International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-3)

Research Article | **March 2014**

Improved Secure Routing Scheme with Encrypted Session keys in WSN

Surinderjit Kaur[1], Mrs. Amrit Kaur[2] , Kiranveer Kaur[3]
[1]M.tech Scholar, Computer Engineering Department , [2]Asst.Professor, Computer Engineering Department, [3]Department of Computer Science
[1]Punjabi University, Patiala, Punjab, India, [2]Punjabi University, Patiala, Punjab, India,
[3]Punjabi University, Patiala, Punjab, India

Abstract:

Wireless sensor network nodes are very tiny in size and their cost is also not very high. During the process of data sensing, data gathering and data transmission, the charge of the power unit associated with any node gets low, after certain time, i.e., each node has its life time. In this paper a secure symmetric key will be proposed for wireless sensor network. After deployment of nodes, we will assign keys manually with Hash Function which is Blowfish. Time synchronization and clustering technique is used. RSSI message will be used for cluster head for cluster selection. To defend against the threats proper security schemes are required Elliptic Curve Cryptography (ECC) is the best candidate due to its smaller key size. This paper focus discuss and evaluate the performance of Ad hoc On Demand Distance Vector (AODV) routing protocol for monitoring of critical conditions with the help of important metrics like delay, throughput and network load with different techniques in different scenarios for mobile nodes. On the basis of results derived from simulation a conclusion is drawn on the comparison between these different techniques with parameters like delay, throughput and network load.

Keywords: WSN, Elliptic Curve Cryptography (ECC), AODV, RSSI

I. INTRODUCTION

A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks are the helpful effort of sensor nodes. Sensor nodes are fitted with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and Transmit only the required and partially processed data [1].In wireless sensor networks the energy dissipation in transmission of data directly depends on the routing algorithm. Hence, resource constraint Sensor Networks requires an optimum algorithm for routing [2]. The security mechanism employed in wireless sensor network should be as light as possible. Authentication and encryption based on symmetrical cryptography are lightweight security measures, but they can only prevent most outside attacks. In addition, routing decision is always affected by many factors, and most current routing protocols make routing decision only by energy or distance which cannot balance the efficiency and the life of the network well. In this paper, we try to put forward an efficient secure routing scheme by considering the security and the routing related factors naturally [3]. The sensor nodes are usually scattered in a sensor field as shown in Fig.1.1. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink.

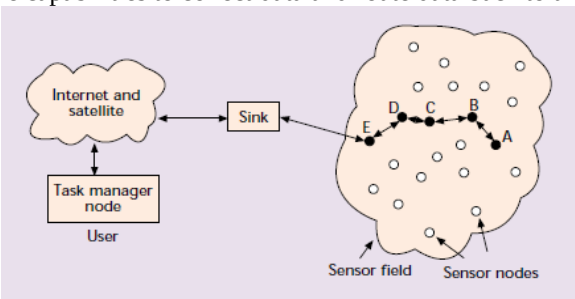

Fig. 1 Sensor nodes scattered in a sensor field

Data are routed back to the sink by a multihop communications less architecture through the sink as shown in Fig.1.1. The sink may communicate with the task manager node via Internet or satellite. The design of the sensor network as described by Fig.1.1 is influenced by many factors, including fault tolerance, scalability, production costs, operating environment, sensor network topology, hardware constraints, transmission media, and power consumption.Hence there is a necessity to propose new routing scheme secure routing in cluster based wireless sensor network with session keys by

symmetric cryptography (SRCWSNS). Cluster routing model more energy efficient model compare to direct or multi-hop routing. Proposed scheme easy to understand and takes little amount of memory for storing keys. Overhead is also lesser compare to complex cryptograph based protocols. The proposed scheme implemented on OPNET simulator, which has given better results compare to existing protocols[4].

II. ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS

The routing techniques are classified into three categories based on the underlying network structure: flat, hierarchical, and location-based routing. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, and coherent based depending on the protocol operation.Protocols is divided according to the structure of network which is very important for the required operation. The routing techniques are divided into two categories according to their functionalities:-

2.1 Network Structure

In flat networks all nodes play the same role, while hierarchical protocols aim to cluster the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy. Location-based protocols utilize position information to relay the data to the desired regions rather than the whole network.

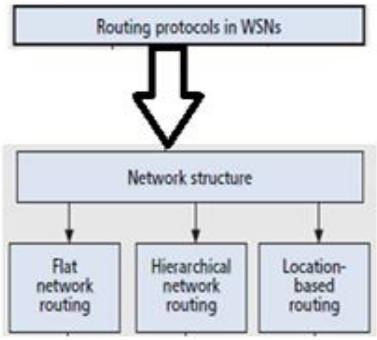

Fig. 2 Classification of Routing protocol in WSN

2.2 Protocol Operation

In QoS Based Routing to minimizing energy consumption, it is essential to consider QoS requirements in terms of delay, reliability and fault tolerance for routing in WSNs.

Both fault tolerance and reliability require the deployment of more than necessary sensors so that the network can continue to function properly and deliver accurate sensed data to the sink even with some sensor failures and Query Based Routing:-In query based routing, the sink node initiates the communication by broadcasting a query for data over the network.

III. LITREATURE SURVEY

In this present, a brief account has been put forth of the available literature that has been studied briefly. Considering the deterministic underlying dynamics of Routing Protocols, author collected additional knowledge of specific Routing Protocols and its applications through the literatures in order to make improved performance.

K.S.Arikumar,(2011) et al [6] presented a two-factor user authentication protocol for WSN, which provides strong authentication, session key establishment.This scheme allows the users to choose and change their passwords freely, and do not maintain any verifier table. Authors compare proposal with other exiting technique through simulation and we show that it achieves high efficiency.

Wassim Drira, (2012) et al [7] studied a hybrid authentication and key agreement scheme where symmetric cryptography is used in sensor/actuator nodes while identity-based cryptography concept is used between smart phone (MN) and the storage site (SS). We present two protocols to authenticate and establish pair wise and group keys between all tiers and to provide public and private keys for MNs.

Asha Rani Mishra, (2012) et al [8] has described different issues of Wireless Sensor Network (WSN) and the relevance of the Elliptic curve y cryptography. Traditionally security is implemented through hardware or software and is generally achieved through cryptographic methods. Limited area, nature of links, limited processing, power and memory of WSNs leads to strict constraints on the selection of cryptographic techniques. Elliptic Curve Cryptography (ECC) is the best candidate due to its smaller key size. High security despite of smaller key size results in area and power efficient crypto systems.

Donnie H. Kim, (2010) et al [9] has proposed secure code-update protocols for sensor networks have been based on asymmetric-crypto primitives such as digital signatures. In this approach, Castor explores the feasibility of securing an existing code-update protocol, Deluge, using symmetric-crypto mechanisms that are more suited to the resource constraints of sensor nodes.

Shohreh Ahvar, (2011) et al [10] has proposed an energy efficient query-based routing protocol called EEQR. This protocol is able to operate as both energy saver and energy balancer. In addition, it is intended for contexts in which

geographic routing criteria are not applicable. The results of EEQR simulations are compared with some well-known query-based routing protocols. Results show that EEQR achieves significant improvements in terms of energy saving and energy balancing.

IV. SIMULATION SETUP

4.1 Simulator: - The simulation is performed using the OPNET (Optimized Network Engineering Tool) Modeler 14.5 simulator. OPNET is a discrete event network simulator that provides virtual network communication environment. OPNET Modeler 14.5 is chosen because it is one of the leading environments for network modeling and simulation. It offers easy graphical interface. This tool is highly reliable, robust and efficient. It supports large number of built-in industry standard network. I started proceeding with pre deployment of sensor nodes and continue with implementation of traffic on sensor network. After this process distributes the pre defined symmetric keys to all sensors with hash function Blowfish algorithm of 128 bit encryption. This key distribution will provide private encryption to the deployed network.

Initially find out delay, throughput and network load without using any technique. In wireless sensor network, there are 50 sensors nodes which are randomly deployed in a field of (10km*10km). FTP application is used having data rate is 1mbps. I have used AODV protocol in all scenarios with using different techniques. All scenarios were simulated with 4500 seconds (1hour 15minutes).

In next step time synchronization technique find out delay, throughput and network load.

Afterwards using clustering technique and selection of cluster head done on the bases of total energy depleted by the sensor. Sensor with more energy remaining will become the cluster head. Energy will also be measured and must be more than threshold energy level.

In Next step again used clustering technique find out delay, throughput and network load with some failure nodes. After the completion of all process compiled the simulation and analyzed the results.

4.2 Simulation Parameters

To perform this simulation the network designed is wireless local area network (WLAN) consisting of network as sensor nodes and base station. All the networks are modeled on area of 10X10 km and FTP application is used data rate 1mbps and 11mbps. All scenarios are simulated for 4500 seconds (1hour 15minutes). To configure the application and for mobility of nodes profile configuration and application configuration objects are included as shown in figure according to scenario. Therefore, all simulation scenarios consisting of different number of nodes i.e. 50 are considered for routing protocol AODV. Different web traffic is generated using the Application and Profile Configuration. Table 1 and Table 2 shows the simulation parameters used in this study.

TABLE1. Simulation Parameters

Area of the sensor field	10×10 km
Sensor Nodes in all scenarios	50
Simulation Time	4500 seconds
Protocol	AODV
Traffic type	FTP
Performance Parameters	Throughput, Delay and Network load
Type of Nodes	Mobile
Data rate	1mbps,11mbps

Table 2: AODV parameters

Active Route Timeout(seconds)	3
Hello Interval(seconds)	2
Allowed Hello Loss	2
Route Error Rate limit(pkts/sec)	10
Timeout Buffer	2

4.3 Performance Metrics

a) *Throughput: - The average rate at which the data packet is delivered successfully from one node to another over a communication network is known as throughput. The throughput is usually measured in bits per second (bits/sec).* Throughput= (number of delivered packet*packet size)/total duration of simulation.

b) Delay: - It is time taken by the packet from the movement it is transmitted on the network by source node to reach the destination node.

c) Network Load (bits/sec): Network Load is a statistic represents the total data traffic received (in bits/sec) by the network from the higher layers of the MACs that accepted and queued for transmission. This statistic doesn't include any higher layer data traffic that is rejected without queuing due to full queue or large size of the data packet.

V. RESULTS AND DISCUSSIONS

The results of simulations are analyzed and discussed in this chapter. The results are analyzed and discussed in different scenarios having networks of fifty sensor nodes for monitoring applications. In proposed framework, I have uses symmetric key cryptographic Blowfish algorithm which is applicable to all three level of the network.

In the first scenario there are fifty sensor nodes and the parameter delay, throughput and network load for the routing protocol AODV is analyzed. In second scenario the number of nodes is same. It is based on time synchronized technique and the many parameters are set and performance of the protocols is analyzed. In the third scenario the number of nodes is again same. In this scenario clustering technique is used and in this design the cluster heads for best performance of the network. Finally in the fourth scenarios some nodes of network is failed and performance of network is analyzed by using same technique which is used in third scenario and the parameter delay, throughput and network load for the routing protocol AODV is analyzed.

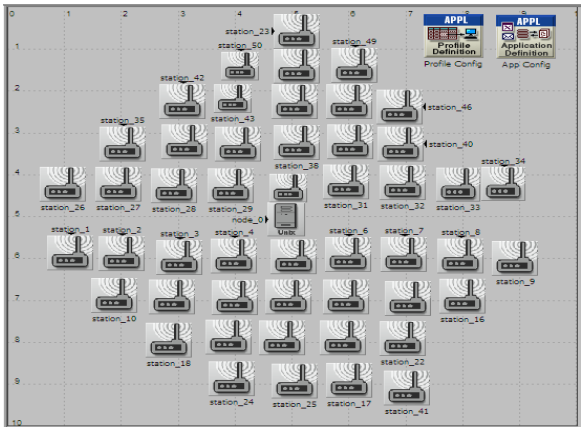

Fig. 3 Simple Wireless Sensor Network

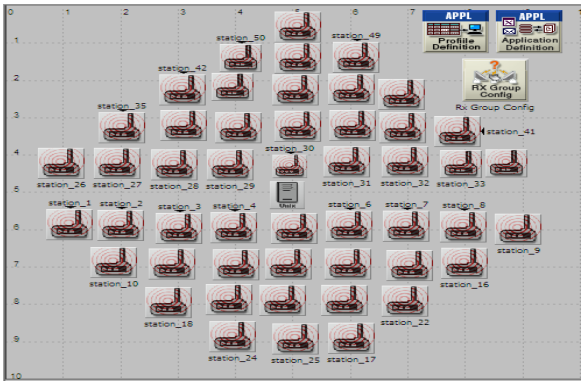

Fig. 4 Wireless Sensor Network using Time Synchronization Technique

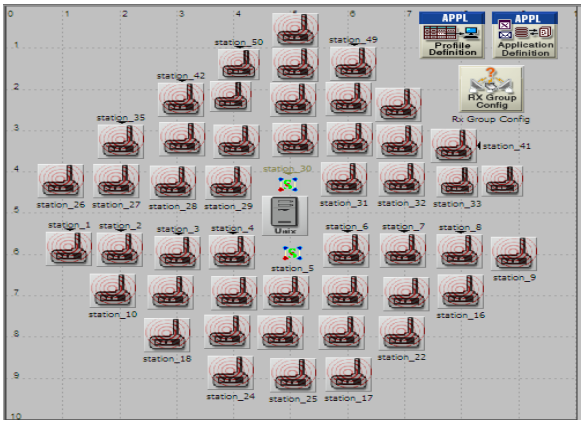

Fig. 5 Wireless Sensor Network using clustering Technique

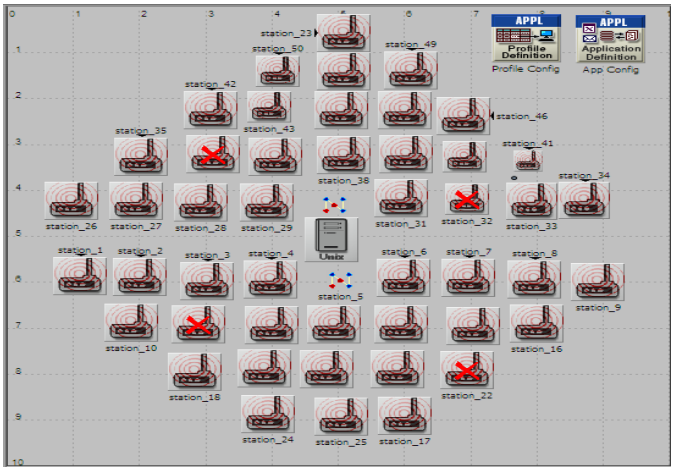

Fig. 6 Wireless Sensor Network using clustering Technique with some node failure

A. Delay

In figure 7 no technique applied on mobile nodes in a given scenario. During simulation delay is found at different intervals. In showing graph x-axis shows the time and y-axis shows the delay in term of seconds. Maximum delay is finding at 0.0023 sec.

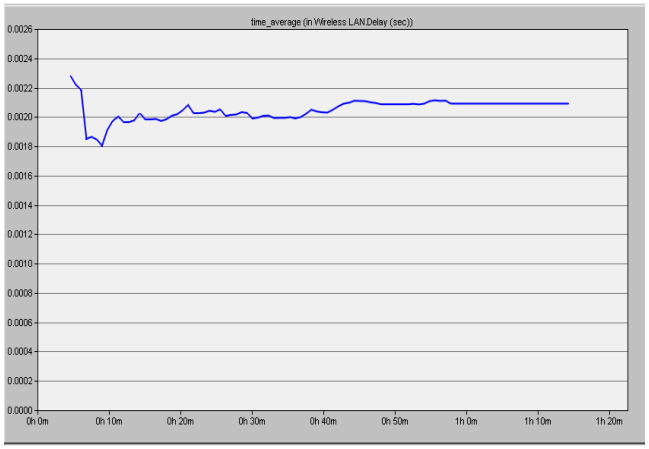

Fig. 7 Delay of Simple scenario

The value of delay decreases gradually till 0.0018 sec. Value of delay increases and decreases gradually throughout the simulation process. It is concluded that during simulation for delay there is more fluctuation, and find more delay when there has no technique applied.

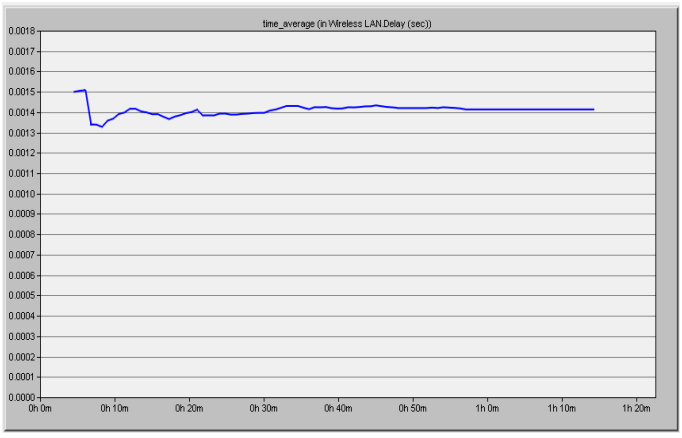

Fig. 8 Delay using Time Synchronization technique

In figure 8 time synchronization technique is applied on mobile nodes in a given scenario. During simulation delay is found at different intervals. Maximum delay is finding at 0.0015 sec. The value of delay decreases gradually till 0.0013 sec. It is concluded that during simulation for delay there is less fluctuation, and find less delay when there has time synchronization technique applied as compared to first scenario.

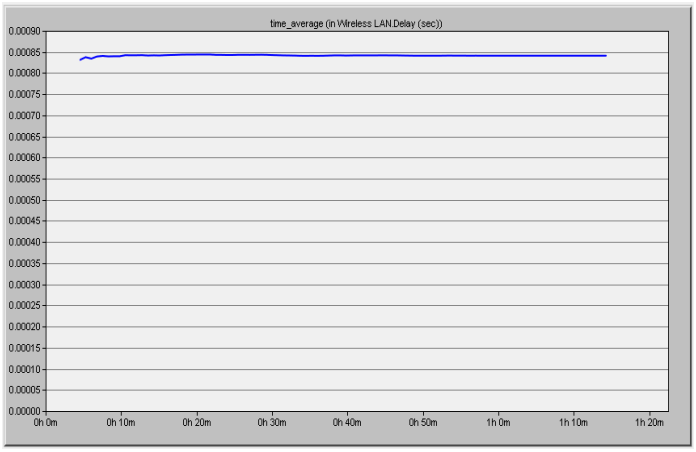

Fig. 9 Delay using clustering technique

In figure 9 clustering technique is applied on mobile nodes in a given scenario. During simulation there is no change in the delay by using clustering technique as shown in figure. It is concluded that during simulation for delay there is no fluctuation, and find no delay when there has clustering technique applied as compared to second scenario.

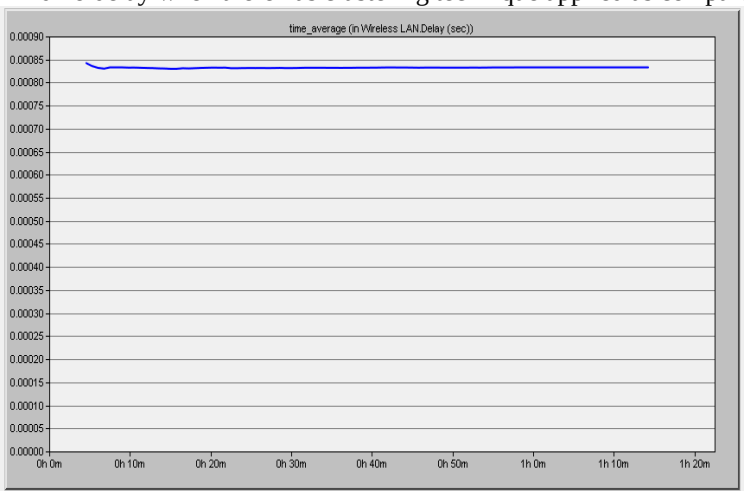

Fig. 10 Delay using clustering technique with some failure nodes

In figure 10 again clustering technique is applied on mobile nodes in a given scenario but with some failure nodes. During simulation there is no change in the delay by using clustering technique when some nodes are failed as shown in figure.

It is concluded that during simulation for delay there is no fluctuation, and find no delay when there has some nodes of network is failed by using clustering technique.

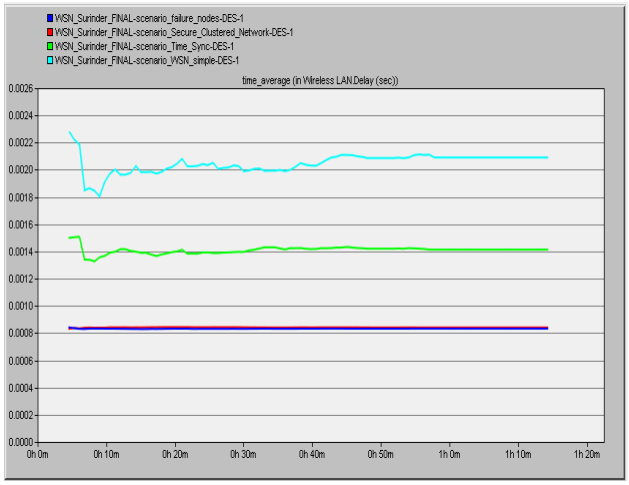

Fig. 11 Comparison of Delay

So according to the simulation the performance analysis of clustering technique is better in aspect of delay.

B. Throughput

In figure 12 there is no technique applied on mobile nodes in a given scenario. Maximum throughput is finding at 7500 sec. Value of throughput increases and decreases gradually throughout the simulation process.

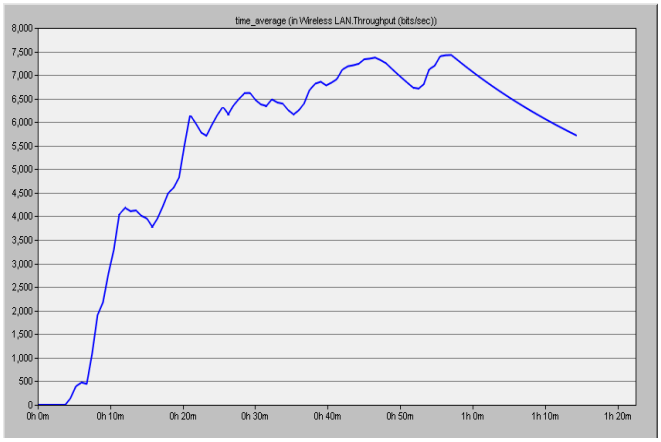

Fig. 12 Throughput of Simple Scenario

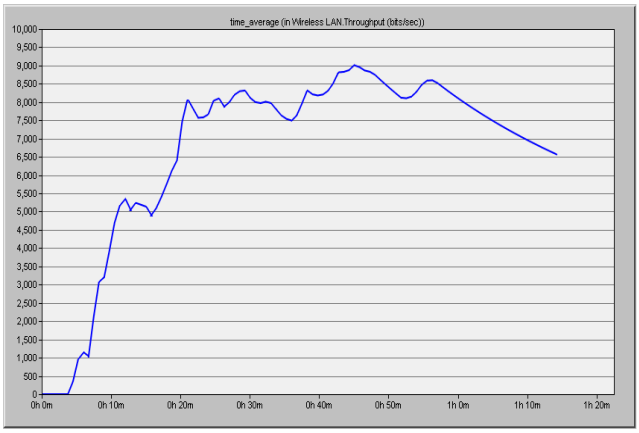

Fig. 13 Throughput using Time Synchronization Technique

In figure 13 there is time synchronization technique is applied on mobile nodes in a given figure. Maximum throughput is finding at 9000 sec. Value of throughput increases and decreases gradually throughout the simulation process. It is concluded that during simulation for throughput there is more throughput when there has time synchronization technique applied as compared to first scenario.

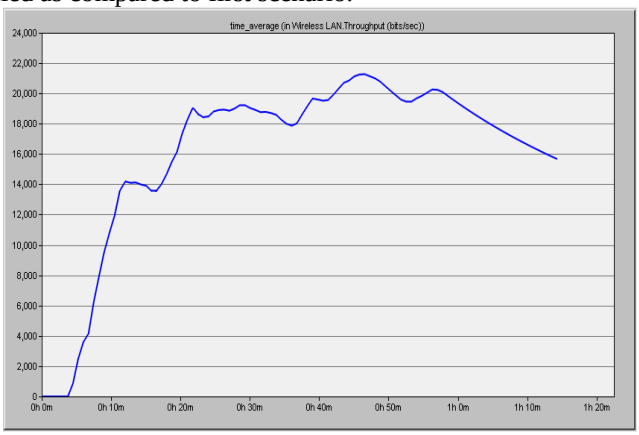

Fig. 14 Throughput using clustering technique

In figure 14 there is clustering technique is applied on mobile nodes in a given scenario. Maximum throughput is finding at 21000 sec. It is concluded that during simulation there is increase in throughput as compared to other techniques when there has clustering technique is applied.

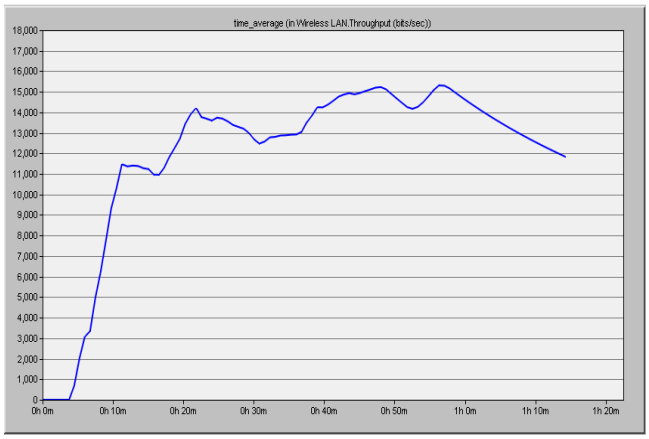

Fig. 15 Throughput of using clustering technique with some failure nodes

In figure 15 again clustering technique is applied on mobile nodes in a given scenario but i have failed some nodes. Maximum throughput is finding at 15550 sec. It is concluded that during simulation there is increase in throughput as compared to first and second scenarios but less as compared to third scenario when there has clustering technique is applied.

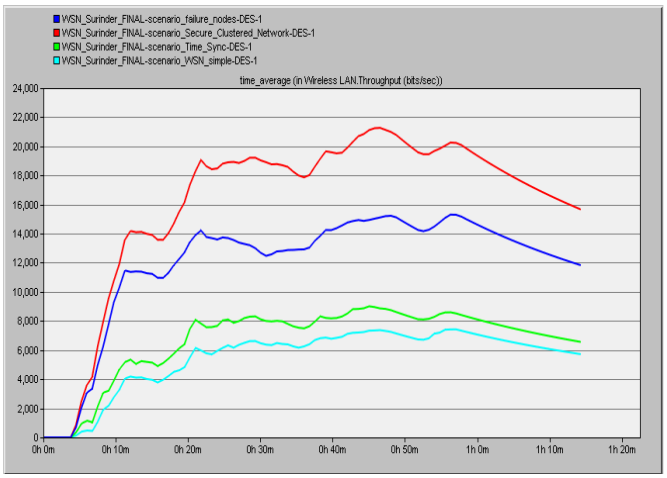

Fig. 16 Comparison of Throughput

So according to the simulation the performance analysis of clustering technique is better in aspect of throughput for mobile nodes.

C. Network Load

In figure 17 there is no technique applied on mobile nodes in a given scenario. Maximum network load is finding at 5800 sec. and network load is decreases gradually till the end of simulation. Value of network load increases and decreases gradually throughout the simulation process.

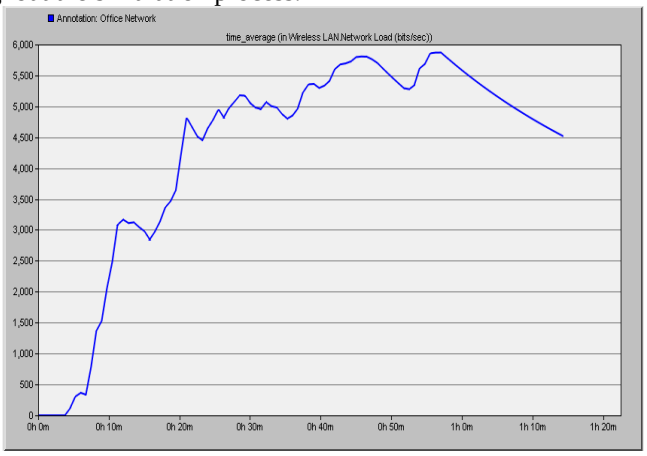

Fig. 17 Network Load of Simple Scenario

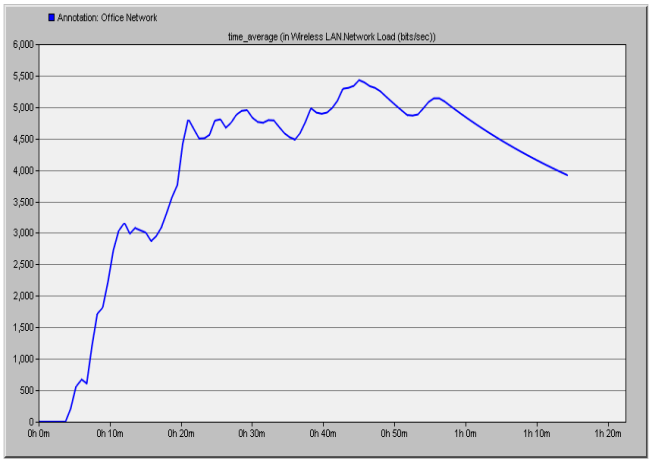

Fig. 18 Network Load using Time Synchronization Technique

In figure 18 there is time synchronization technique is applied on mobile nodes in a given scenario. Maximum network load is finding at 5400 sec. It is concluded that during simulation there is less network load when there has time synchronization technique applied as compared to first scenario in which no technique is used.

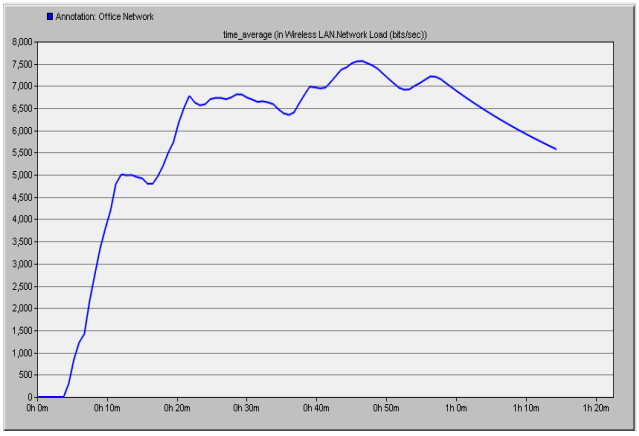

Fig. 19 Network Load using Clustering Technique

In figure 19 there is clustering technique is applied on mobile nodes in a given scenario. Maximum Network Load is finding at 7600 sec. It is concluded that during simulation there is increase in Network Load as compared to previous scenarios when there has clustering technique is applied

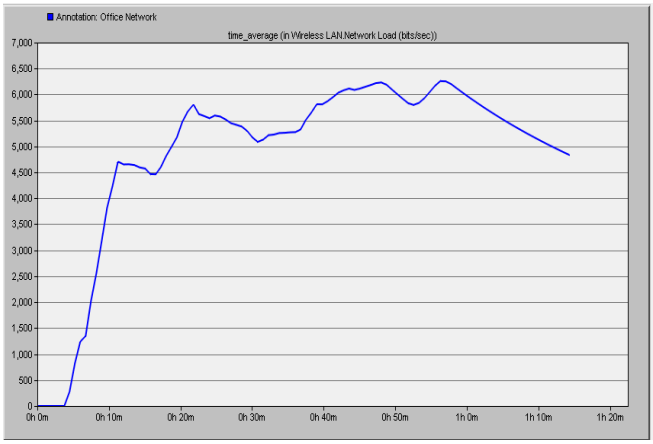

Fig. 20 Network Load using Clustering Technique with Failure node

In figure 20 there is clustering technique is applied on mobile nodes in a given scenario. Maximum Network Load is finding at 6300 sec. It is concluded that during simulation there is increase in Network Load as compared to previous scenarios when there has clustering technique is applied.

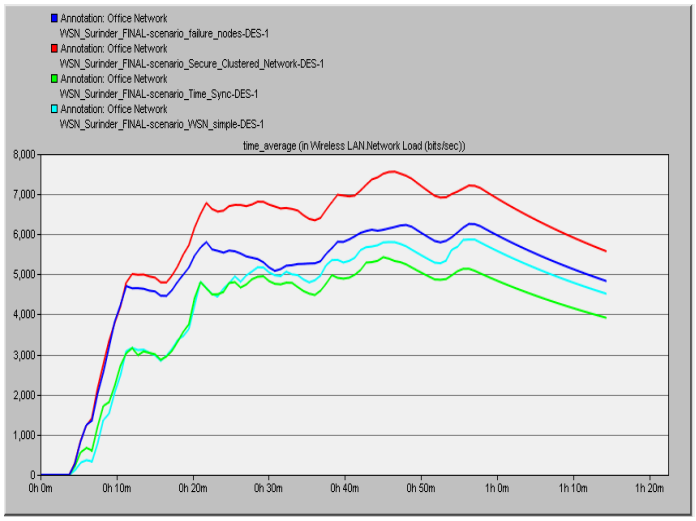

Fig. 21 Comparison of Network Load

So according to the simulation the performance analysis of clustering technique with some failure nodes is better as compared to other scenarios. On selected techniques and protocol conducted study concludes that in overall performance clustering technique is better from other techniques.

VI. CONCLUSIONS AND FUTURE SCOPE

6.1 Conclusions

This paper discuss and evaluate the performance of different techniques in different scenarios for mobile nodes by using Ad hoc On Demand Distance Vector (AODV) routing protocol for monitoring of critical conditions with the help of important metrics like delay, throughput and network load. In each scenario all the nodes were used as source nodes of sending data to a common base station. So according to the simulation the performance analysis of clustering technique is better in aspect of delay and throughput for mobile nodes. In aspect of network delay the performance of clustering technique with some failure nodes is better as compared to other scenarios. On selected techniques and protocol conducted study concludes that in overall performance clustering technique is better from other techniques .The size of the networks also matters for the performance of the protocol. On the basis of results derived from simulation a conclusion is drawn on the comparison between these different techniques with parameters like delay, throughput and network load I conclude that clustering technique is better for the energy efficiency.

6.2 Future Scope

Proposed solution can be distributed wireless mesh network and networks which is having middleware as an operating head. It is very interesting to seeing the performance of the Elliptic curve cryptography (ECC) and described in the proposed work on the network which is managed by middleware and networks where reprogramming as the sensor nodes occurred.

It can be very useful in area of security and monitoring of the network. Encrypted unique key distribution can provide good security option in the sensor network communication. By implementing strong encryption will help in providing good security in the sensor network. Cluster head selection mechanism is also provide useful stuff for the considering security in the network.

REFRENCES

[1] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University, *Wireless Communication and Mobile Computing*, Vol. 4,No 6,pp.623-637,2009.

[2] Harpreet Singh, Gurpreet Singh Josan, "Performance Analysis of AODV & DSR Routing Protocols in Wireless Sensor Networks", *International Journal of Engineering* ,Vol. 2, Issue 5,pp,2212-2216, September- October 2012.

[3] Xuanxia Yao, XueFeng Zheng, "A Secure Routing Scheme for Static Wireless Sensor Networks", *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Vol.2, pp.776-780, 2008

[4] Rayala Upendar Rao, "Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys", *International Journal of Computer Applications*, Vol. 55, Issue. 7, pp.48-52, October 2012.

[5] Bhoopathy, V. and R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks*", International Journal of Engineering Research and Applications (IJERA),* Vol. 2, Issue 2, pp.466-474,Mar-Apr 2012.

[6] K.S.Arikumar, K.Thirumoorthy, "Improved User Authentication in Wireless Sensor Networks", 2011 IEEE.

[7] Wassim Drira," A Hybrid Authentication and Key Establishment Scheme for WBAN", *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Vol. 2, No.3, pp.78-83, 2012.

[8] Asha Rani Mishra, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network," *International Journal of Engineering Research & Technology (IJERT)* ,Vol. 1 Issue 3, pp. 2-3,May-2012.
[9] Donnie H. Kim, "Exploring Symmetric Cryptography for Secure Network Reprogramming", *International conference on Information, Networking and Automation(ICINA),*Kunming, IEEE, pp. 215-218, 2010.
[10] Shohreh Ahvar1, Mehdi Mahdavi, " EEQR: An Energy Efficient Query-Based Routing Protocol for Wireless Sensor Networks", *Journal of Advances in Computer Research* ,Vol. 2, No. 3, pp. 25-38, August 2011.