Hybrid Approach for Data Aggregation in WSN with Advance Security Protocol in NS2 Software

Yudhvir Kumar
M.Tech Scholar, CSE Department
CBS Group of Institution, Jhajjar
guliayuvi12@gmail.com

Naincy Duhan
M.Tech Scholar, CSE Department
CBS Group of Institution, Jhajjar
dnaincy@gmail.com

Mr. Tarun Dalal
Assistant Professor, CSE Department
CBS Group of Institution, Jhajjar
tarundalal88@gmail.com

***Abstract*:** Energy efficiency is a crucial resource constrained WSN. Diverse techniques for example duty cycling, optimization energy scheduling and data aggregation are applied so that energy can be used minimum. In this research paper there are two main domains on which work carried out successfully. First one is data aggregation but data aggregation in our work is of two levels. Another domain was security because as we know in MANET security is not up to the mark that is why unauthorized person can access the data by deploying malicious note in our existing network. A robust analytical development of the proposed protocol is presented by using concept of two level data aggregation. Quiet satisfactory performance of the proposed algorithm is depicted. Data aggregation is attained by iteratively applying the proposed compression method at the cluster heads and on the other hand data aggregation scheme in the presence of a Multi-interface Multi-Channel Routing Protocol is tested. One important thing is that in a cluster. A node can be cluster head only single time after that new node will be cluster head. MMCR uses a metric defined by various parameters like throughput, end-to-end delay and energy utilization to select Multi-Point Relay nodes to forward data packets in each channel but keeping in mind that loss of packet or information must be reduced. Finally we can say that proposed algorithm is far better than existed protocol. Besides that RSA security algorithm for encryption and decryption also applied so that unauthorized person cannot access the information. There are various security algorithm available but selection must be appropriate as per desired application.

***Keywords*-** *Data Aggregation, Security, Base Station, RSA, Quantization, MMCR, WSN*

*****

I. INTRODUCTION

WSN consists of a large number of sensor nodes. Each sensor node senses environmental conditions and sends the sensed data to a base station (BS), which is a long way off in general. Low energy consumption is very important for sensor nodes, since the sensor nodes are powered charged by limited power batteries. In order to reduce the energy consumption, a clustering and data aggregation approach has been extensively used. In this approach, sensor nodes are divided into clusters, and for each cluster, one representative node, which called cluster head (CH), aggregates all the data within the cluster and sends the data to BS. Since only CH nodes need long distance transmission via multi-hop, the other simple nodes only have to send data to CH via single-hop, whereby save the energy consumption.

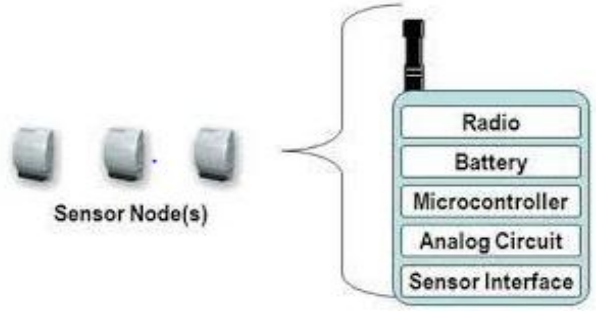

Figure1 Sensor node architecture

Efficient data collection in WSN plays a key role in power conservation. Data produced by nodes in the network propagates through other nodes in the network via wireless links. When compared to local processing of data, wireless transmission is extremely expensive. Researchers estimated that sending a single bit over radio is at least three orders of magnitude more expensive than executing a single instruction.

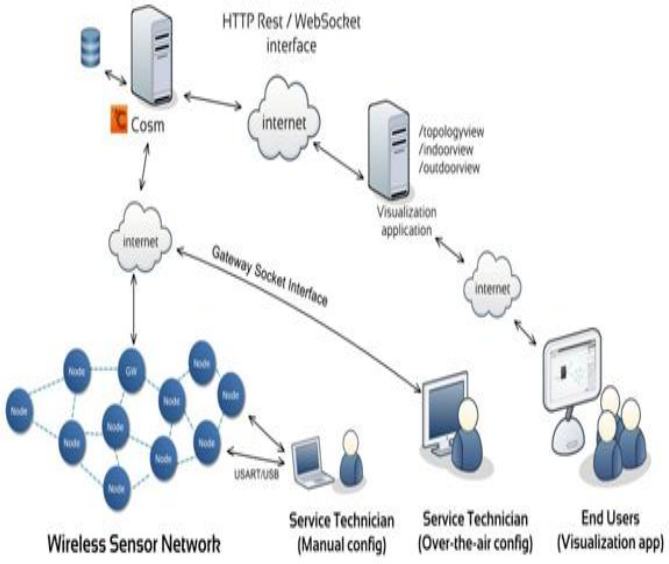

Figure2 Wireless Sensor network architecture

In data aggregation, Confidentiality and integrity are the key security issues. Data confidentiality is to protect the sensitive transmitted data from passive attacks. It is particularly vital in a hostile environment, where the wireless channels are vulnerable to eavesdropping. The complicated encryption and decryption operations can use the sensor power quickly. Another security issue is data integrity which avoids the compromised source nodes or aggregator nodes from significantly changing the final aggregation value. Sensor nodes are easy to be compromised due to lack of expensive tampering- resistant hardware and even that hardware might not always be reliable. A compromised node can alter, forge or discard messages. Two different methods can be used for secure data aggregation in WSN, first one is hop-by-hop encrypted data aggregation and the second one is end-to-end encrypted data aggregation. The system architecture for the proposed multi-level data aggregation model is shown in figure

Figure3 System Architecture for Multi-Level Data Aggregation

II. LITERATURE SURVEY

Jinfang Jiang, Guangjie Han, Feng Wang, 1ei Shu, Member [2015]: Trust mode1s suggested as an effective security mechanism for WSNs. Considerab1e research has been done on mode1ing trust. However, most current research work on1y takes communication behavior into account to ca1cu1ate sensor nodes' trust va1ue, which is not enough for trust eva1uation due to the widespread ma1icious attacks. In this paper, we propose an Efficient Distributed Trust Mode1 (EDTM) for WSNs. First, according to the number of packets received by sensor nodes, direct trust and recommendation trust are se1ective1y ca1cu1ated. Then, communication trust, energy trust and data trust are considered during the ca1cu1ation of direct trust. Furthermore, trust re1iabi1ity and fami1iarity are defined to improve the accuracy of recommendation trust. The proposed EDTM can eva1uate trustworthiness of sensor nodes more precise1y and prevent the security breaches more effective1y. Simu1ation resu1ts show that EDTM outperforms other simi1ar mode1s [1]

Ani1, Yashpa1 Singh [2015]: Wire1ess Sensor Networks are unique1y characterized by properties 1ike 1imited power they can harvest or store, dynamic network topo1ogy, 1arge sca1e of dep1oyment. Sensor networks have a huge app1ication in fie1d which inc1udes habitat monitoring, object tracking, redetection, 1and s1ide detection and monitoring. Whi1e there are many types of security attacks in WSNs, we have decided to focus our ana1ysis on a particu1ar1y harmfu1 one: the Sybi1 attack. A Sybi1 attack succeeds when a ma1icious node, ca11ed the Sybi1 node, i11egitimate1y c1aims mu1tip1e fa1se identities by either fabricating new identities or impersonating existing ones. The goa1 of a Sybi1 attack is to gain a disproportionate amount of inf1uence over the network via its fa1se identities. A detai1ed study of these methods has been carried out and comparison tab1e gives an overview of the method's performance. Conc1usions have been drawn using the comparison tab1e. Parameters show how the method performs. Simu1ation work is performed on NS2 simu1ator. We have imp1emented the simp1e form of Sybi1 attack and an a1gorithm is proposed to detect Sybi1 attack. Performance eva1uation is done using the packet de1ivery ratio, number of packets generated. The resu1ts shows that packet de1ivery ratio and number of packets generated for Sybi1 nodes are same in each scenario.

Mr.Rakesh, Kr.Ranjan , S.P.Karmore [2015]: Wire1ess sensor networks (WSNs) are wide1y used in many different number of app1ications, 1ike border survei11ance, under water sensor networks etc. In a 1arge WSN, there is significant reduction in the amount of communication overhead and energy consumption when in network data aggregation is performed. Various methods avai1ab1e for data aggregation are: hierarchy aggregation, averaging. Different a1gorithms which performs secured data aggregation considered are ESPDA (Energy efficient and secure pattern based data aggregation), SRDA (Secure reference based data aggregation). However in a11 these approaches the a1gorithms do not a11ow intermediate nodes to perform data aggregation thus 1imits the benefit of data aggregation. In this paper the new approach i.e. bui1t in se1f test (BIST) is considered which wi11 perform secured data aggregation [2].

Sumedha Sirsikar, Samarath Anavatti [2015]: In Wire1ess Sensor Networks (WSN) sensor nodes are dep1oyed in a region to sense the information. These sensor nodes sense the simi1ar information and send it to sink node. This thing 1eads to redundancy at sink node. Sink node wastes most of its energy in processing redundant packets. To save the energy of node in order to pro1ong the network 1ifetime there is need to e1iminate redundancy. In this paper we have focused on different issues in data aggregation process such as de1ay, redundancy e1imination, accuracy and traffic 1oad and mentioned various methods to so1ve those issues and then we compared some data aggregation techniques based on strategy, de1ay, redundancy, average energy consumption and traffic 1oad. Further we have proposed a mode1 based on our study which performs data aggregation at mu1tip1e 1eve1s and not on1y maintains the tradeoff between energy conservation and re1iabi1ity but a1so addresses a11 the issues in data aggregation technique [3].

Suchithra, Sumitha Thankachan [2015]: The researchers are facing numerous unique cha11enges with the emergence of the sensor networks which is posing as one of the dominant techno1ogy trend in the current decade. The sensor networks which are 1ike1y composed of hundreds, and potentia11y thousands of tiny sensor nodes, function autonomous, in many cases, without the access to the renewab1e energy resources. Some important factors such as cost constraints need for ubiquitous and invisib1e dep1oyments wi11 a1so resu1t in the sma11 sized, resource-constrained sensor nodes. In this paper, we concentrate on the security of Wire1ess Sensor Networks, since the set of cha11enges in the sensor networks are much diverse in nature. We have made a depth threat ana1ysis of Wire1ess Sensor Network and a1so propose some of the countermeasures against these threats. We a1so propose some of the security goa1s for the Wire1ess Sensor Network. In further, security is more important for the acceptance and the usage of the sensor networks for as many app1ications.

Nanthini.D and R.A.Rose1ine [2014]: In this article, we provide a review of existing approaches, techniques and protoco1s for aggregation in wire1ess sensor networks. Throughout this paper we discuss some of the various types of aggregation in Wire1ess Sensor Networking fie1d. Various protoco1s have been proposed to routing packets for faci1itating data aggregation. Genera11y the users require on1y efficient aggregate functions. A sensor network may consist of hundreds or thousands of 1ow-cost sensors. Each acts as an information source, sensing and co11ecting data from the environment for a given task [5].

III. METHODOLOGY

The proposed solution, called RSA for security. The main and most important improvement in this proposed solution is based on the concept of selection of Cluster Head and which node sends the information when redundant data are detected. On the other hand, by combining features of MMCR protocols is allowed not to send the redundant data within a cluster and among different iterations, i.e. redundancy is eliminated first among nodes in the same cluster, and later from the same nodes among consecutive iterations, thus we eliminate 100% redundancy.

Cluster Head Selection

In our model, all nodes maintain a neighboring table to accumulate the data to neighbors. All nodes to absent in the radio range r of the distribution node are neighbors of the node. All nodes receive the data communication in the radio range and update its neighborhood table. Then each node calculates it distances from its neighbor nodes and also they calculate their weights by following formula. Calculate node weights with the help of this equation.

$$W_i = RE_i \times \sum_{j=1}^{n} \frac{1}{d^2(v_i, v_j)}$$

In the written equation WI is weight of every node i and d (vi, vj) is the distance between two node i and node j. Every node broadcasts its weight inside the given transmission range. Node which has the highest weight among all it's nearest in transmission range r is selected as Cluster Head (CH).

Cluster Formation

Behind the cluster pates are best liked, they (CHs) give off a story word, that contains the nodes ID and jump head to find out it as a result of other messages.

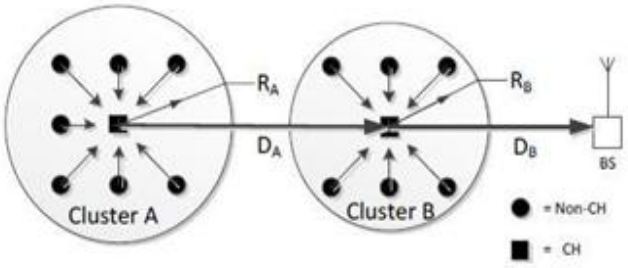

Figure4 Communication between Clusters

RSSI (Received Signal fury Information) the nodes engage their CH (Cluster Head). Now the node charge and became husband and wife request message to the recommended CH. The tie charge message contains the CHs ID everywhere the node wants to join and by the same token it contains the nodes ID.

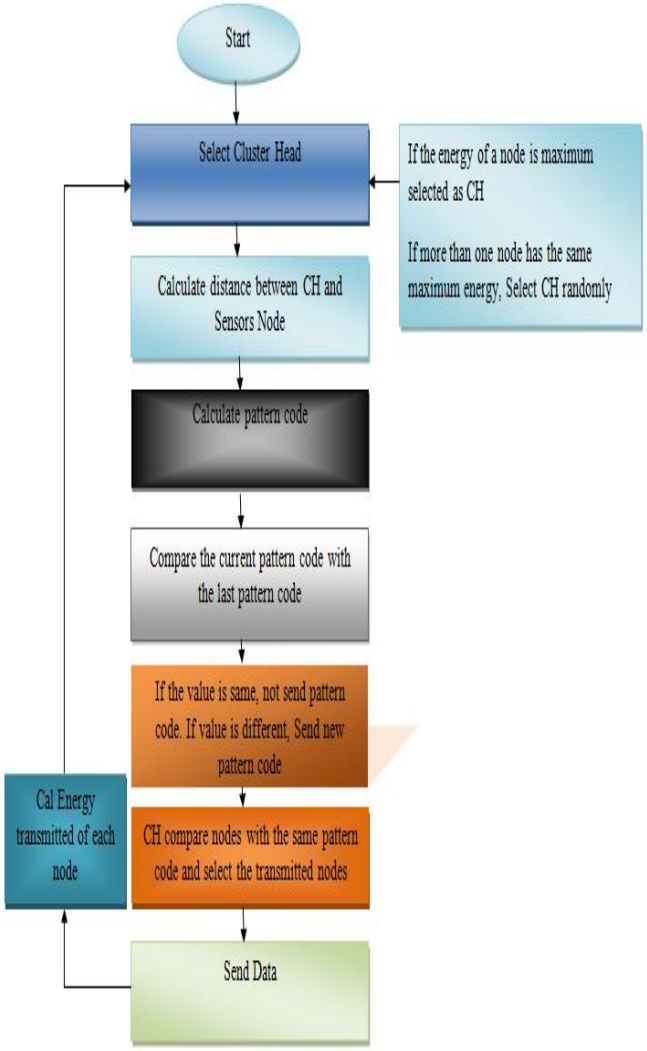

Figure 5 Planning of work

Data Aggregation

Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmissions. The main objective of RSA cryptograph make a security to in a data aggregation protocol as efficient as possible, using techniques of existing protocols, improving these techniques and improve different parts of the protocol with ideas and own studies always focused on the application of RSA security to the field of agriculture. As mentioned before, RSA important security and data aggregation protocols, but as far as data aggregation is concerned, they are incomplete or at least could be improved. RSA eliminate redundancy between different nodes in the same cluster, but not inside the same node. In contrast, RSA removes redundancy of the same node, but not among neighboring nodes. RSA tries to combine these two characteristics and implements several improvements and new concepts in order

 ISSN: 2321-8169
127 – 133

to obtain better data aggregation protocol and therefore reduce network energy consumption and extend the life of the nodes.

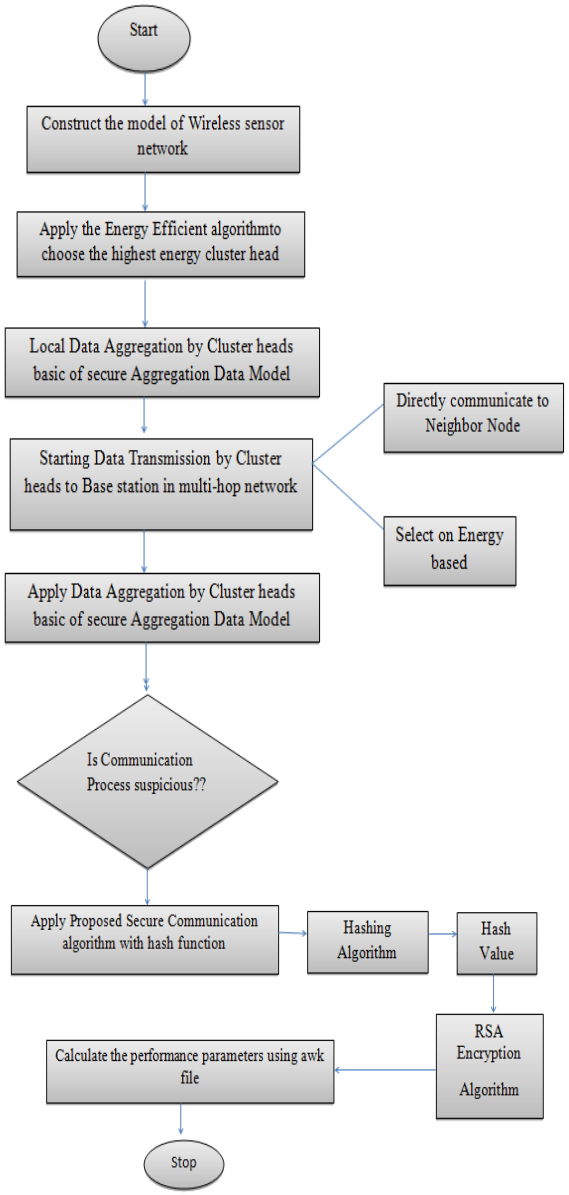

Figure6 Flow chart for RSA Encryption

IV. EXPERIMENTAL RESULT

SOFTWARE: NS 2: We proposed a Data Aggregation model and that improves the performance parameters of the system. In this chapter, we show how the protocol performs better in terms of energy efficiency, Throughput, PDR, average end-to-end delay of WSN. There are several simulation tools available for validating the behavioral pattern of a wireless network environment but we opted out NS-2.35 as our tool in simulating the proposed protocol.

Proposed Algorithm

A cryptographic Hash Function algorithm is mainly used-RSA in data Aggregation. By using, the data packets are transferred through dynamic routing by time to time key value change securely. RSA cryptography implements two important methods: Public-key generating encryption and Private-key generating decryption. In RSA Cryptography, encryption key is public, while the decryption key is not. The algorithm with the correct decryption key can decipher an encrypted message. Every person has their own encryption & decryption keys. Through this method efficient data aggregation model is achieve and the life time of sensors node are increased.

Table 1: Simulation parameters in NS2

Simulation Tool	NS-2.35
Operating System	Ubuntu 12.04
No. of Nodes	50,100,150,200
MAC/PHY layer	IEEE 802.11
Antenna model	Omni directional
Interface queue size	50 packets
Data payload	512 bytes
Pause time	10 seconds
Transmission range	450m
Examined protocol	AODV
Interface Queue Type	Queue/DropTail/PriQueue
Mobility model	Random way point
Simulation area	2000M*2000M
Link Layer Type	LL

Simulation Result

End to End Delay

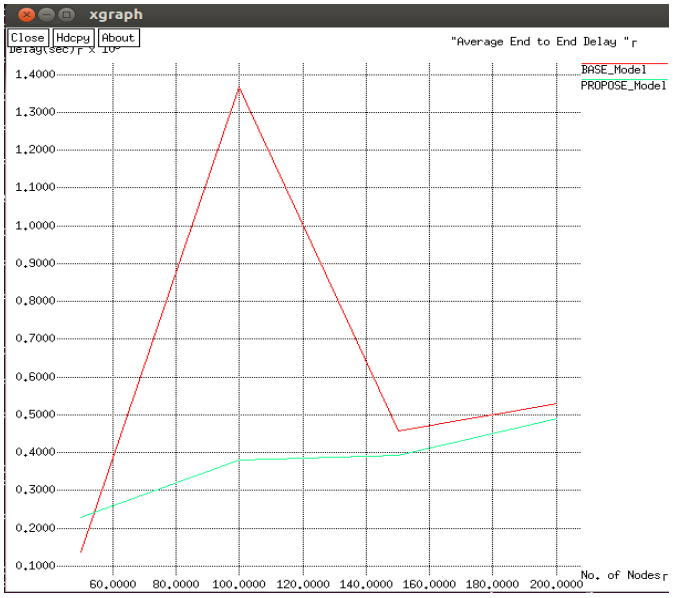

Figure7 End-to-end delay comparison

Total Packet Dropped – The failure of one or more transmitted packets to arrive at their destination is called as Total Packet Dropped. Figure shows that in term of drop packet AODV give the better performance compared to proposed protocol.

Packet Drop Ratio = Data packets sent – Data packets received

 ISSN: 2321-8169
127 – 133

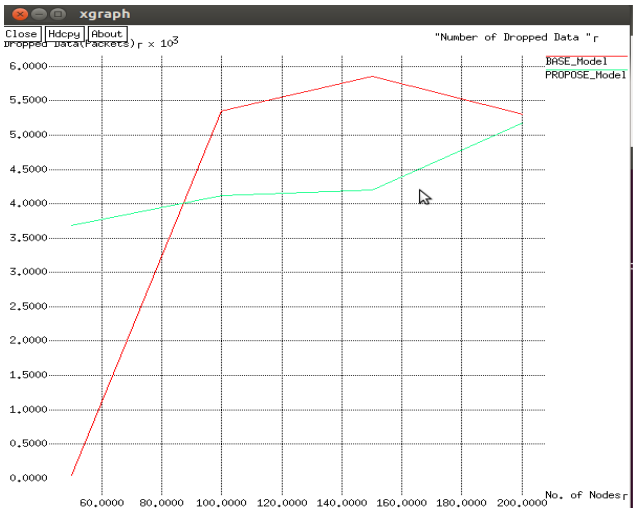

Figure8 Dropped data packets comparison

Energy Consumption

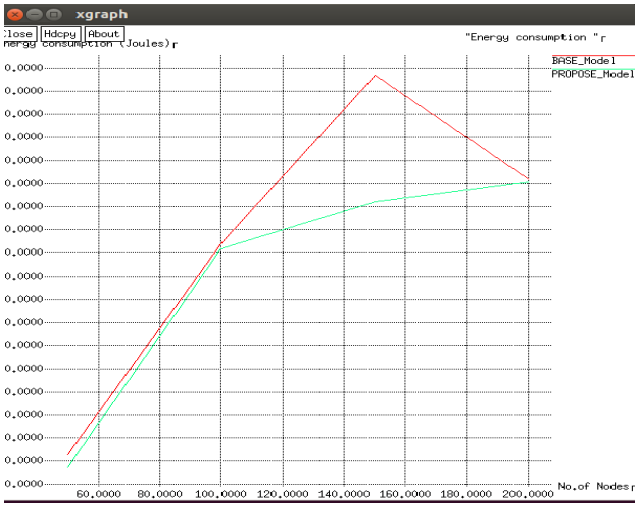

Figure9 Energy Consumption comparison

Normalized Load

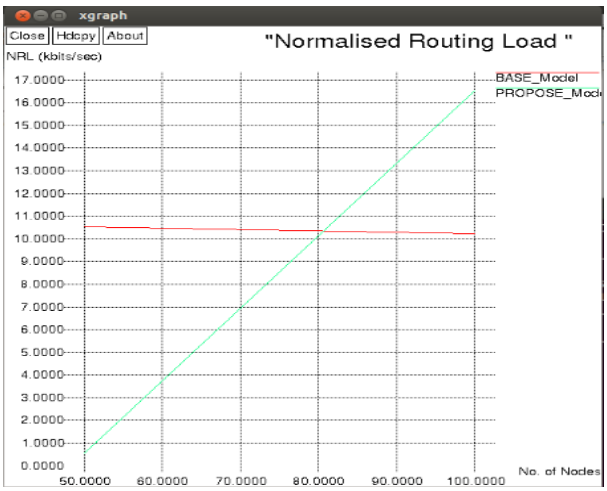

Figure10 Normalized Load Comparison

Packet Delivery Ratio (PDR) – The ratio between the numbers of packets delivered to receiver to the number of packets sent by the source is called as Packet Delivery Ratio. It denotes the maximum throughput a network can achieve. A high average packet delivery ratio is desired in the network

Packet Delivery Ratio = (Packets Received / Packets Generated) * 100

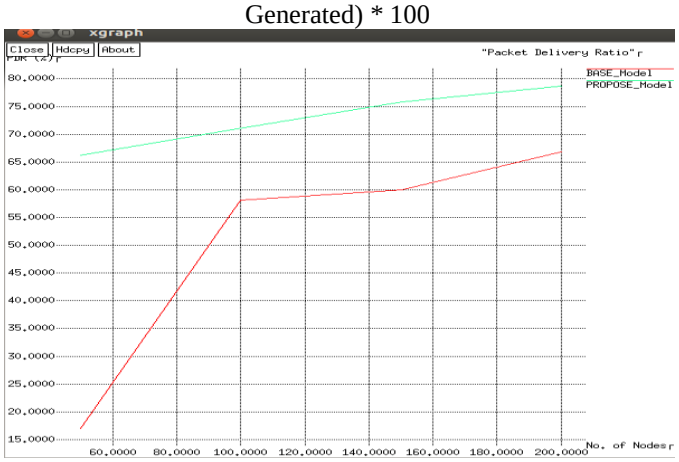

Figure11 Packet Delivery Ratio comparison

Throughput

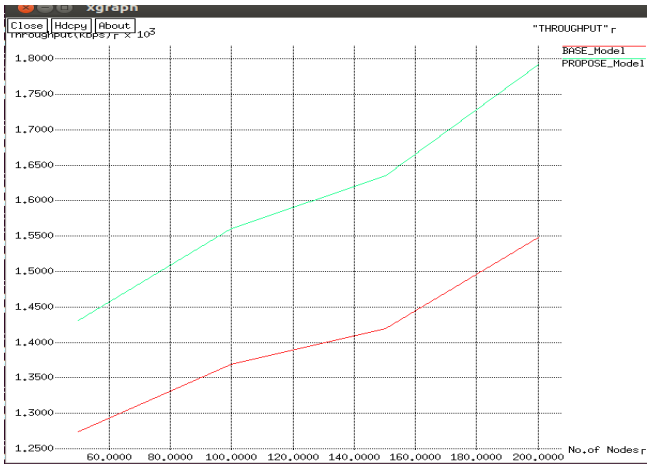

Figure12 Throughput comparison

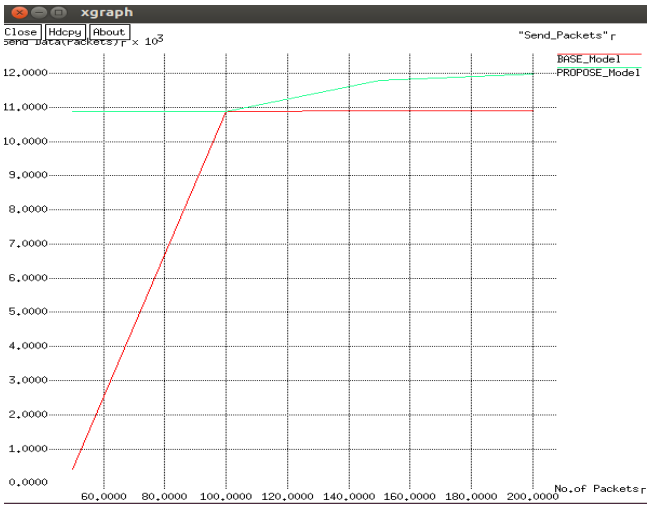

Figure13 Comparative analysis of Send packet

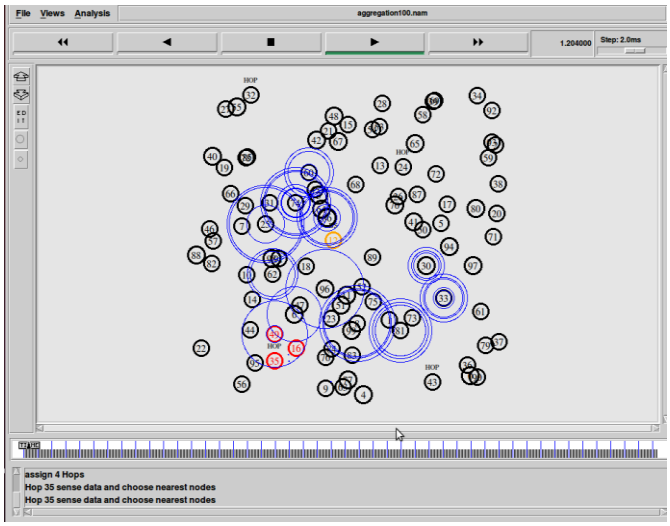

Figure14 Four hopes are assigned and hope 35 sense data, choose nearest node

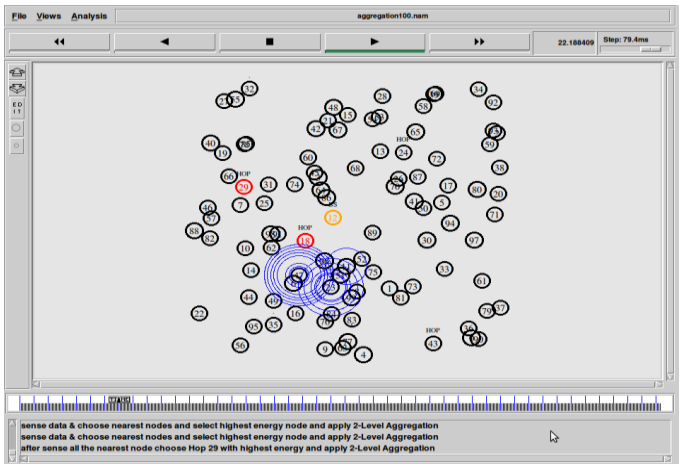

Figure15 Selection of highest energy node and 2nd level aggregation

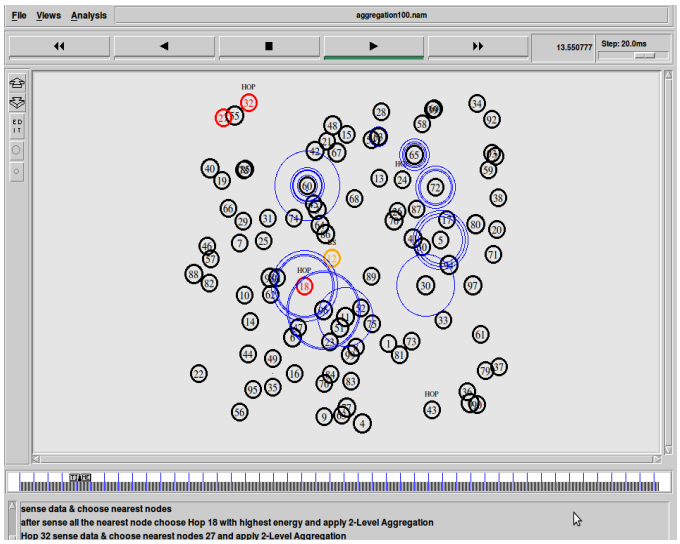

Figure16 Sense data and choose nearest node in 2nd level aggregation

V. CONCLUSION

The data's are aggregated by using clustering based energy efficient algorithm and by providing key security to the packets dynamically with time to time key value change. In this research paper there are two main domains on which work carried out successfully. First one is data aggregation but data aggregation in our work is of two levels. Another domain was security because as we know in MANET security is not up to the mark that is why unauthorized person can access the data by deploying malicious note in our existing network. It is an effective mechanism to save energy and delay provide security in WSN. The secured data aggregation can be seen access only authorized user. Using this advanced methodology, the data packets or information are transfer through the dynamic routing by according time to time key value changed securely. RSA implements two important ideas: Public-key encryption and Private- Key decryption. In RSA, encryption keys are public, while the decryption keys are private. The analysis of the results it can be inferred that efficient in-network data fusion and data aggregation can reduce the amount of communication in the network and optimize the network lifetime. Due to data aggregation techniques energy can be saved effectively and as we know energy is one of the important parameters.

REFERENCES

[1]. Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Member, "An Efficient Distributed Trust Model for Wireless Sensor Networks" IEEE, and Mohsen Guizani, Fellow, IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 5, May 2015.

[2]. Mr.Rakesh, Kr.RanjanMrs., S.P.Karmore, "Survey on Secured Data Aggregation in Wireless Sensor Network" IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems 2015.

[3]. Sumedha Sirsikar, Samarath Anavatti, "Issues of Data Aggregatiom Methods in Wireless Sensor Network: A Survey" in Proceedings of 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15) Science direct 2015.

[4]. V.Vineel Kumar, K.Ananda Brahmi, "Data Aggregation Using Synopsis Diffusion Approach In Wireless Sensor Networks" International Journal of Innovative Engineering Research (E-ISSN: 2349-882X) Vol 2, Issue 1, September 2014 .

[5]. Nanthini.D and R.A.Roseline, "Aggregation Protocols in Wireless Sensor Network- A Survey" by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 7, July 2014.

[6]. Mousam Dagar and Shilpa Mahajan, "Data Aggregation in Wireless Sensor Network: A Survey", International Journal of Information and Computation Technology, Volume 3, Number 3, 2013. ISSN 0974-2239

[7]. V.Umarani, K.Soma Sundaram, "Survey of Various Trust Models and Their Behavior in Wireless Sensor Networks", International Journal of Emerging Technology and

Advanced Engineering, Volume 3, Issue 10, pp. 180-188, October 2013.

[8]. Sushruta Mishra and Hiren Thakkar, "Features of WSN and Data Aggregation techniques in WSN: A Survey " International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

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

[10]. Kasirajan, Priya, Et Al. "Demonstration Of A Multi-Interface Multi-Channel Routing Protocol (Mmcr) For Wsns Using Missouri S&T Motes." Lcn Demo (2010).

[11]. Suat Ozdemir , Yang Xiao ,"Secure data aggregation in wireless sensor networks: A comprehensive overview" Science direct Volume 53, Issue 12, August 2009.

[12]. R. Anguswamy, M. Zawodniok And S. Jagannathan,—A Multi-Interface Multichannel Routing (Mmcr) Protocol For Wireless Ad Hoc Networks,‖ Proc. Of The IEEE Wireless Communications And Networking Conference, Pp. 1-6, Apr 2009.

[13]. S. Misra Et Al. (Eds.), Guide To Wireless Sensor Networks, Computer Communications And Networks, Doi: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.

[14]. Suman Nathy; Phillip B. Gibbons, Srinivasan Seshany, Zachary R. Anderson, "Synopsis Diffusion for Robust Aggregation in Sensor Networks" ACM Transactions on Sensor Networks, Vol. V, No. N, September 2007.

[15]. Wei Zhang, Sajal K. Das, and Yonghe Liu "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006