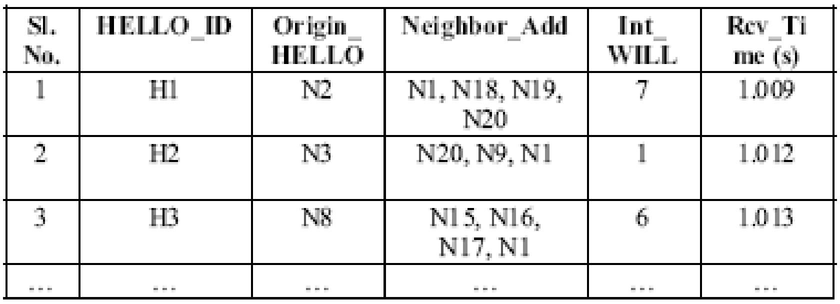


Fig.4: Description of Sensor Monitors

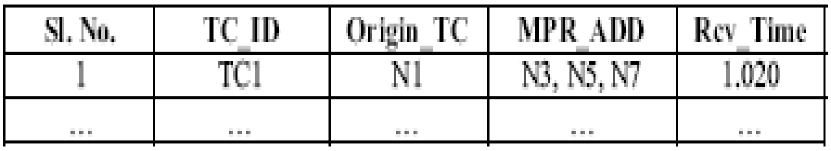
The willing status in terms of integers are stored in the hello table. The values of node N2, N3, N4, N5, N6, N7, and N8 are 7, 1, 6, 1, 6, 1, and 6 respectively. Now node N1 for data transmission selects the node N2. The SM1 checks that node N1 has selected node N3 for transmission. Then SM1 also checks the willing status of N3 in hello table. The SM1 comes to know that N1 has selected N3, N5, and N7 for transmission and chosen it as the MPR nodes. The SM1 doubts that the node N1 might be the malicious node. Then the node N1 is added to the malicious list by changing the source IP address. The node N3 is connected to 2-hop neighbor with the N20 and N9. The node N2 (WILL_ALWAYS) is also connected to the node N20. The SM1 and SM2 is communicated through the node N2 (WILL_ALWAYS).

TABLE.I: HELLO TABLE



Sl. No.	HELLO_ID	Origin_ HELLO	Neighbor_Add	Int_ WILL	Rcv_Ti me (s)
1	H1	N2	N1, N18, N19, N20	7	1.009
2	H2	N3	N20, N9, N1	1	1.012
3	H3	N8	N15, N16, N17, N1	6	1.013
...	...	...	...	...	...

TABLE.II: TOPOLOGY CONTROL TABLE



Sl. No.	TC_ID	Origin_TC	MPR_ADD	Rcv_Time
1	TC1	N1	N3, N5, N7	1.020
...	...	...	...	...

It also communicates SM3 through the node N4. In which the node N4 has the willing status WILL_HIGH. By communicating with all the sensor monitor the node N1 is moved to the blocked list. Then the packet transmission made from node N1 is discarded and stopped. So by this the node N1 is stopped for doing any transmissions. Table I shows the hello table. Table II shows the topology control table. Each time the values of the nodes are changed. The tables are updated frequently. The SM checks the tables for the willing status of each nodes.

V. RESULTS

The sleep deprivation torture attack has overcome and detected. The IDS algorithm helps to detect the attacks of the sleep deprivation torture attack. The performance of EE-ERWS is increased. It is increased and measured through a specific parameters. The parameters in order to measure the performance used are the throughput, packet delivery ratio [15], End to End delay [15], average life time. Here for the simulation we use NS-2 simulator. We are using NS-2.34 version for the simulation. Linux is used as the operating system, which is flexible in the network simulation. The number of nodes used here is 10-100. The total time taken for the simulation process is the 500sec. The wireless channel communication is used. The hello packets are transferred within 2sec and the time taken for TC interval is the 5sec.

The throughput graph is as shown in the Fig. 5. It shows the comparison between the four parameters. The first parameter is EE-ERWS under the sleep deprivation torture attack. The second parameter is better than the first parameter which is ERWS. The third parameter which gives better throughput than using IDS. The good throughput is given by the EE-ERWS.

Packet delivery ratio is represented in Fig. 6. The same four parameters is used to measure the packet delivery ratio. The EE-ERWS helps to get good packet delivery ratio.

The graph of End to End delay is as shown in Fig.7. When attacked by the sleep deprivation torture attack there is a long delay. The delay of packets is reduced when used with EE-ERWS.

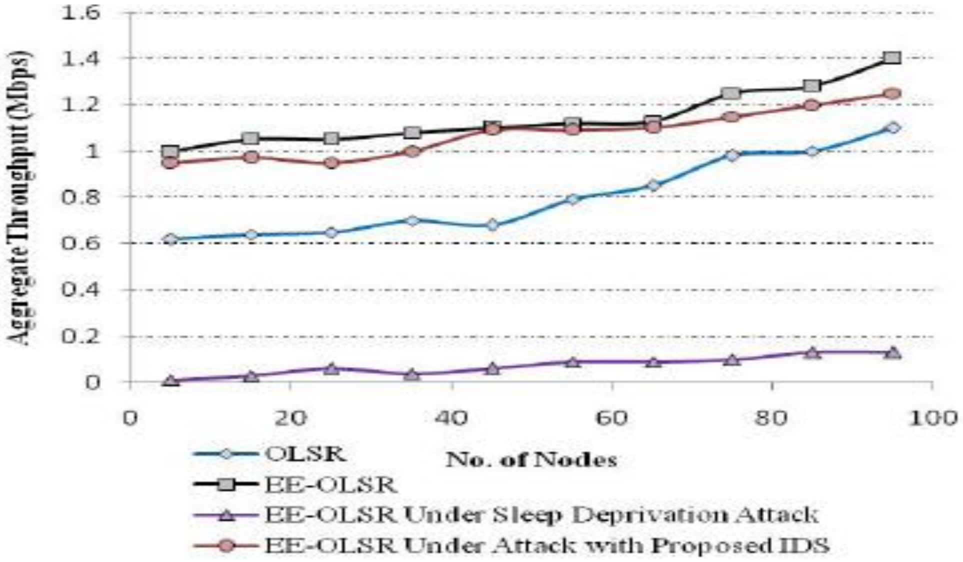


Fig.5: Throughput

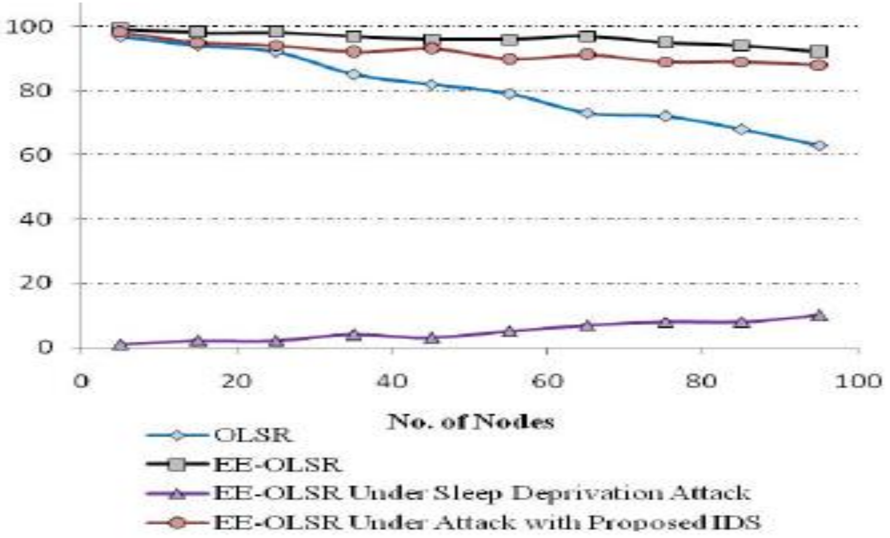


Fig.6: Packet Delivery Ratio

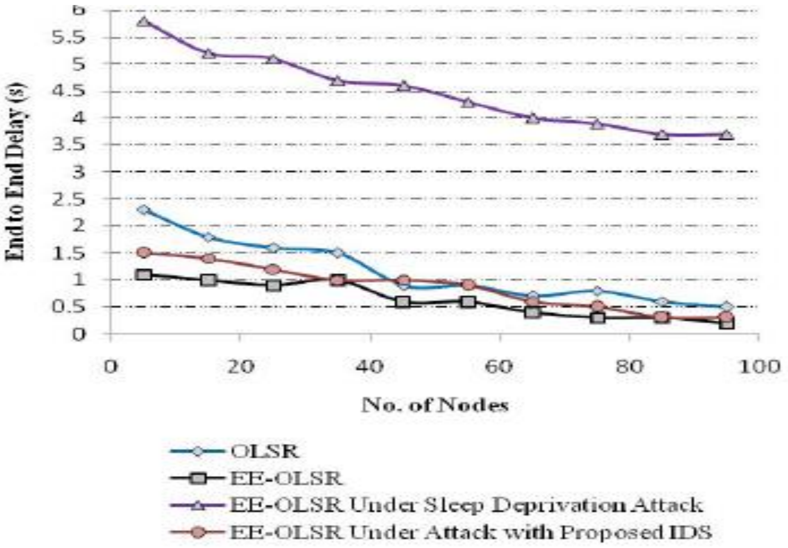


Fig.7: End to End Delay

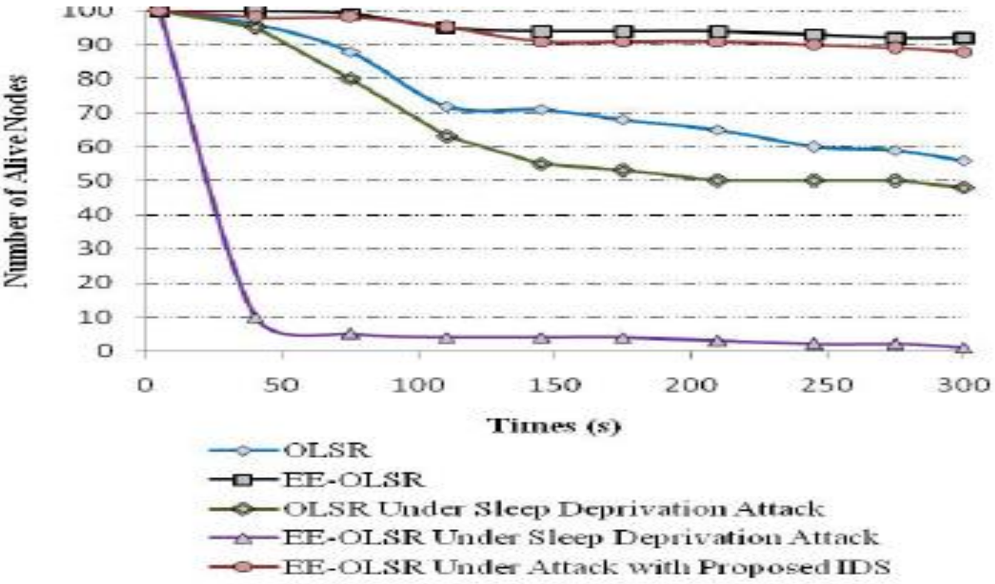


Fig.8: End to End Delay

The average lifetime of the packets is as shown in the Fig. 8. Average life time shows us the lifetime of each and every node.

VI. CONCLUSION

In WSN the first beneficence is the energy efficient ERWS. The MPR election rule is a different energy plan. The throughput, packet transmission, point-to-point delay, general nodes life span in EE-ERWS outperforms historic ERWS. In EE-ERWS the sleep deprivation attack is possible when trustworthiness of packets is not checked in EE-ERWS. The sleep deprivation attack is blocked by the EE-ERWS in which the network is divided and life span of the node is miniaturized.

The ERWS protocol is scheduled for disclosure workings especially considering sleep deprivation attack. With rate regarding quantity, PDR, end-to-end delay and general node life span, the issue about the intrusion can be nullified through huge extension which is illustrated in the experimental results of the IDS.

REFERENCES

[1] Naznin, Mahmuda, “Wireless Sensor Network: Coverage, Scheduling and Optimization”, 1st Edition, VDM Verlag, 2009.I.S.

[2] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci “A Survey on Sensor Networks”, IEEE Communications Magazine, vol. 40, no.8, pp. 102–114, August 2002.

[3] Al-Karaki, J.N.; and Kamal, A.E., "Routing techniques in wireless sensor networks: a survey”, Wireless Communications, IEEE , vol.11, no.6, pp. 6-28, December 2004.Y.

[4] F. Stajano, “Security for Ubiquitous Computing”, John Wiley & Sons, Ltd., New York, June 6–9, 2004, Hyatt Harborside, Boston, MA, USA. 2002.

[5] Michael Brownfield, Yatharth Gupta, Mem and Nathaniel Davis IV (2005):” Wireless Sensor Network Denial of sleep attack” published by IEEE 2005.

[6] Chaitali Biswas Dutta, Utpal Biswas, “Specification Based IDS for Power Enhancement Related Vulnerabilities in AODV”, The Fifth International Conference on Network Security & Applications (CNSA 2012), Springer, pp. 209-218, July. 2012.