Multiple Data Aggregation Technique in MANET to Secure Data against Attack using Secure Protocol

Vinita Jain
M.Tech Scholar, CSE Department
SKIT Jaipur, RTU Kota

Pankaj Dadheech
Associate Professor, CSE Department
SKIT Jaipur, RTU Kota

Abstract--- The difficulties of diminishing the transmission delay and optimize the sensor lifetime is always prime research parts in the arena of wireless sensor network. By debarring the impact of routing protocol on the transmission direction of data packets, the MAC protocol which controls the time point of transmission and reception is also crucial parameter on the communication performance. In this research paper there are two main domains on which work carried out successfully. First one is data aggregation and security. In MANET security is prime concern because this network is prone to threat and data can be accessed by unauthorized person by placing false nose in network. Therefore need to integrate protocol with security algorithm so that data cannot be accessed by unauthorized person. In this paper multiple data aggregation technique used with RSA encryptions so that data must be secure. Data aggregation is a technique through which energy of network can be saved. In this technique repeated information received from node of network are dropped and useful information sent to cluster head. In this way battery life of network increased which is very crucial in these types of network. With multiple data aggregation RSA security algorithm also integrated for encryption and decryption so that uncertified person cannot able to get data.

Keywords—*Multiple Data Aggregation, Security, Cluster Head, RSA Security Algorithm, MANET*

I. Introduction

WSN consists of a huge number of sensor nodes. Each sensor node senses environmental conditions and sends the sensed data to a BS. Wireless Ad hoc Network gives a tender which gives cost constructive communication between various users [1]. It is distinguished by redistributed architecture, mobile nodes, and zestful topology which make network formation typically tedious. 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 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 [2].

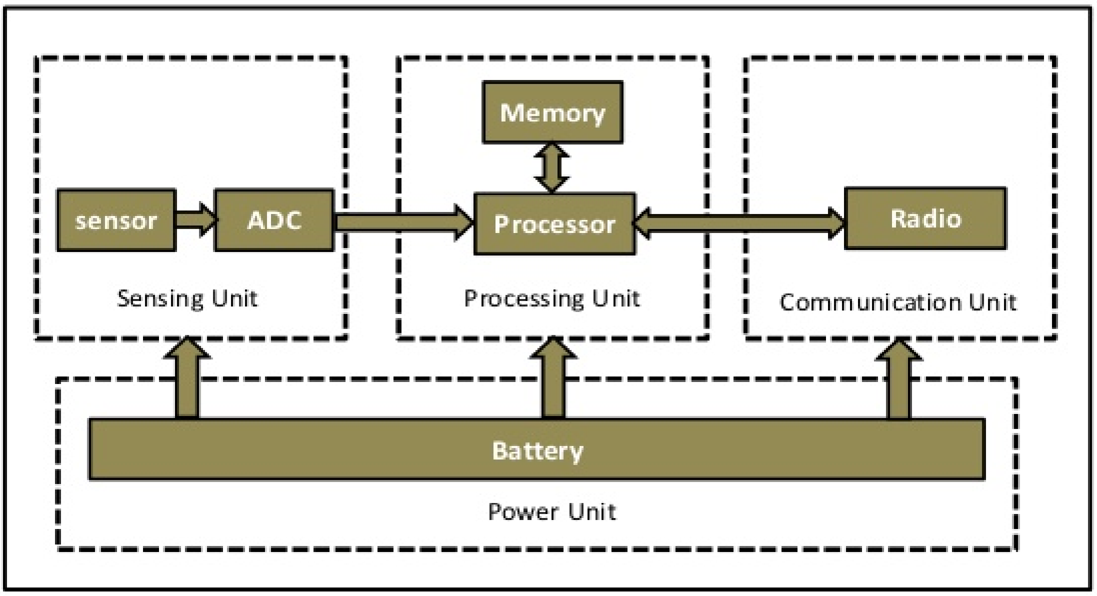


Figure1 Architecture of sensor node

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 [4].

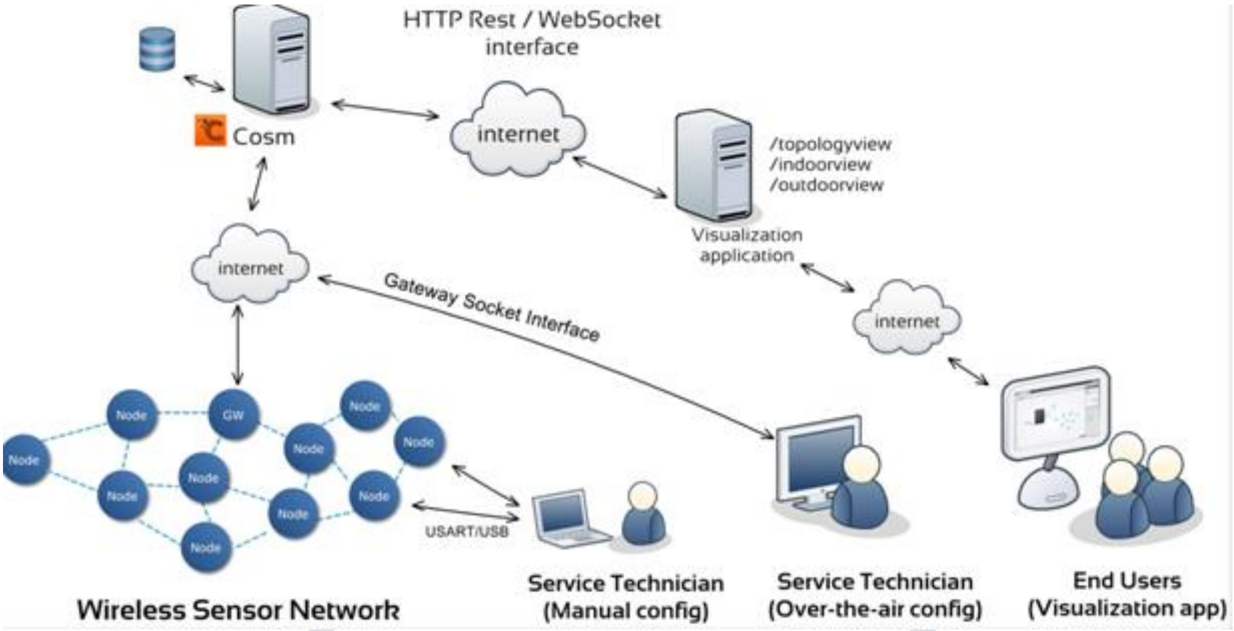

HTTP Rest / WebSocket interface
Cosm
internet
/topologyview
/indoorview
/outdoorview
Visualization application
internet
Gateway Socket Interface
internet
Node
GW
USART/USB
Wireless Sensor Network
Service Technician (Manual config)
Service Technician (Over-the-air config)
End Users (Visualization app)

Figure 2 Architecture of WSN

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 [5-6]. In the proposed multi-level data aggregation model for reliable data transmission, distributed data server is used to store and process the data. The key distribution centre is used to generate session keys and digital signature which is then used to distribute the signature to all the authenticated nodes. Data aggregation avoids the duplication and removes the similar data set while updating the final group of data based on the region along with the session. The sensors sense the data and forward it to the base station for computation [3]. The malicious node detection process is used to evaluate the nodes based on its behavior [7]. 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

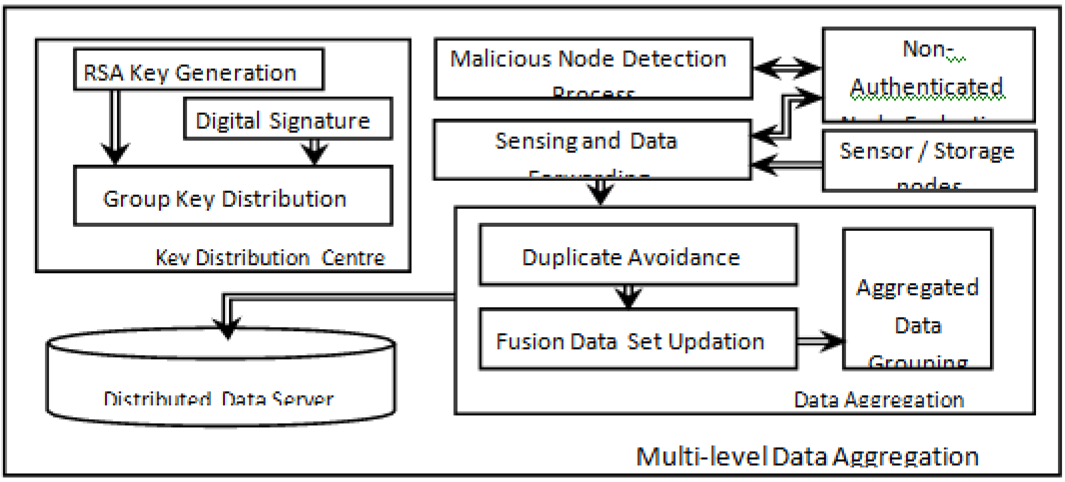


Figure 3 Multi-Level Data Aggregation System Architecture

II. METHODOLOGY

The significant enhancement in RSA algorithm practically depends upon choosing the cluster head and also selecting the node that is used to transmit the informative data. That is used to transmit the information whenever we detect any unnecessary data. However when we combine the features of MMCR algorithm it does not allow transmission of the unnecessary information in the cluster between peculiar iterations [8]. Due to this fact redundancy can be excluded in the nodes of one cluster, after these same nodes between successive iterations excluding the unnecessary data completely. We can also say that in one cluster if many nodes are having the same information, among them only one node can transmit the data at once. If any node gives repetitive output between successive iterations, it cannot transmit any information. By using this method the passage on the network can be utilized completely resulting in reduction in BW and also the most crucial factor energy that is exhausted can be minimized.

Cluster Head Selection

In our model, all nodes maintain a neighbouring table to accumulate the data to neighbours. All nodes to absent in the radio range r of the distribution node are neighbours of the node. All nodes receive the data communication in the radio range and update its neighbourhood table [10]. Then each node calculates it distances from its neighbour 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.

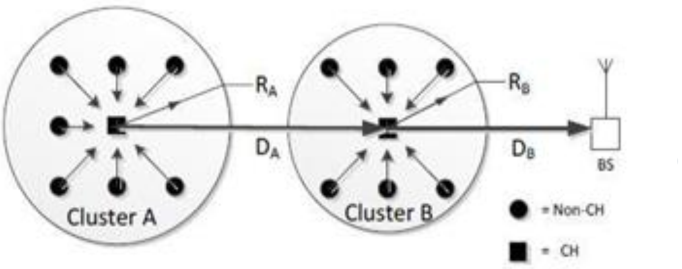


Figure 4 Communication between Clusters

Received Signal fury Information the nodes engage their CH. 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.

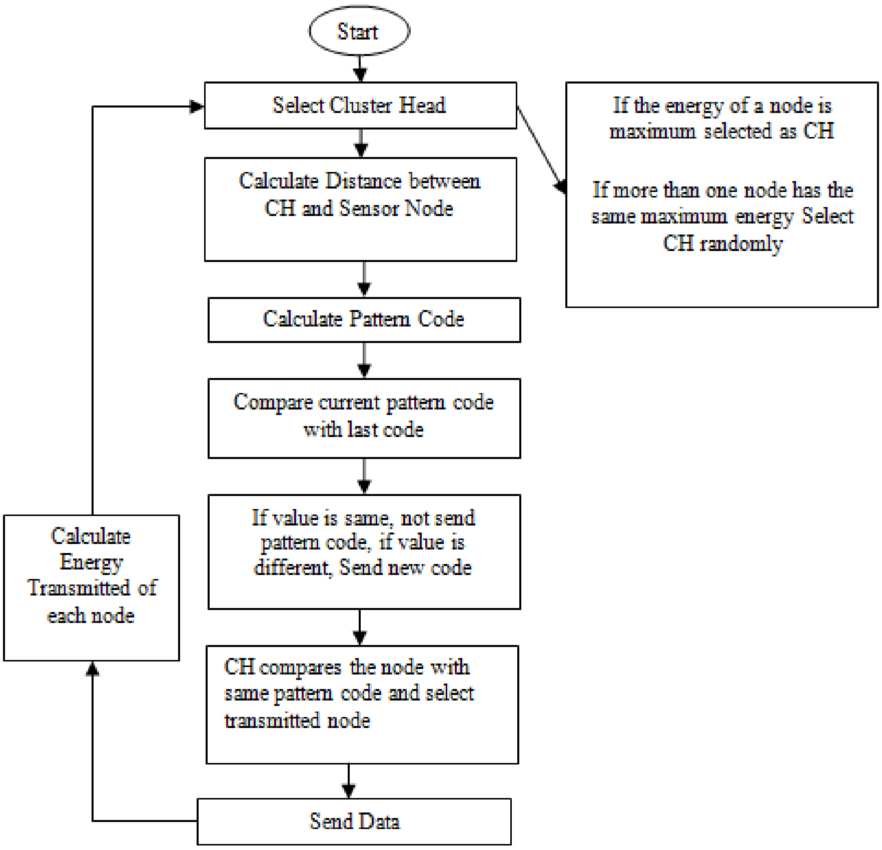

Start
Select Cluster Head
If the energy of a node is maximum selected as CH
If more than one node has the same maximum energy Select CH randomly
Calculate Distance between CH and Sensor Node
Calculate Pattern Code
Compare current pattern code with last code
If value is same, not send pattern code, if value is different, Send new code
CH compares the node with same pattern code and select transmitted node
Send Data
Calculate Energy Transmitted of each node

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 prime 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. The procedure of redefining information which is collected from various sensors is known as data aggregation [13]. There are so many threats for data therefore to secure data various security techniques can be used so that unauthorized person cannot access to the data [12]. One of the security algorithms is RSA cryptography which is very beneficial to keep privacy to the information. With pace of time hackers are so advanced and they try to get access to the data illegally for their own profit at cost of others. Therefore time to time new protocols with innovative ideas are used to keep everyone privacy.

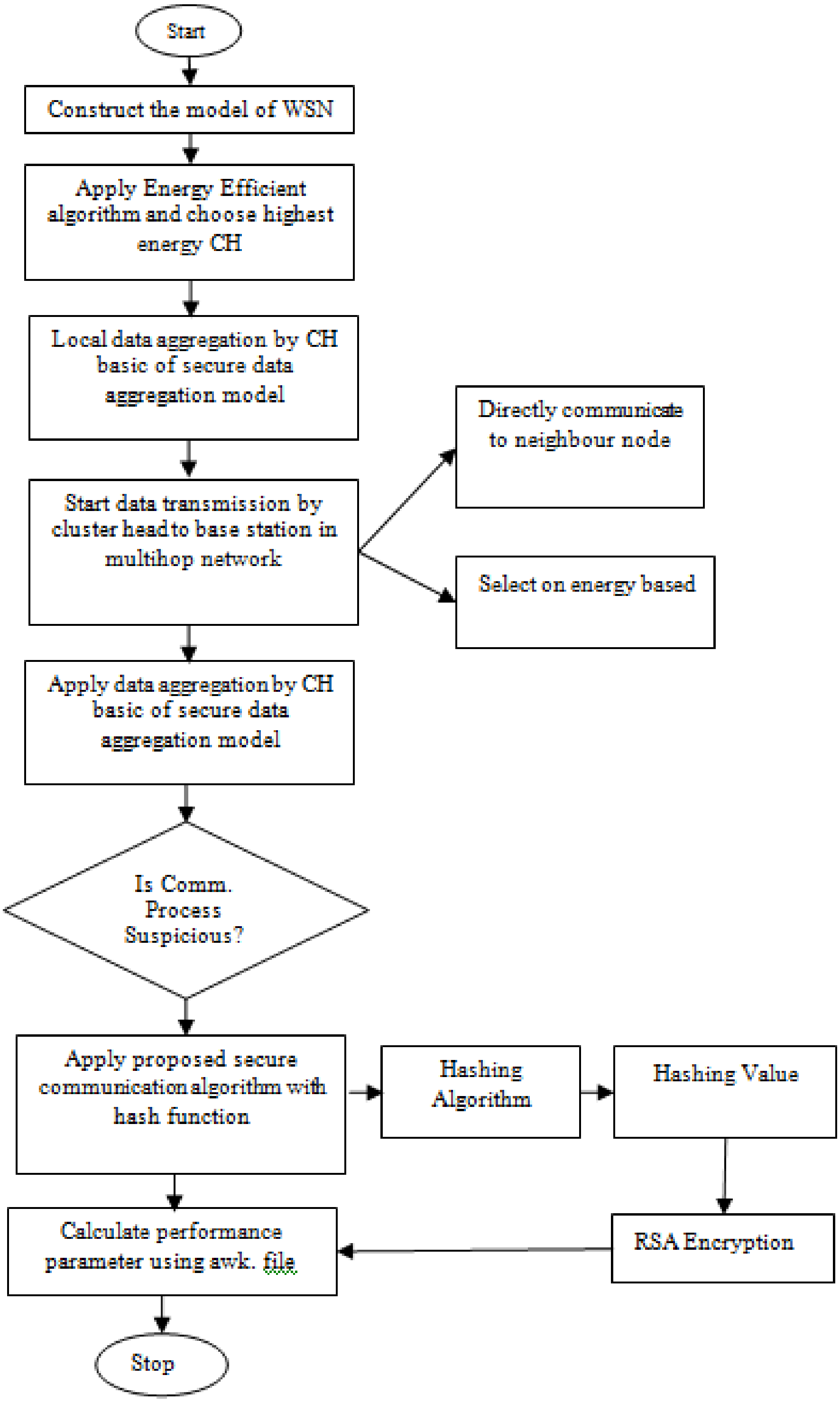

Start
Construct the model of WSN
Apply Energy Efficient algorithm and choose highest energy CH
Local data aggregation by CH basic of secure data aggregation model
Directly communicate to neighbour node
Start data transmission by cluster head to base station in multihop network
Select on energy based
Apply data aggregation by CH basic of secure data aggregation model
Is Comm. Process Suspicious?
Apply proposed secure communication algorithm with hash function
Hashing Algorithm
Hashing Value
Calculate performance parameter using awk. file
RSA Encryption
Stop

Figure 6 RSA Encryption Flow chart

III.SOFTWARE AND SIMULATION

SOFTWARE: NS 2: Multiple data aaggregation model implemented with security algorithm and that improves the performance parameters of the system. This section will depict better performance of implemented protocol in terms of energy efficiency, Throughput, PDR, average end-to-end delay of WSN with respect to base. 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.

Implemented 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	50-200 (Variable)
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/ Drop Tail/ Pri-Queue
Mobility model	Random way point
Simulation area	2000M*2000M
Link Layer Type	LL

Simulation Result: There are various parameters in networking which play an prime roll for comaritive analysis purpose among different routing protocol for example transmitted packet, received packet, energy consuption, propagation delay, overhead, throughput, end to end delay. Out of these parameters some of them are depicted below showing comaritive analysis between base model and proposed model.

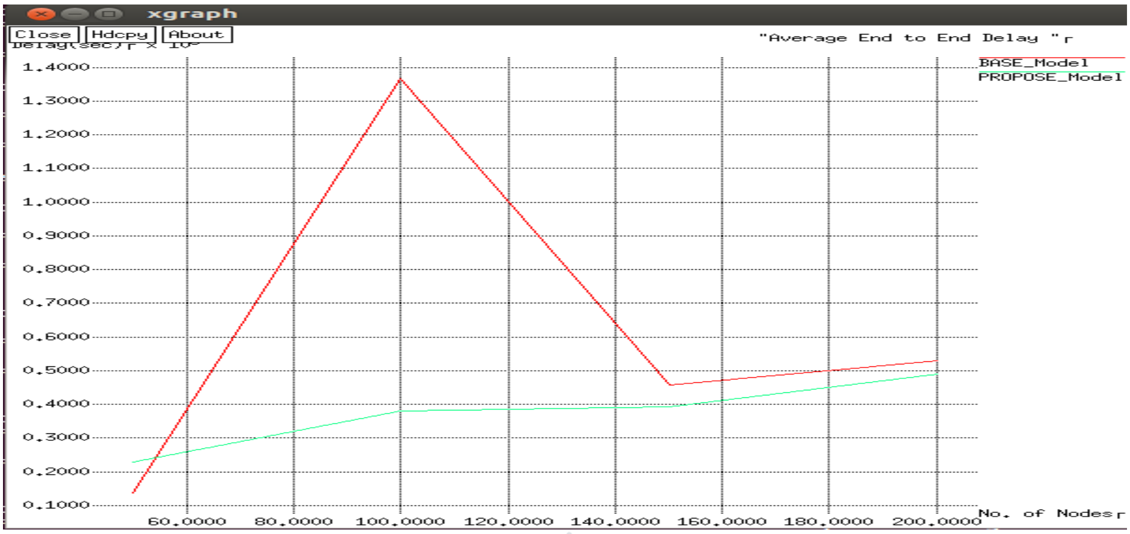


Figure7 End-to-end delay comparison

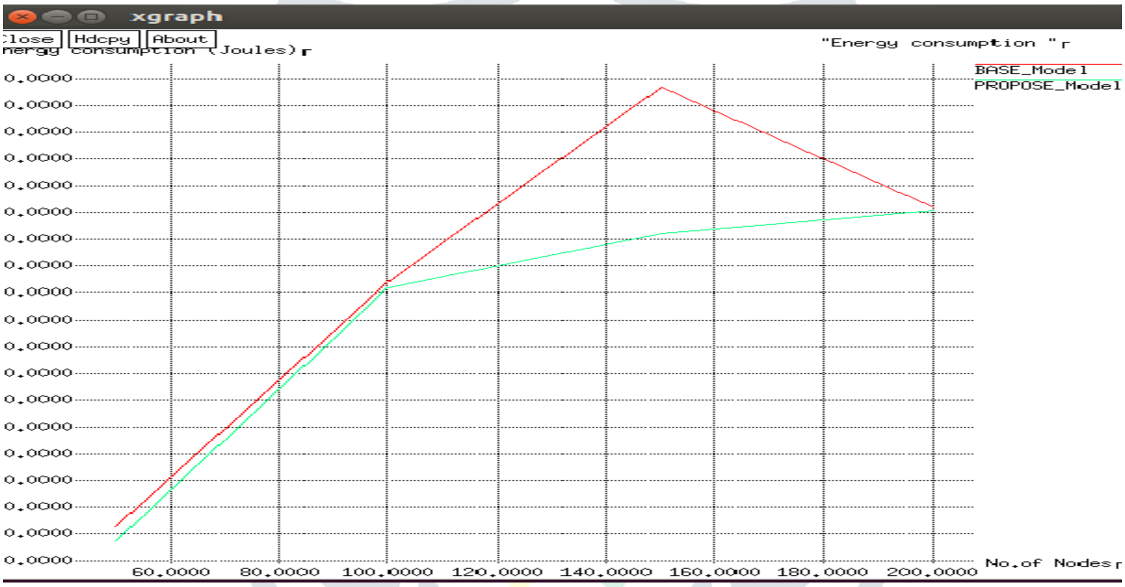


Figure 8 Energy Consumption comparisons

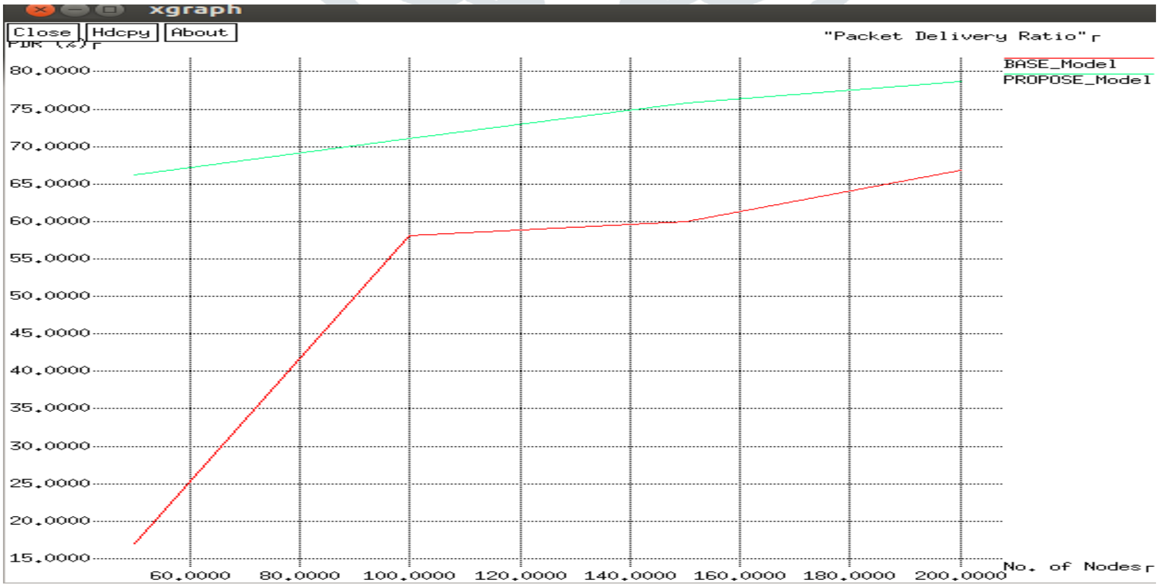


Figure 9 Packet Delivery Ratio comparison

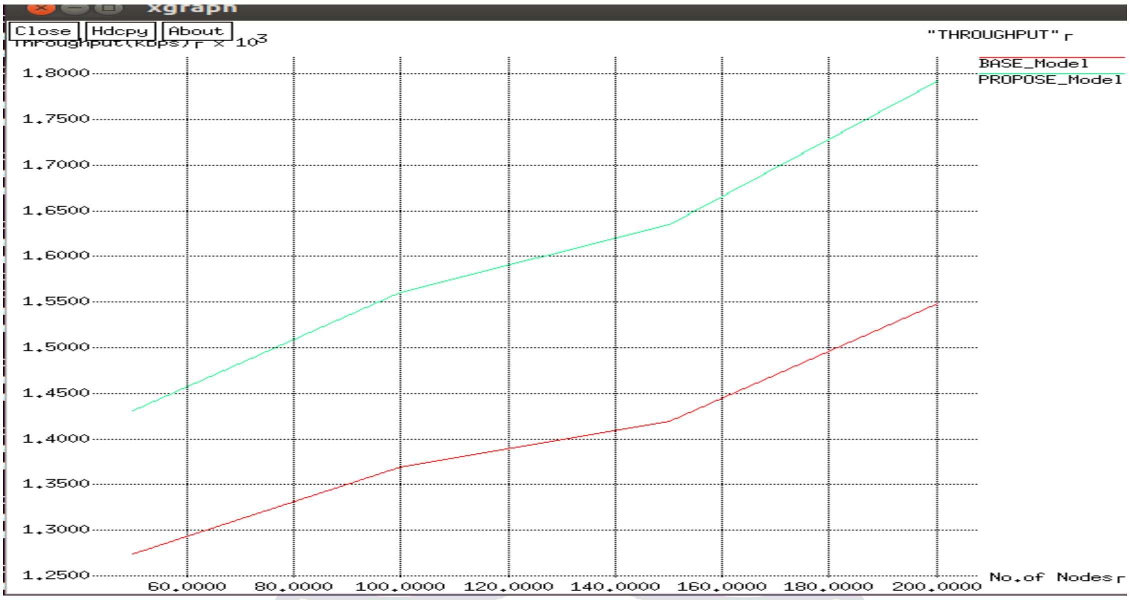
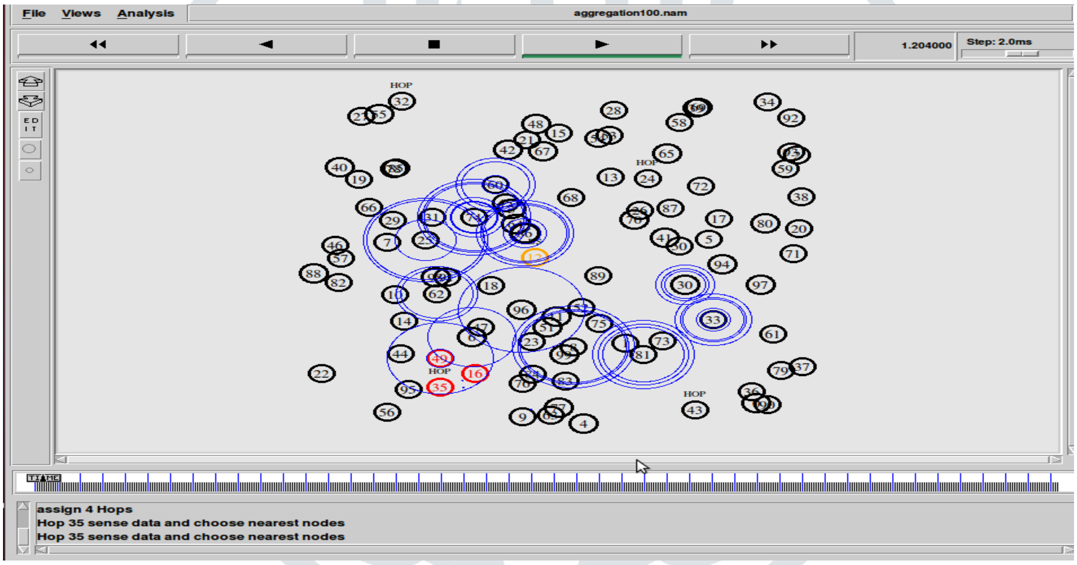
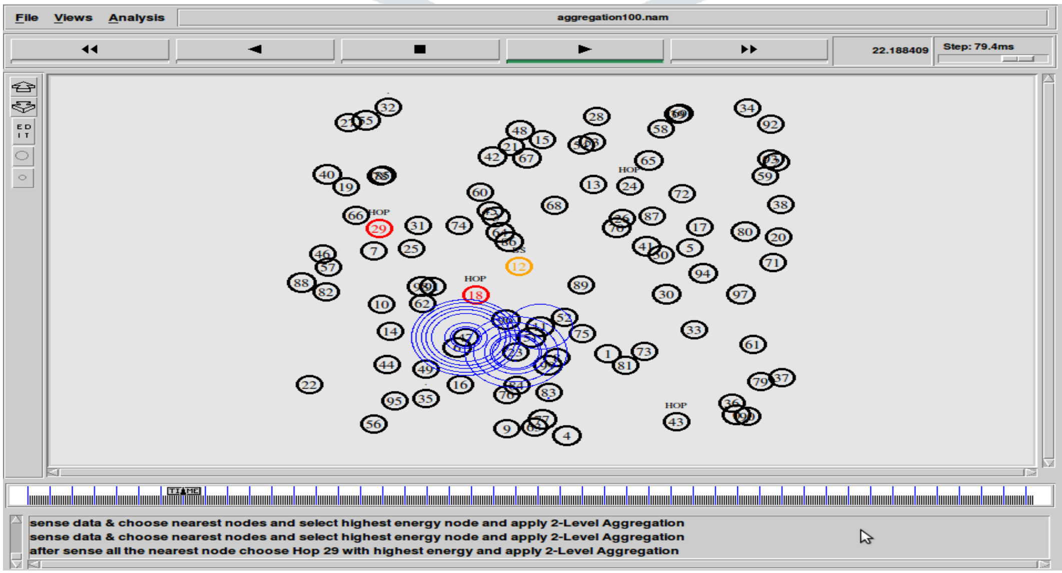


Figure 10 Throughput comparison



```
assign 4 Hops
Hop 35 sense data and choose nearest nodes
Hop 35 sense data and choose nearest nodes
```

Figure 11 Four hopes are assigned and hope 35 sense data, choose nearest node



```
sense data & choose nearest nodes and select highest energy node and apply 2-Level Aggregation
sense data & choose nearest nodes and select highest energy node and apply 2-Level Aggregation
after sense all the nearest node choose Hop 29 with highest energy and apply 2-Level Aggregation
```

Figure 12 Selection of highest energy node and 2^nd level aggregation

IV. CONCLUSION

The data's are aggregated by using clustering based energy efficient algorithm and by providing key security to the packets dynamically. In this paper multiple data aggregation is studied into detail with security algorithm. Besides this energy consumption and propagation delay also becomes prime performance parameters. Data aggregation is a tremendous mechanism through which energy can be saved and lifetime of network increase. RSA implements two prime facts: Public-key and Private-Key. In RSA, encryption keys are public, while the decryption keys are private. The implemented aggregation technique increases the lifetime of the network by making the energy optimization at individual sensor nodes as well as sink node. Energy saved effectively due to implementation of multiple data aggregation techniques. In future work two cluster head concept can be implemented to secure data and for optimization of network.

.

REFERENCES

[1]. Gaukhar Yestemirova, Sain Saginbekov, "Efficient Data Aggregation in Wireless Sensor Networks with Multiple Sinks", 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications, DOI 10.1109/AINA.2018.00029

[2]. Hassan Harb, Abdallah Makhoul, Samar Tawbi and Raphael Couturier, "Comparison of different data aggregation techniques in distributed sensor networks", IEEE ACCESS, VOL 00, NO. 00, FEBRUARY 2017, DOI 10.1109/ACCESS.2017.2681207

[3]. Sagi Sai Sruthi, G Geethakumari, "An Efficient Secure Data Aggregation Technique for Internet of Things Network", 2016 IEEE 6th International Conference on Advanced Computing, DOI 10.1109/IACC.2016.116

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

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

[9]. 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

[10]. 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.

[11]. 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.

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

[13]. 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.