Security Based Two-Level Data Aggregation Model Hash Function & RSA Cryptography Using Energy Efficient Algorithm in WSN

Ajay Singh Sikarwar[1], Kapil Sharma (Asst.prof)[2]
[1, 2] Dept of CSE
[1, 2] ITM University, Gwalior, India

Abstract- *Data aggregation(DA) becomes an effective and minimizes the number of transmission and then to save energy in Wireless Sensor Network (WSN) using proposed model. To aggregate data model by using clustering based energy efficient algorithm. Like Cluster, it simply collects all the node information and sends to the destination node or Base Station. The DA techniques employs Dynamic routing protocol and can forward packets with key security and according to time key value changed dynamically by using RSA algorithm using hash function. The resources especially energy in wireless sensor networks are quite limited. Many more applications can be deployed in WSNs and various sensors is embedded in no. of nodes, the packets generated by heterogeneous sensors or different types of applications have different parameters. Data aggregation scheme employ static routing protocols, which cannot dynamically forward packets according to network state or packet types. DA more efficient, proposed method using a RSA algorithm to implement a key based (encryption, decryption) data transmission on network. The data are aggregated using Cluster based techniques; a cryptography-based dynamic routing is support and therefore improves the efficiency of secure data aggregation model. The proposed work is to send the packets through secure routing and dynamically changed the key value according to the time. To check the simulation performance of this model using NS-2.*

Keywords- Wireless Sensor Network, Data Aggregation, Clustering-aware Energy Efficient Model, Dynamic Routing, Security.

I. INTRODUCTION

Wireless sensor networks (WSNs) have been extensively used in numerous real world applications [1], such as industrial and agricultural productions, security surveillance, medical and health services. In most applications, the WSN is composed of number of sensor nodes and one or more base stations (BSs)[2]. Most of the data aggregation schemes in a WSN used for the collection of data from the sensor nodes are either tree-based or cluster-based in which the BSs act as the central points of control and collect data from the sensor nodes in the network in a multi-hop fashion. The most common method in such approaches is to allow every sensor node to forward its own data to a BS via other intermediate nodes (called the cluster heads or the roots). Eventually, the BS will receive the data and perform the final aggregation. However, most of the approaches would suffer from a great deal of communication overheads as well as high computation cost, consuming more energy of the wireless sensor nodes and ultimately shortening the life of WSN [3].

In data aggregation (DA) process the assigned nodes collect the data packets from its neighboring nodes and forwards it to base station, this makes a massive impact on traffic as well as on the communication time. The main task of aggregation is to increase the efficiency however some other constraints that affects is security and delay. In WSN the aggregated sensor are more vulnerable to false data inject by intruders that mislead incorrect information. So secure communication is necessary as it take place before transmission data is encrypted while for aggregation protocols, it would be preferable to process the data and forward it to the next hop prior to encryption. So it is a difficult task to combine both taking in consideration that we could not apply the computing encryption protocols to wireless sensor networks due to their limitation in resources. Although there could be some compromise while adopting aggregation and encryption, both are deemed essential for a stable and accurately performing network [4].

II. RELATED WORK

Mohamed Ben et al. [5] proposed a Secure Data Aggregation Model (SDAM) aiming towards providing a secure aggregate communication at a low cost (in terms of resources). They proposed a simplistic and efficient method by adding modules able to authenticate non-legitimate nodes in the network as well as simplifying the energy in a communications to limited resources of the wireless sensor

Networks (WSN) and the impact of the use of encryption on aggregated data. The result of proposed method shows 40% improvement in the cross-layering overhead and also increase in energy efficiency.

V. Vaidehi et al. [6] proposed a secure method to process data aggregation by providing a light-weight security scheme called Combinatorial Key Distribution mechanism which consumes minimal power. The nodes in the sensor network are clustered and use dynamic cluster head for secure data aggregation. The security is achieved by appending an additional field in the packet which is a hash of the data present in the packet. The proposed scheme is simulated in OMNeT++ network simulator and provides better results in data aggregation and security than the existing schemes.

S. Siva Ranjani et al. [7] proposes the energy efficient secure data aggregation. WSN are used in many critical applications. Due to its open nature, WSN is prone to security attacks. Sensor nodes are having limited resources hence we design trust based secure communication methods. SCDA forms and maintain the cluster using ECBDA approach. CHs, node with highest energy are calculating the total trust probability. Thus the energy of every node which is involving in the data communication is saved. More nodes are giving supporting information to the CHs for long time so the fairness of trust probability is good in SCDA. Simulation results shows that their approach out performs the existing methods in energy as well as security.

Komal et al. [8] proposed a novel SDA scheme with Outlier Detection using AMAC. This scheme provides data integrity and authentication. In this also defined a tree construction and a key establishment algorithm to make our protocol complete. Integrity of outlier values is maintained by appending MAC with the abnormal messages, aggregating at the aggregator nodes and then verifying it at the BS. The protocol resists against replay, dropping and forging attacks. None of the schemes proposed in the literature provide a complete framework, including Topology construction, Key Establishment, Data Processing and Verification. In this implemented their scheme in TinyOS and also evaluated the same for memory requirement and energy consumption.

Abhilash et al. [9]proposed a model using data aggregation. With this optimize the energy use of sensor nodes in a multi-hop WSN and increase the bandwidth of network by eliminating unnecessary data packets. The model works in two steps: in first step use of Exponential Weighted Moving Average (EWMA) data aggregation technique that compares the current data value with the previous one valueto decide whether to drop or forward the packet. The second step optimizes the network even further by considering readings from neighboring sensors into the equation. The algorithm allows flexibility to adjust precision level based on user requirements. The result of work shows the reduce number of packets transmitted and the normalized energy consumed by the nodes.

III. PROBLEM STATEMENT

Data Aggregation protocols are used to eliminate redundant data transmission and thus improve the lifetime of energy constrained WSN. In WSN, data transmission took place in multihop fashion where each node forwards its data to the corresponding neighbor node which is located nearer to sink. But closely placed nodes may sense same data, above approach cannot be considered as energy efficient. So an improvement can be done over the abovementioned approach would be clustering where each node in the network sends data to cluster-head (CH) and then cluster head aggregates the received raw data and then send it to sink.

IV. PROPOSED METHODOLOGY

RSA cryptography techniques used to provide security in Ad-Hoc Demand Distance Vector (AODV) routing protocol. An RSA technique is one of the most popular examples of asymmetric cryptographic algorithm. In RSA algorithm, one can easily find and multiply large to very large prime numbers together but it is very difficult to factor their product. These very large prime numbers are used in Private and Public keys increase the complexity of the proposed approach. The security aspects being provided can be seen in these formats

Encryption and Decryption using RSA Algorithm

1) Firstly, choose the 2 prime numbers A & B.
   set L 3
   set 2powl [expr pow(2,$l)
   setscreat [expr int($2powl+)]
   then “screat:$screat”
2) Second step, Calculate M such that N = A*B.
   For {set A 0} {$A<$screat} (incr A}{
   Set elt [expr ($i+$p)%$screat]
3) Third step, select public key W such that W is not a factor of (A-1) and (B-1).
4) After that, select the private key K such that it follows equation (K*W) mod (A-1) and (B-l) = l
   Set cmg [list]
   Set key pairing group: $cag”
   Set B [expr $B+(BIAG*cmglt]

5) In next step, for encryption process calculate the cipher text ED from plain text PT such that ED = PTW mod M
6) Finally, send ED as the cipher text to the receiver point.
7) For Decryption method calculate the plain text KT from the cipher text ED such that KT = ED K

Thus we can say that the RSA is useful algorithm to obtain security in AODV protocol. RSA uses both Public as well as Private Key.

A new approach for generation of ID keys for the authentication of a node has been proposed. This proposed technique is based on cycling chain mechanism. In this mechanism any previous record of data is automatically destroyed. In other words the process of key generation is maintained independent of next value. The naming convention used for our algorithm is as follows

{Cyclic Additive Group} set of notation represent the value of source point, mediator node & sink node.

Set key pairing group:$cag
Set Hlist [list]

For {set i 0} {$i<$screat} {incri}{
Set hlv [myRand 0 1]
nk = session-key.
(Pi)s = secrete-key.
Ne = session in one Node to another Node.
Cid = for Communication & its identity node
WT = represent the values of communication node, it equals H
Token(t) = generate a token
(Y) = Message
HS(Y) = Hash messages

Generating public key and private key for Network Manager
Registration method (request secret key corresponding to its identity) after then issue a ticket to trusted node

Key-Generation scheme discuss the Dynamic-key generation which is one of our important contribution proposed, in additional information to the type of confidential information shared b/w the 2 nodes. These method requires 2 set of keys pair to be generated at each and every party side which are secondary-key (Pi)s and session key (sk)s. (Pi)s is required to generate Y values is used as a security enhancement step to generate a session keys. The node M1 wills issue the mediator node (N1) and a communication authentication once authenticated.

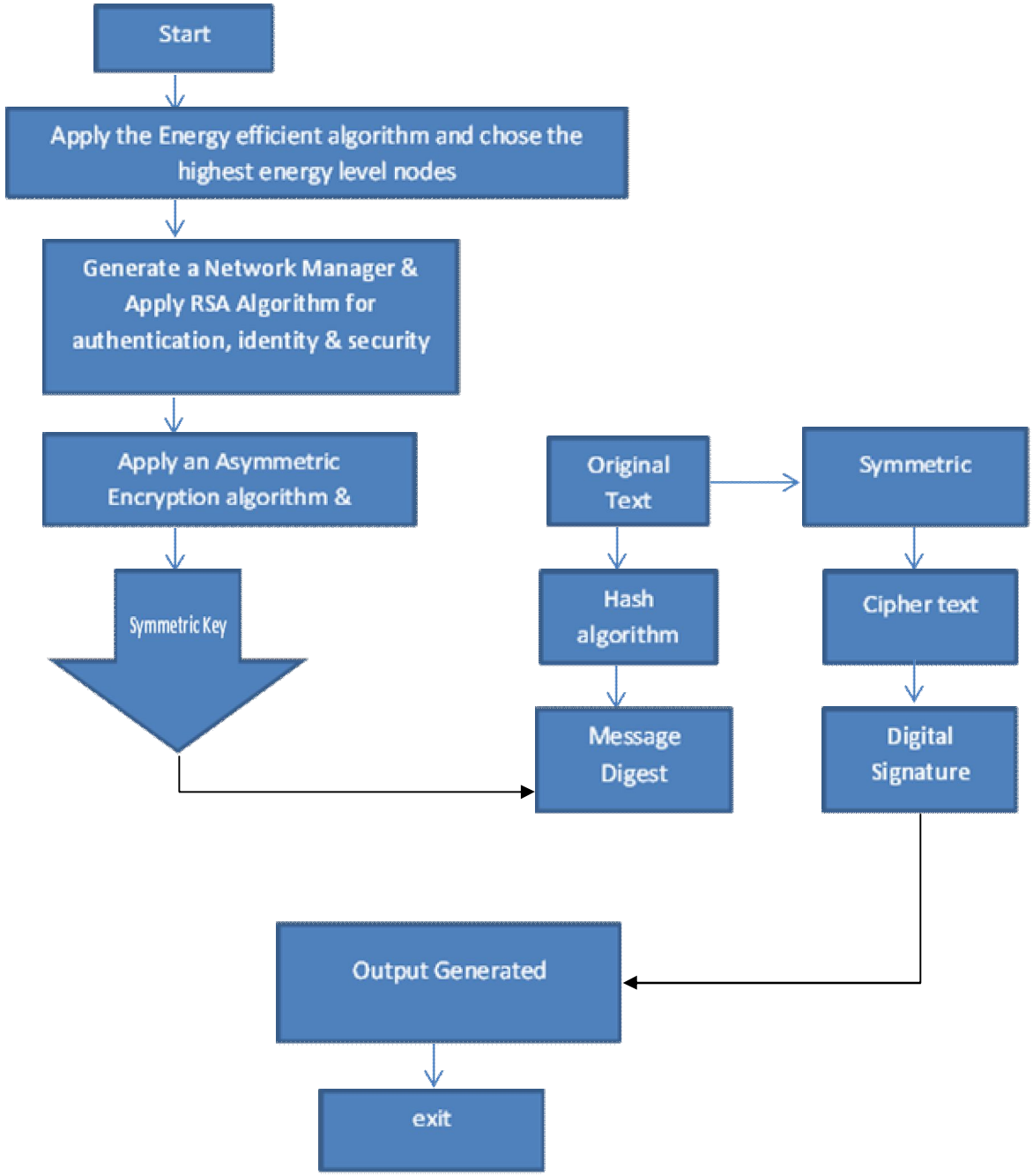

Fig.1 Flow Chart of Proposed Work Model

The following algorithms had to be implemented: Hash-Based Message Authentication Code (HMAC) HMAC is a mechanism for message authentication using cryptographic hash functions, such as MD5 or SHA-256, in combination with a secret shared key. Our implementation makes use of the available implementations for the underlying hash functions and needs only to append the resulting byte streams correctly according to the protocol security algorithms.

The proposed protocol is based on shared secret key technology. An approach is assumed to set up pair-wise secret keys. Source and Destination nodes both are not compromised. AODV routing protocol assuming that bi-directional links which means if a node A is able to receive packet transmitted directly by some node d then node d is also capable of receiving packet directly transmitted by node c. The notation used to describe cryptography operations is as follows. c and f are source and destination nodes respectively. KS denotes the secret key shared between nodes E and S. Each node holds the MAC (hash function based message

authentication) algorithm. The Hash function techniques denote the computation of the message authentication security code of message N using secret key KS between nodes c and f.

- Starting process of the communication between 2 nodes. Client send the request the server side and server send the acknowledge. Transmission will be sone between Network Manager and 0 node 1 is a intermediate node between transmission process.
- The communication in WSN network starting to sending and receiving the Data using authentication process generated secret key, issuing the tickets.
- The packet dropping during communication process between network manager and a WSN node. When client generate the request message to server then server generate the reply message with in same window size. If that time client drops the packet that means, it's a suspicious node.
- After that the authentication process is completed after then generates a request message to issuing the ticket or certificate authentication. Node request secret key to generate a request of a valid CA or ticket
- The node 0 Authentication process of a node and checking its corresponding identity node and if authentication process is completed then network manager generates a secret key of a node 0.
- After completion the Trusted or untrusted process node network manager issue a ticket, and authenticated node send the service request for a valid session key
- The process of Registration, Authentication, Validation, trusted node all process is completed then generates a valid key session.

V. PERFORMANCE EVALUATION

We are modified some files in ns-2 for implement method

- Mobilenode.cc , Mobilenode.h
- Packet.cc, Packet.h
- Cmu-trace.cc, Cmu-trace.h
- prequeue.h, prequeue.cc
- Ns-lib.tcl, ns-mobilenode.tcl, ns-agent.tcl, ns-default.tcl, ns-packet.tcl
- Makefile.in, Makefile.cc.

The result performance of proposed model for secure data aggregation is compare on different parameters as:

1) Average End-to-End Delay :

The average time packets take to traverse the network. This is the time from the generation of the packet by the sender up to send at the destination application layer and expressed in second. It therefore include all the delay in the network such as buffer Queue, transmission and delay induced by routing protocol activities and MAC control data exchanges.

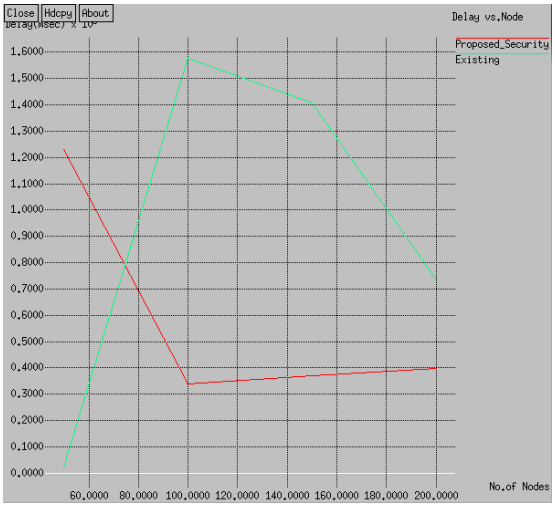

Fig.2 Average End-End Delay Ratio is compared with Proposed Model and Base Model

2) Energy consumption :

Energy consumed by the sensor nodes in transmission of packets, receiving packets & forwarding of the packets in the WSN. When the value of energy consumption is low, it means the algorithm achieves high energy efficiency which is good for the Routing protocol.

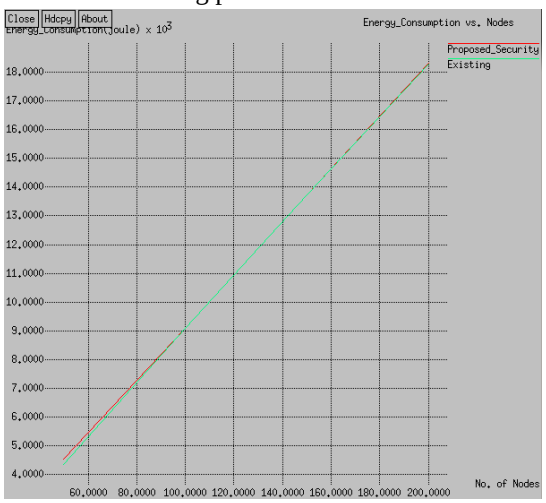

Fig.3 Energy Consumption is compared with Proposed Model and Base Models

3) Packet Delivery Ratio (PDR) :

The ratio between the numbers of packets delivered to the receiver and the number of packets sent by the source. It represents the maximum throughput that the network can

achieve. A high average packet delivery ratio is desired in a network.

$$PDR = 100 \times \frac{\text{Received packets}}{\text{generated packets}}$$

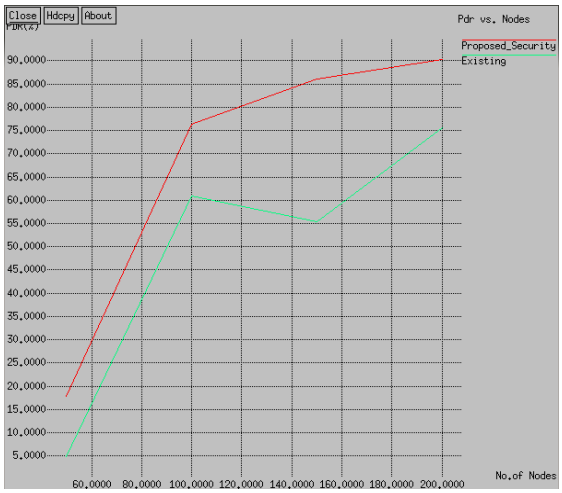

Fig. 4 PDR Ratio is compared with Proposed Model and other Models

4) Total Packet Dropped:

The failure of one or more transmit packets to arrive at their destination.

Packet Drop Ratio = data Packet Sent - data Packet Receive

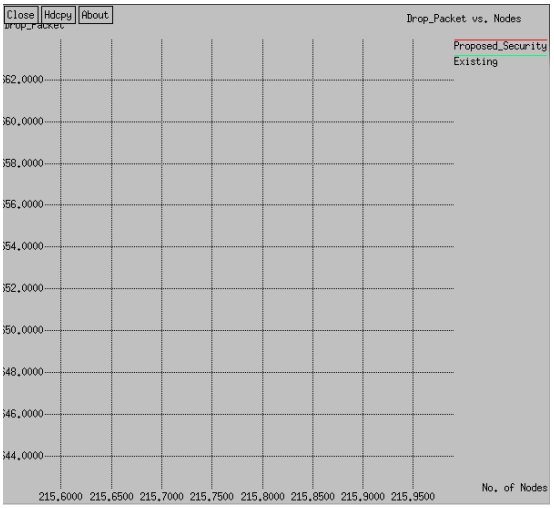

Fig. 5 Number of Dropped Data is compared with Proposed Model and Base Model

5) Normalized Routing Load (Normalized Routing Overhead) :

It is defined as the total number of routing packet transmitted kilo bites per data packet. It is calculate by dividing the total no. of routing packets sent (includes forwarded routing packets) by the total number of data packets received.

$$NRL = \frac{\text{Routing packets}}{\text{Received packets}}$$

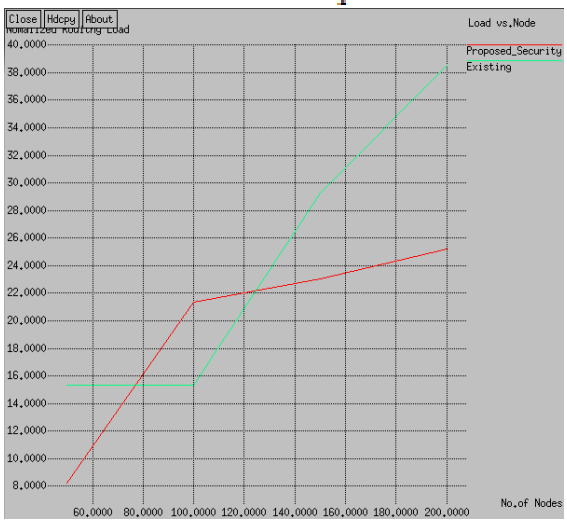

Fig. 6. NRL Ratio is compared with Proposed Model and other Models

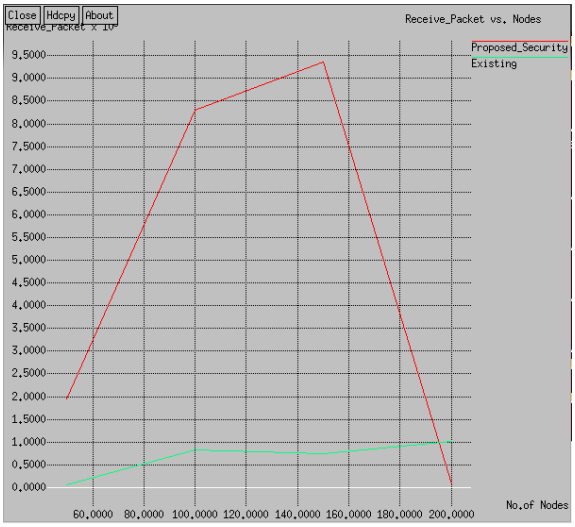

Fig. 7. Receive Packets is compared with Proposed Model and other Models

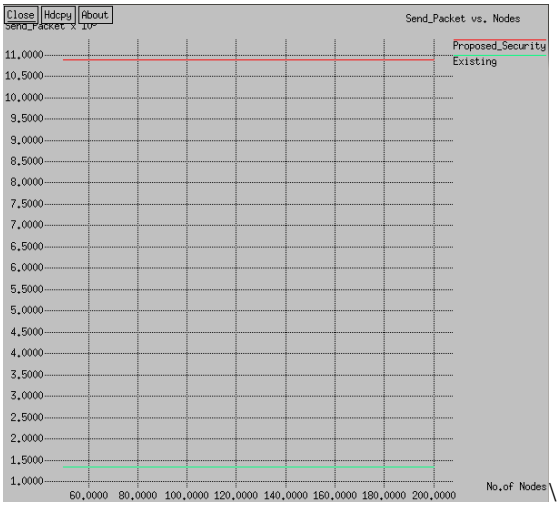

Fig. 8. Send Packets is compared with Proposed Model and other Model

TABLE I. SIMULATION PARAMETERS

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	20 seconds
Transmission range	450m
Examined protocol	AODV,RSA, Hashing
Interface Queue Type	Queue/DropTail/PriQueue
Mobility model	Random way point
Simulation area	2000M*2000M
Link Layer Type	LL

TABLE II. COMPARISON TABLE BETWEEN PROPOSED MODEL WITH EXISTING MODEL

Existing Model	Energy(Joule)	PDR (%)	Delay(msec)	NRL(kbits/sec)	Send Packet	Receive Packet	Dropped Packet
50 Nodes		4.95	24.61	15.36	1353.00	67.00	1224
100 Nodes		60.98	1575.66	15.34	1353.00	825.00	618
150 Nodes		55.36	1408.72	29.28	1353.00	749.00	781
Proposed Algorithm	**Energy(Joule)**	**PDR (%)**	**Delay(msec)**	**NRL(kbits/sec)**	**Send Packet**	**Receive Packet**	**Dropped Packet**
50 Nodes		17.91	1229.64	8.26	10877.00	1948.00	9317
100 Nodes		76.31	337.90	21.38	10877.00	8300.00	4870
150 Nodes		86.00	369.94	23.05	10877.00	9354.00	3968

VI. 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. It is an effective mechanism to save energy and delay provide security in WSN. PDR is improved by using this technique. Transmission of packets will be increased in WSN. Duplication will be avoided. The secured data aggregation can be seen access only authorized user. Using this methodology, the data packets are transfer through the dynamic routing by according time to time key value changed securely. 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. The clustering algorithms are scalable and a distributed implementation of the clustering algorithm terminates in finite time. Good clustering can lead towards efficient heuristics for routing protocols. Structural similarity can be an efficient metric to divide a large dense network into manageable clusters.In future work this system can be deployed in real world IoT environment containing smart sensors, constrained devices and smartphones with real time application. Such deployment helps to deeply study of ECSM and evaluate significance of this system with confidential application.

REFERENCES

[1] M.Liu, N.Patwari, A.Terzis Special issue on sensor network applications. Proceedings of IEEE, 2010.

[2] T.Ko, J.Hyman, E.Graham, M.Hansen, S.Soatto, D.Estrin Embeded imagers, Detecting and Localizing and recognizing objects and events in natural habitats, Proceedings of IEEE, 2010.

[3] Mingxin Yang "Constructing Energy Efficient Data aggregation Tree based on Information Entrophy in Wireless Sensor Networks" Proceeding of IEEE, 2015.

[4] Karthikeyan, B., Velumani, M., Kumar, R., and Inabathini, S.R.:'Analysis of data aggregation in wireless sensor network', in Editor (Ed.)^(Eds.): 'Book Analysis of data aggregation in wireless sensor network' (IEEE, 2015, edn.), pp. 1435-1439.

[5] Mohamed Ben Haj Frej, Khaled Elleithy "Secure Data Aggregation Model (SDAM) in WirelessSensor Networks" 14th International Conference on Machine Learning and Applications, IEEE 2015.

[6] V. Vaidehi, R. Kayalvizhi, N. Chandra Sekar "Secure Data Aggregation in Wireless SensorNetworks" Proceedings of IEEE, 2015.

[7] S. Siva Ranjani, Dr. S. Radhakrishnan and Dr. C.Thangaraj "Secure Cluster based Data Aggregation in WirelessSensor Networks" International Conference on Science, Engineering and Management Research (ICSEMR) IEEE, 2014.

[8] Komal Bharuka, Devesh C.Jinwala "A Secure Data Aggregation protocol for Outlier Detection in Wireless Sensor Networks Using Aggregate Message Authentication Code" IEEE .

[9] Abhilash L N, Devaansh Goenka, Chetan Kumar "Dynamic Data Aggregation for Energy Optimizationin Multi-Hop Wireless Sensor Networks" Proceedings of IEEE, 2014.