ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2014.0146

SPY AGENT BASED SECURE DATA AGGREGATION IN WSN

T. Lathies Bhasker[1] and G. Arul Jagan[2]
[1]*Department of Computer Science and Engineering, Manonmaniam Sundaranar University, India*
E-mail: lathiesbhasker@gmail.com
[2]*Department of Computer Science and Applications, Anna University Chennai, India*
E-mail: aruljagang@gmail.com

Abstract

Wireless sensor network consist lot of sensor devices which are activated by using the battery power. These sensor devices are mostly used in hostile environment, military applications etc. So in this type of environment it is highly difficult to collect and transmit the data to the Sink without any data lost. In this paper we proposed SPY Agent based secure data aggregation scheme. Here one SPY Agent moves around the network and monitors the aggregator nodes i.e, the Cluster Heads for secure data collection. In the Simulation section we have analyzed our proposed architecture for both proactive and reactive protocols.

Keywords:
Wireless Sensor Network (WSN), SPY Agent, Cluster Head (CH), Data Aggregation, Residual Energy

1. INTRODUCTION

1.1 WIRELESS SENSOR NETWORK

A wireless sensor network is a group of nodes which forms a cooperative network. Each node has processing capability and different types of memory (program, data and flash memories), have a RF transceiver (usually with a single omni-directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion.

A wireless sensor network (WSN) contains a Sink (Base Station) that can able to communicate will all the nodes in the network through the radio link. The data (message) can be collected from the sensor nodes then compressed and transmitted to the Sink directly or using the intermediate sensor nodes or gateway nodes [1].

These sensor networks combine the data sensing, data computation and communicate between the data into a single small device. These small sensor nodes have the ability to sense the data, process the data and communication between them. These sensors are small in size so the device has limitations in data storage, battery power and network bandwidth [2] Because of these drawbacks the wireless sensor network differs from normal communication networks in several ways. These limitations requires specialized optimization techniques [3]

1.2 DATA AGGREGATION IN SENSOR NETWORK

Data aggregation is one of the basic data processing methods in distributed environment for saving the energy and minimizing the medium access layer contention in sensor network. The important pattern for routing is presented by data aggregation in wireless sensor network. The main concept of data aggregation is collecting the data from different data sources and re-route the data packets to the sink. In data aggregation scheme the data redundancy and optimal energy usage can be achieved. For energy preservation and achieve longer network life time, it is necessary for the network to maintain high incidence of the in-network data aggregation [4].

1.3 DATA AGGREGATION IN CLUSTER BASED NETWORK

Sensor networks are energy constraint network and large in size. Due to the network size it is inefficient for the sensors to directly transmit the data to the sink. But in the case of Cluster-based approach the entire network is divided into many small groups and each small group selects one Cluster Head among the group members. During the data aggregation process the data are collected by the Cluster Head from the cluster members then this collected data will be sent to the Sink. Because of the direct communication between the cluster heads and the sink reduce more energy consumption and increase the network life time. [5] In recent years lot of cluster based data aggregation protocols such as LEACH, E-LEACH, TL-LEACH, M-LEACH, etc. were proposed [6].

Advantage: The data aggregation process uses to enhance the robustness and increase the data accuracy. With the help of data aggregation the data redundancy can be avoided, the network traffic and energy conservation can be reduced. The data fusion method is a very efficient method for eliminating data redundancy.

Disadvantage: In this data aggregation process the aggregator or the cluster head do the data fusion suppose the aggregator node is attacked by the attacker or compromised, then the sink can't get the accurate data. Another disadvantage is existing systems are several copies of the aggregate result may be sent to the receiver (Base Station or Sink) by uncompromised nodes. It increase the power consumed at these nodes [7].

In this Paper we have proposed a SPY agent based secure data aggregation, in this proposed architecture one spy node moves around the entire network and collects the information about the aggregator nodes and updates it's status on the table, based on this updated information the SPY Agent isolates the malicious nodes and the section two explains about the existing methodologies section three explains about the proposed architecture in detail section four shows the simulation result of the proposed methodology and finally section five gives about the conclusion and future enhancement work.

2. RELATED WORK

Sung-Hwa Hong et al [8] have proposed a simple cluster-based data aggregation and routing algorithm (SCAR) that

decreases the incurred overhead during the selection of cluster heads in wireless sensor networks.

Preethi Y. R. et al [9] have proposed a Cluster Based Data Routing for In-Network Aggregation that has some key concepts such as a reduced number of messages for setting up a routing tree, maximized number of overlapping routes, high aggregation rate, and reliable data aggregation and transmission.

Hiren Thakkar et al [10] have proposed a modification in Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. Their modified protocol is considering residual energy as a criterion for a node to be a cluster head during Cluster head selection and Clusters setup phase. They also have proposed multi level data aggregation among Cluster heads to reduce the packet size which in turn reduces the transmission and receiving energy for a node. They also proposed multi-hop transmission of aggregated data. The data aggregated by Cluster heads will not be transmitted to base station directly but through multi-hop transmission by Cluster heads which are nearer to base station, which in turn reduces the transmission distance and so as energy consumption of nodes. Their main focus to achieve energy efficiency is by reducing packet size by multi level data-aggregation among Cluster heads and by proper selection of nodes as Cluster heads by considering maximum residual energy of a node as a constraint.

Nan Guofang et al [11] have proposed an algorithm to select a cluster leader that will perform data aggregation in a partially connected sensor network. The algorithm reduces the traffic flow inside the network by adaptively selecting the shortest route for packet routing to the cluster leader. The algorithm can find a cluster leader in a robust way by using fewer packets than previous work, thus reducing the energy consumption of the sensor network.

Amrutha Mohanan. K, et al [12] have proposed an encryption and signature techniques are used and also the base station can recover all sensing data even these data has been aggregated. The base station can perform any aggregation function on them. Without compromising any nodes an attacker can interrupt the network system. The hierarchical trust management protocol detects the malicious behavior of the nodes. It is based on four trust components intimacy, honesty, energy, unselfishness of the nodes. It maintains two levels of trust SN-level trust and CH-level trust.

Soubhagya Ranjan Behera et al [13] have proposed a cluster based routing algorithm to ensure high reliability such that the entire network becomes fault tolerant by the introduction of multi cluster heads. Their simulation results shows that the optimal resultant energy of the sensing nodes as a suitable energy retention criterion which makes this scheme more fault tolerant such that a cluster lifetime also is enhanced and is not dependent on a single cluster head.

Lathies Bhasker [14] has proposed a genetically derived secure cluster-based data aggregation in WSN. Initially the cluster heads are selected based on the node connectivity, which acts as a data aggregator. Then, the clustering process is executed using the genetic algorithm. When a cluster member wants to transmit the data to aggregator, a data encryption technique are utilized that offers authenticity, confidentiality and integrity.

3. PROPOSED ARCHITECTURE

In our proposed method one SPY agent (SA) is used to collect the information about the Cluster Heads (CH). The Following Fig.1 shows the functionality of SPY agent in the sensor network.

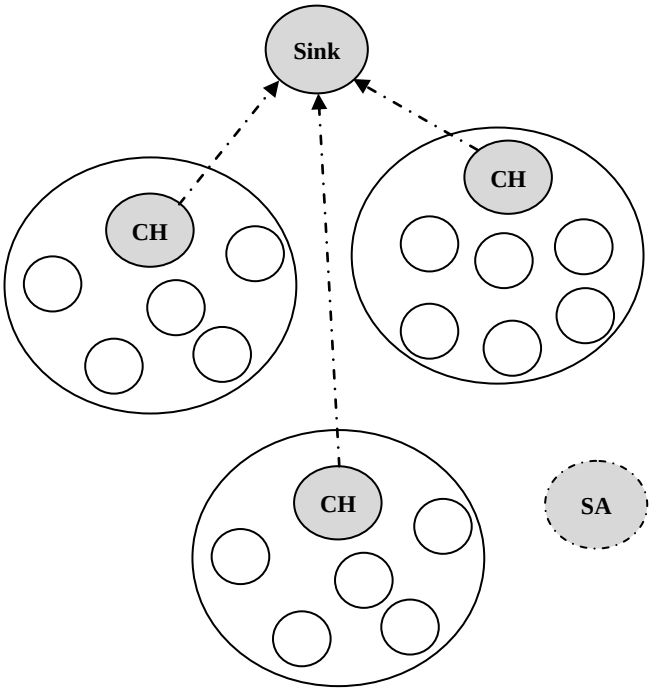

Fig.1. Proposed Architecture

3.1 SPY AGENT

The SPY Agent (SA) is the key element in our proposed architecture. The SA is a moving agent which moves around the network and monitors the Cluster Head's (CHs) status, CH status means it checks whether the CH is in active state or the CH node has sufficient amount of energy to continue the aggregation process. If any of the above conditions are failed means immediately the SPY Agent actively will participates in Weak CH identification and recovery process. The SPY Agent contains the following fields.

Table.1. SPY Agent Fields

CH ID	Life Time (LT)	Residual Energy(RE)

In the above Table.1, CH ID defines the Cluster head identification number. Life Time (LT) defines the total life period of the nodes in the network and Residual Energy defines the nodes energy level value.

This life time value is used for finding the next generation Cluster Head nodes from the earlier existing network environment i.e, at the end of previous aggregation process the SA will checks the LT value, if one node or CH has high LT value means that nodes will be chosen as a CH for the next generation.

3.2 CLUSTER HEAD FORMATION AND WEAK CLUSTER HEAD IDENTIFICATION

3.2.1 CH Formation:

In wireless sensor network each node has some initial energy power (Battery power) and there is some threshold energy (T) level for each node. There is lot of methods are available for selecting Cluster Head from the sensor network environment, In our approach, there is some voting among the sensor nodes taken place each node gives voting to the neighbor nodes, the node which obtained more number of votes elected as Cluster Head (CH).

3.2.2 Weak CH Identification:

Finding the Weak Cluster Head and the Cluster Head which was attacked by the malicious nodes will be done by the SPY Agent (SA). The SA in the network moves around the network and checks which are the Cluster Heads has less energy level than the Threshold energy (T) level, if any CH has lesser value means then that CH will mark as weak CH node and the weak node losses its votes then the weak CH become acts as an ordinary cluster member then the other nodes which contains more number of votes and the energy level which is higher than the threshold level will be chosen as new CH.

3.2.3 Residual Energy:

The residual energy (RE) of each node (Ni) is calculated by using the following formula.

$$RE = Ei – (Etx + Erx + Ea)$$

Where,

RE - It is the Residual Energy

Ei - Initial Energy of Each node

Etx - Energy utilized at the time of transmission

Erx - Energy utilized at the time of data reception

Ea - Energy required to keep the node active [14]

3.3 SPY AGENT ALGORITHM

Step 1: Initially the Spy Agent (SA) moves around the network.

Step 2: SA updates its SA Field table [i.e., the CH-ID, Life Time (LT) Value and Residual Energy (RE)]

Step 3: Check, if the Residual Energy (RE) < Threshold (T)

Step 4: If yes, the CH will mark as weak CH and losses its votes

Step 5: Otherwise the SA moves to the next CH and repeat step (2) to (4)

The following flow chart shows about the SPY Agent Process.

The Proposed architecture and the SPY Agent algorithm are explained through the above flow chart. The security for the data transmission is achieved through efficient encryption and decryption mechanism which is explained in [14].

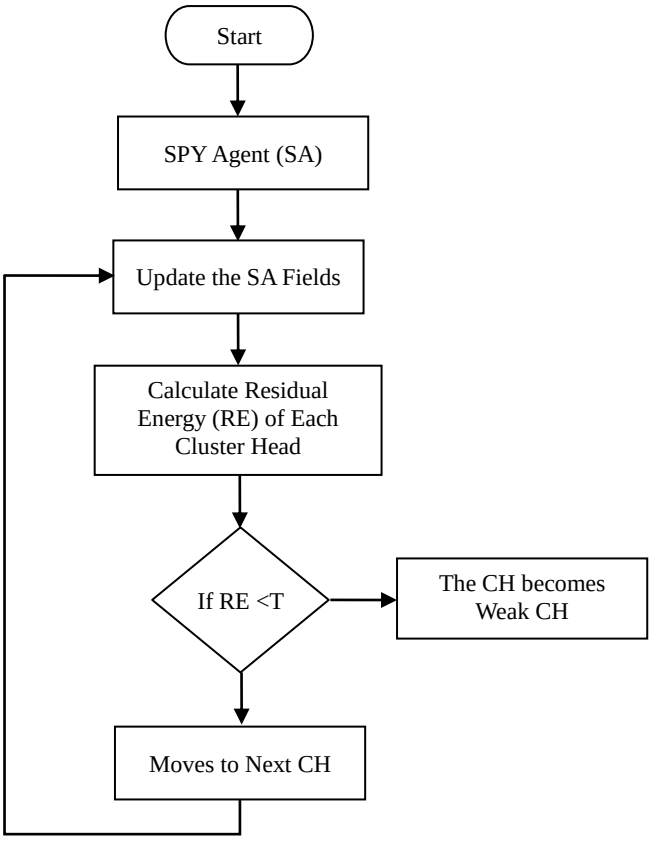

Fig.2. SPY Agent Process Flow Chart

4. SIMULATION RESULTS

Simulation Model and Parameters

The Network Simulator (NS2) [15], is used to simulate the proposed architecture. In the simulation, the mobile nodes move in a 500 meter × 500 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in table.

Table.2. Simulation Settings and Parameters

No. of Nodes	20,40,60,80 and100
Area Size	500 × 500
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Rate	50,100,150,200 and 250kb
Initial Energy	10.1J
Transmission Power	0.660
Receiving Power	0.395
Routing Protocols	AODV and DSDV

Performance Metrics

The proposed SPY Agent based secure data aggregation is analyzed for proactive and reactive protocols. Here we have

taken AODV and DSDV protocols. The performance is evaluated mainly, according to the following metrics.

Packet Delivery Ratio: It is the ratio between the number of packets received and the number of packets sent.

Packet Drop: It refers the average number of packets dropped during the transmission

Residual Energy: It is the energy level remain in each node after the flow transmission

Delay: It is the amount of time taken by the nodes to transmit the data packets.

4.1 RESULTS

4.1.1 Based on Nodes:

In the initial experiment our proposed architecture is evaluated based on number nodes as one of the parameters and the results are shown below. We vary the number of nodes as 20, 40, 60, 80 and 100.

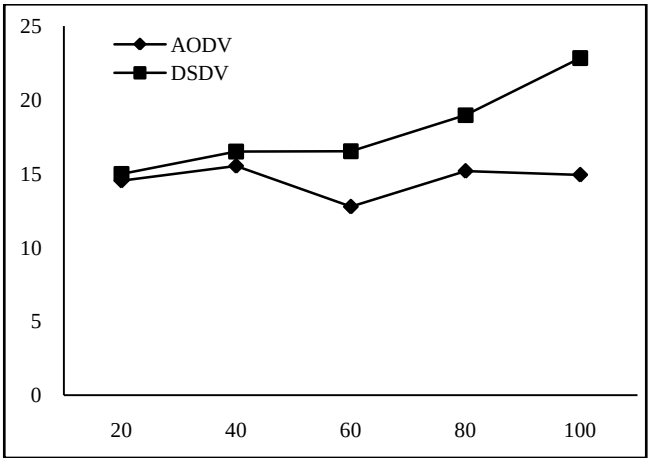

Fig.3. Nodes Vs Delay

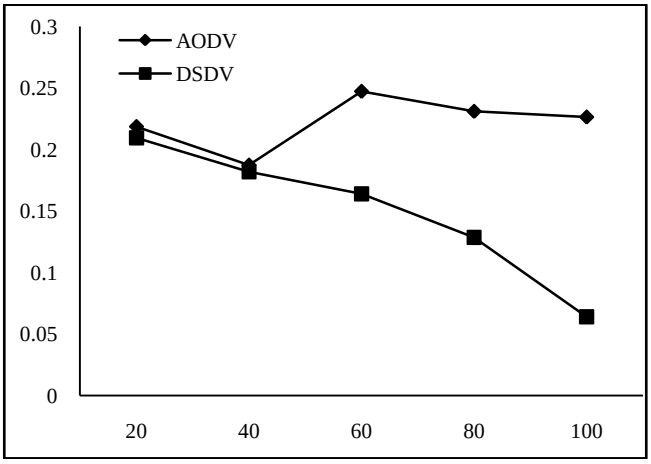

Fig.4. Nodes Vs Delivery Ratio

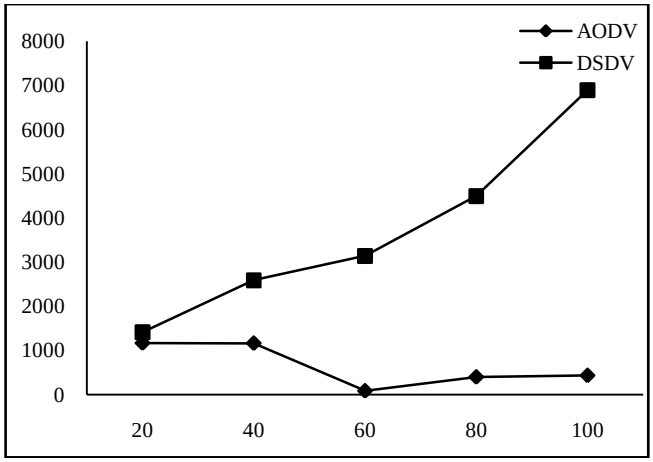

Fig.5. Nodes Vs Drop

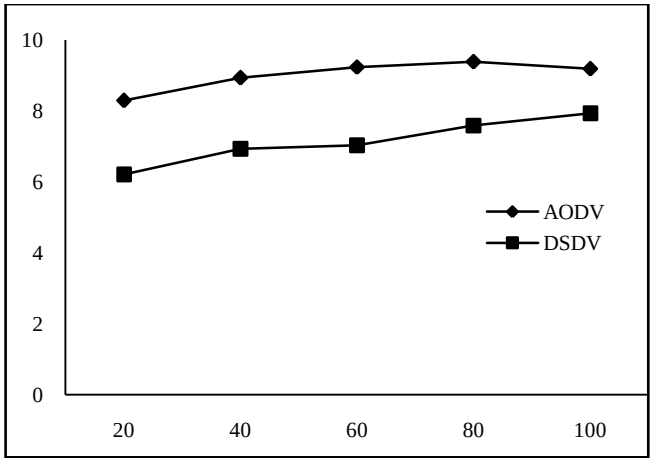

Fig.6. Nodes Vs Residual Energy

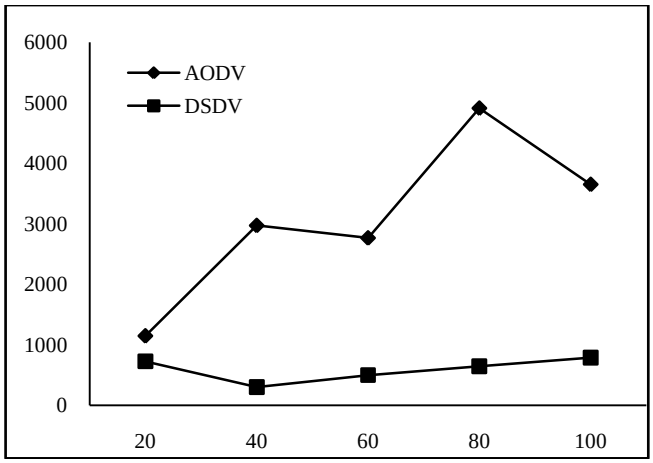

Fig.7. Nodes Vs Throughput

From the above results we can analyze the efficiency of our proposed methodology for the proactive routing protocol and reactive protocols for different number of nodes scenario.

4.1.2 Based on Rate:

In our second experiment we vary the transmission rate as 50, 100, 150, 200 and 250Kb.

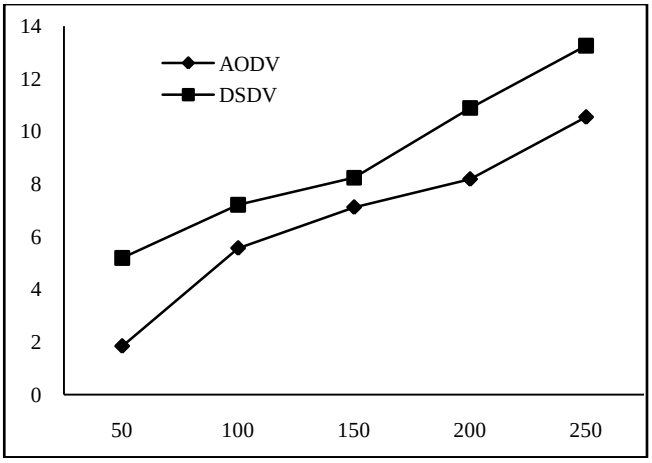

Fig.8. Rate Vs Delay

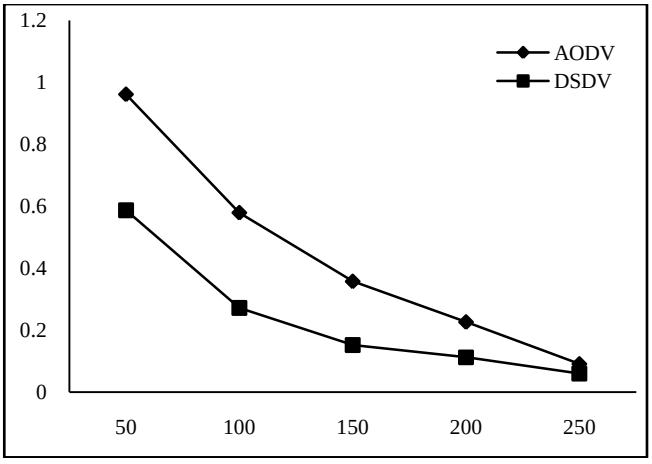

Fig.9. Rate Vs Delivery Ratio

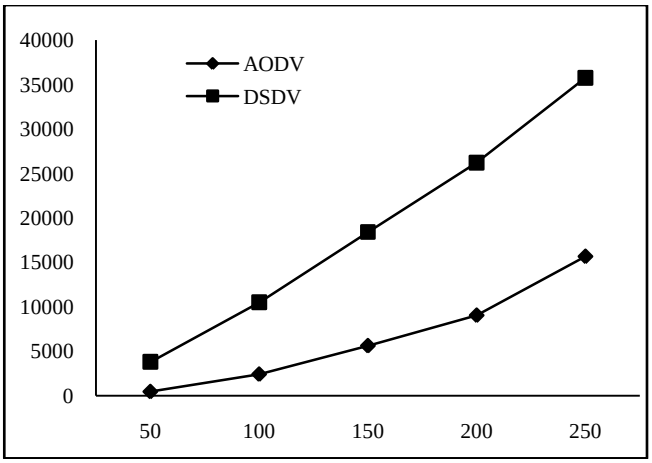

Fig.10. Rate Vs Drop

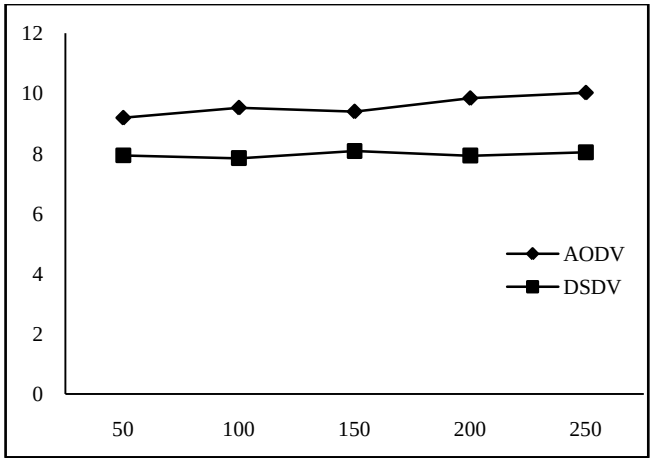

Fig.11. Rate Vs Residual Energy

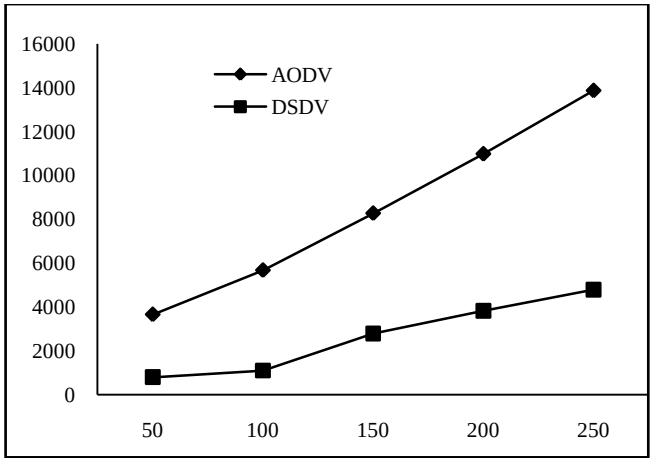

Fig.12. Rate Vs Throughput

From the above results we can analyze the efficiency of our proposed methodology for the proactive routing protocol and reactive protocols for different rate scenario.

5. CONCLUSION

In this paper we have proposed SPY Agent based data aggregation in Wireless sensor network. In here the SPY agent moves around the network and checks the status of each cluster head whether the cluster head is available to transmit the data to the Sink or the cluster head is in weak state based on their status it will updates its table. We have analyzed the proposed architecture for two different routing protocols. In future we have the plan to improve our SPY agent based secure data aggregation scheme by using some standard encryption and decryption methods.

REFERENCES

[1] G. Vijayalakshmi, S. Hema and S. Geethapriya, “Secure Data Aggregation & Query Processing in Wireless Sensor Networks using Enhanced Leach Protocol”, *International Journal of Emerging Science and Engineering*, Vol. 2, No. 1, pp. 51-56, 2013.

[2] M. Umashankar and C. Chandrasekar, "Energy Efficient Secured Data Fusion Assurance Mechanism for Wireless Sensor Networks", *European Journal of Scientific Research*, Vol. 49, No. 3, pp. 333-339, 2011.

[3] Kumar Padmanabh and Sunil Kumar Vuppala, "An Adaptive Data Aggregation Algorithm in Wireless Sensor Network with Bursty Source", *Wireless Sensor Network*, Vol. 1, No. 3, pp. 222-232, 2009.

[4] V. Bhoopathy and R. M. S. Parvathi, "Energy Efficient Secure Data Aggregation Protocol for Wireless Sensor Networks", *European Journal of Scientific Research*, Vol. 50, No. 1, pp. 48-58, 2011.

[5] Vaibhav Pandey, Amarjeet Kaur and Narottam Chand, "A review on data aggregation techniques in wireless sensor network", *Journal of Electronic and Electrical Engineering*, Vol. 1, No. 2, pp. 1-8, 2010.

[6] Nandini. S. Patil and P. R. Patil, "Data Aggregation in Wireless Sensor Network", *IEEE International Conference on Computational Intelligence and Computing Research*, 2010.

[7] Kiran Maraiya, Kamal Kant and Nitin Gupta, "Wireless Sensor Network: A Review on Data Aggregation", *International Journal of Scientific & Engineering Research*, Vol. 2, No. 4, pp. 1-6, 2011.

[8] Sung-Hwa Hong, Jeong-Min Park and Joon-Min Gil, "Performance Evaluation of a Simple Cluster-Based Aggregation and Routing in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, Vol. 2013, Article ID: 501594, pp. 1-9, 2013.

[9] Y. R. Preethi, C. R. Manjunath and M. Manohar, "Data Routing in In-network Aggregation in WSN: a Cluster Based approach", *International Journal of Modern Engineering Research*, Vol. 3, No. 3, pp. 1636-1640, 2013.

[10] Hiren Thakkar, Sushruta Mishra and Alok Chakrabarty, "A Power Efficient Cluster-based Data Aggregation Protocol for WSN (MHML)", *International Journal of Engineering and Innovative Technology*, Vol. 1, No. 4, pp. 241-246, 2012.

[11] Mohammad Mostafizur Rahman Mozumdar, Nan Guofang, Francesco Gregoretti and Luciano Lavagno, "An Efficient Data Aggregation Algorithm for Cluster-based Sensor Network", *Journal of Networks*, Vol. 4, No. 7, pp. 598-606, 2009.

[12] K. Amrutha mohanan and P. Vijayalakshmi, "Trust based Data Aggregation in Wireless Sensor Networks", *International Journal of Computer Applications*, Vol. 73, No. 22, pp. 8-12, 2013.

[13] Soubhagya Ranjan Behera and Asit Sar, "Optimal Residual Energy Clustered Data Aggregation protocol (ORECDA) in WSNs", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, No. 1. pp. 80-85, 2013.

[14] Lathies Bhasker, "Genetically derived secure cluster-based data aggregation in wireless sensor networks", *IET Information Security*, Vol. 8, No. 1, pp. 1-7, 2014.

[15] Network Simulator, Available at: http:///www.isi.edu/nsnam/ns.