To develop a secure energy efficient routing protocol for improvement in localization in MWSN

Manpreet Kaur, Er. Jasdeep Singh Mann

M.Tech Scholar, Assistant Professor
Bhai Maha Singh College of Engineeirng and Technology,, Sri Muktsar Sahib, Punjab

Abstract*— In the proposal an approach is defined for energy efficiency and reduction in data dropped in the WSN network. In Data Aggregation algorithm a subset is defined, in which if a single node in that subset is died out then the whole subset have to be replaced. A modification in the data aggregation algorithm is made to achieve the objectives of the research in which energy efficiency is improved and security algorithm is embedded. In this scheme the optimization is done in the existing data aggregation scheme so that the drops in the network may be reduced. In this way the data dropped due to energy dissipation is reduced. Using this approach the data dropped and other Quality parameters are also improved like, delay, load and throughput etc as defined in results and discussion. From the above defined results it may be clear that the proposed algorithm is more secure and efficient as compare to existing algorithms of data aggregation. In case of scalability the proposed results are better than that of the existing data aggregation technique.

***Keywords*-WSN,data aggregation,clusters,localization,mobility.**

I. INTRODUCTION

Wireless Sensor Network consists of hundreds of low cost, energy and computational power sensor nodes and has achieved a widespread applicability in many application domains ranging from precision agriculture and office automation and animal welfare to home. Although sensor network implementation have initiated to appear, the industry still be prepared for the maturing of this technology to realize its full benefits.[1] Due to the limited communication range of sensors, large geographical areas cannot be covered. In addition, a large number of Internet subscriptions are needed to connect cluster heads or base station of each cluster to the Internet in order to relay data from fields to users through Internet. As each sensor network has an individual Web interface, users do not have a complete view of different geographic sensor fields. A large scale sensor network with a common application interface is, therefore, significantly required. In this research, we investigate a large scale heterogeneous wireless network consisting of three overlay networks:

(1) sensor network
(2) Wi-Fi meshed network and
(3) an infrastructure network plane, such as a Wi-Max.

The main constraints to large scale commercial adoption of sensor networks have been the lack of available control and network management tools. Such tools include the ability to determine the degree of data aggregation prior to transforming it into useful information, since data aggregation reduces the number of communications and energy consumptions, especially in dense sensor deployment, by aggregating redundant data packets in intermediate nodes[2]. Designing an efficient data aggregation technique is, therefore, very important to efficiently use the resources by reducing communications among nodes. Most existing data aggregation techniques are, however, not designed for large scale WSNs and do not consider the tradeoff between energy efficiency, end-to-end delay and data accuracy. Static time driven monitoring provides user with highly detailed and redundant information. For instance, temperature information from each sensor of a field is highly redundant, which causes the depletion of sensor energy very fast.

II. ROUTING IN WSN

Routing in WSNs is a very challenging problem due to the inherent characteristics which differentiate such networks from other wireless networks such as ad hoc networks and cellular networks . In recent years, many algorithms have been proposed for the routing issue in WSNs. The minimum energy routing problem has been addressed. The minimum total energy routing approaches in these papers are to minimize the total consumed energy. However, if all traffic is routed through the minimum energy path to the destination, the nodes along that path will run out of batteries quickly rending other nodes useless due to the network partition even if they do have available energy. Instead of trying to minimize the total consumed energy on the path, the objective is to maintain the connected network as long as possible. If sensor nodes consume energy more equitably, they continue to provide connectivity for longer, and the network lifetime increases [3]. Crucial to the success of ubiquitous sensor networks is the availability of small, lightweight, low cost network elements, called Pico nodes. These nodes must be smaller than one cubic centimeter, weigh less than 100 grams, and cost substantially less than 1 dollar (US). Even more important, the nodes must use ultra-low power to eliminate frequent battery replacement. A power dissipation level below 100 microwatts would enable self-powered nodes using energy extracted from the environment, an approach called energy scavenging or harvesting [4]. As sensor networks have specific requirements on energy saving, data-oriented communication, and inter-connection between non-IP and IP, therefore sensor network dedicated routing protocols may be required, for energy efficient routing scheme. In WSN there are the routing protocols that minimize the used energy, extending subsequently the life span of the WSN. Energy awareness is an essential in routing protocol design issue.

III. EXISTING SECURE DATA AGGREGATION SCHEMES

Single Aggregator Model

In this model, the aggregation process takes place once between the sensing nodes and the base station or the external user. In other words, all individual collected data in the WSN travels to only one aggregator point in the network before reaching the querier. This aggregator node should be powerful enough to perform the expected high computation and communication. The main role of the data aggregation might not be satisfied fully since redundant data will still travel in the network for a while until they reach the aggregator. This model is useful when the network is small or when the querier is not in the same network. However, large networks are not suitable places to implement this model especially when data redundancy at the lower levels is high. The data aggregation schemes that fit in this model can be divided into two categories: whether they have a verification phase or not.

Multiple Aggregator Model

In this model, collected data in the WSN are aggregated more than one time before reaching the last destination (querier). This model achieves greater reduction in the number of bits transmitted within the network especially in the large WSNs. The importance of this model appears as the network size is getting bigger especially when data redundancy at the lower levels is high. The data aggregation schemes that fit in this model can be divided into two categories: whether they have a verification phase or not.

A WSN is a special type of network. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes.

IV. WIRELESS SENSOR AND ADHOC NETWORKS

WSANs are widely believed to be of great use in many current and forthcoming applications panning diverse domains including environmental monitoring, battle field tasks and tracking animals, equipment and humans. WSANs are formed using tiny nodes that have onboard a processor, memory, wireless transceiver and batteries. These nodes are typically deployed in some ad-hoc manner and self-organize into a network that supports queries from an outside user. The nodes have limited computational power, memory, communication speeds and battery capacity. Conserving battery capacity is more important than optimizing performance metrics and thus most existing algorithms for wired networks are not feasible for WSANs. A key infrastructural component of WSANs is a medium access control (MAC) algorithm. A MAC algorithm allows nodes to access the shared wireless transmission medium efficiently.

There are many ways to classify wireless MAC protocols. One way is to divide them into contention-based, contention-free and hybrid protocols. Contention-based protocols allow nodes to access the medium with very few restrictions. Contention-based protocols often incorporate strategies to reduce the number of collisions, like the DCF in the IEEE802.11 family. Contention-free protocols (attempt to) prevent contention during packet transmission by explicitly scheduling packets. Frequency division multiple access (FDMA), code division multiple access (CDMA), and time division multiple access (TDMA) are all contention-free MAC protocols. Of these TDMA is considered the most suitable for WSAN nodes. Hybrid protocols attempt to combine the advantages of contention-free and contention-based protocols by allowing an initial contention period which is used by nodes to reserve time slots and then a contention-free period during which nodes that with reserved slots transmit their data without collisions.

Some WSAN MAC protocols are TDMA based, while others are contention-based protocols. TDMA based protocols are intrinsically more energy efficient due to the absence of collisions. However, this is hard to do in a distributed manner. Contention-based MAC protocols for WSANs can be further classified as synchronous and asynchronous. In synchronous approaches like SMAC, TRAMA and ADV-MAC, nodes synchronize their sleep-listen schedule with the neighbours. A synchronous protocol (e.g. BMAC, Wise MAC, and XMAC) allow nodes to have independent sleep-listen schedules, but with fixed-length sleeping periods. A sender having data to send must precede the data packet with an extended preamble (at least as long as the sleep period of the receiver). Typically, asynchronous protocols perform worse in heavy loads. This is due to lack of clock synchrony and also due to the higher latency and lower throughput caused by the long preambles preceding data packets. Early synchronized protocols like SMAC do-not perform well at high loads because of fixed duty cycles. Hybrid protocols can achieve better performance by keeping the contention phase much smaller than the data transmission phase, and thus reducing collisions, latency and energy wastage. A recent algorithm called Advertisement-based TDMA Protocol (ATMA) was shown to outperform SMAC, TMAC and ADV-MAC. Later AdAMAC improved on ATMA by prioritizing packets that failed to reserve a slot in a frame. Many protocols divide frames in two parts, a Contention Window (CW) in which nodes contend to reserve timeslots and a Data Window in which packets are sent without contention or collisions. The size of the contention window is key in determining the efficiency of the MAC algorithm. Protocols like SMAC use a fixed contention window. However it is intuitively clear that varying the contention window leads to better performance.

V. ATMA IN WSN

Time in ATMA is divided into frames. Each frame begins with a SYNC period, followed by an advertisement period and ending with a data period. The SYNC period is used for loose synchronization between nodes. The advertisement period is contention-based, and used for advertising for data and for reserving data slots. The data period is divided into slots for data exchange and is accessed in a contention-free manner. The

method of synchronization is the same as in S-MAC [4]. A frame is on the order of a second, which is 104 times normal clock drifts. The SYNC and advertisement periods are contention-based, and, as such, these small drifts do not prevent the exchange of packets. To minimize the effect of these clock drifts in the contention-free data period, we set the data slots to be slightly larger than the duration of a data and an ACK packet. Also, the sending nodes begin transmitting after a small offset. Thus, small clock drifts do not affect the synchronization.

A. Advertisement Period

The advertisement (ADV) period is divided into many small slots, the size of which depends on clock resolution. The size of each ADV packet is a multiple of the slot duration. Each ADV packet contains the ID of the receiver and the chosen data slot number of the data period. All nodes are awake during this period. Each node having data to send randomly selects a slot at the beginning of the ADV period and initializes a timer to that slot value. When the timer reaches zero, the node transmits an ADV packet and waits for an acknowledgement from the intended receiver. If the intended receiver receives the ADV packet successfully, it replies with an advertisement acknowledgement packet, or A-ACK, that contains its own ID and the data slot number. Successful transmission of an ADV and its A-ACK will ensure that all nodes in the two hop neighborhood are aware of which data slots are being used. Hence, different senders will choose unique slots, preventing collisions in the data period. If an intended receiver node receives an ADV packet and knows that the selected slot is already occupied by another node, it does not send an A-ACK. If a node that has data to send and is waiting to transmit its ADV hears another transmission, it will freeze its timer and wait for the entire transmission (ADV and A-ACK) to be over. Then, it will resume its timer again and transmit its ADV packet when the timer expires if there is time left in the ADV period for its ADV packet transmission.

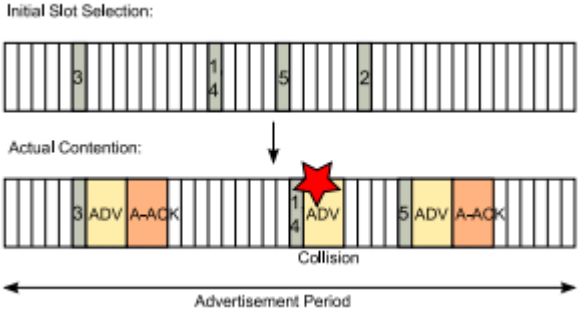

Fig 1: Examples of the operation of the advertisement period. The numbers in the slots indicate the node IDs of nodes choosing those slots.

Fig 1 shows an example of the operation of the ADV period. In the example, nodes with index numbers from 1 to 5 select random slots and initialize their timers. Node 3 selects slot 6, nodes 1 and 4 both selects slot 16, and so on. When the timer of node 3 reaches zero, it transmits its ADV packet with the ID of the intended receiver and the chosen data slot number. Other nodes will hear this transmission and will freeze their timers. Since no nodes chose slot 6 other than node 3, its transmission will be a success, and it will receive back an A-ACK from its intended receiver. All nodes will resume their timers after the end of the A-ACK transmission. Nodes 1 and 4 chose the same slot and hence their ADV packets possibly collide. However, if both receivers are out of the other transmitter's range, no collision will occur and both nodes will receive an A-ACK for their reserved slots. If a collision happens at an intended receiver, no A-ACK will be received by the corresponding transmitter. After these transmissions, node 5 will transmit successfully, but node 2 will have no time left in the ADV period to complete its transmission, and thus it will postpone its transmission to the next frame. We can take advantage of bursty traffic to reduce the overhead in the ADV period and hence reduce the size of the ADV period to save energy. When a node needs to transmit packets in a burst, one single ADV/A-ACK exchange may reserve the same data slot for n consecutive frames, so that the transmitting node need not send an ADV for each data packet. This can greatly reduce the traffic in the ADV period, saving energy. The number of consecutive frames for which a data slot is reserved may be fixed or may be announced in the ADV and A-ACK packets. In this paper, we consider a fixed value of n. Nodes may have fewer than n packets. In that case, the receiver will timeout and go to sleep in the selected data slot. This technique also works with periodic traffic, with a period matched to the frame length, where a single ADV/A-ACK exchange can reserve a particular data slot, and the transmitter node can renew its channel access periodically.

B. Data Period

The data period is divided into longer slots compared to the slots of the ADV period. Each data slot is large enough to transmit a data packet along with an ACK. If a transmitting and a receiving node exchange ADV and A-ACK packets successfully, they will wake up at the beginning of their chosen slot to exchange data. In all other slots they will be asleep. Nodes that do not have any data to send or receive will be asleep during the entire data period. New nodes joining the medium will initially have no information about the available data slots. If such a node has data to send, it can stay awake in the data period to find an unoccupied slot. It may attempt to reserve that slot in the next frame. If, however, the intended receiver knows that this slot is already reserved by another node (not in the transmitter's range), the intended receiver will simply not reply to the ADV packet.

VI. PROBLEM FORMULATION

Current presented algorithm Ad-ATMA for medium access control that improves on a state of the art algorithms ATMA and Ad AMAC in terms of latency and PDR while using slightly less energy than them. The main idea behind the algorithm is an adaptation scheme for the contention window. It would be interesting to see if even better window adaptation algorithms exist for this problem. The most important extension of Ad-ATMA would be to mobile networks since WSANs are increasingly conceived to be mobile.

VII. PROPOSED WORK

It explains the process used to discover the reliable path for routing by discovering the trustable and most stable nodes. The reliable path is secured using cryptography and also optimized. The methodology and flowchart in the next section explains the whole process that make possible to calculate desired results.

The Methodology involved in this research is of three phases:

Deep Investigation: In this phase the Research is done for various WSN routing protocols. From the survey it is cleared that the performance of all the routing protocols is not at par in all kind of networks. For eg. As in case of the Phantom Routing scheme perform well in case of large sized network but it is not quite well in case of small sized and medium sized networks. So in this study the performance of the Phantom Routing is to be improved and security is to be implemented.

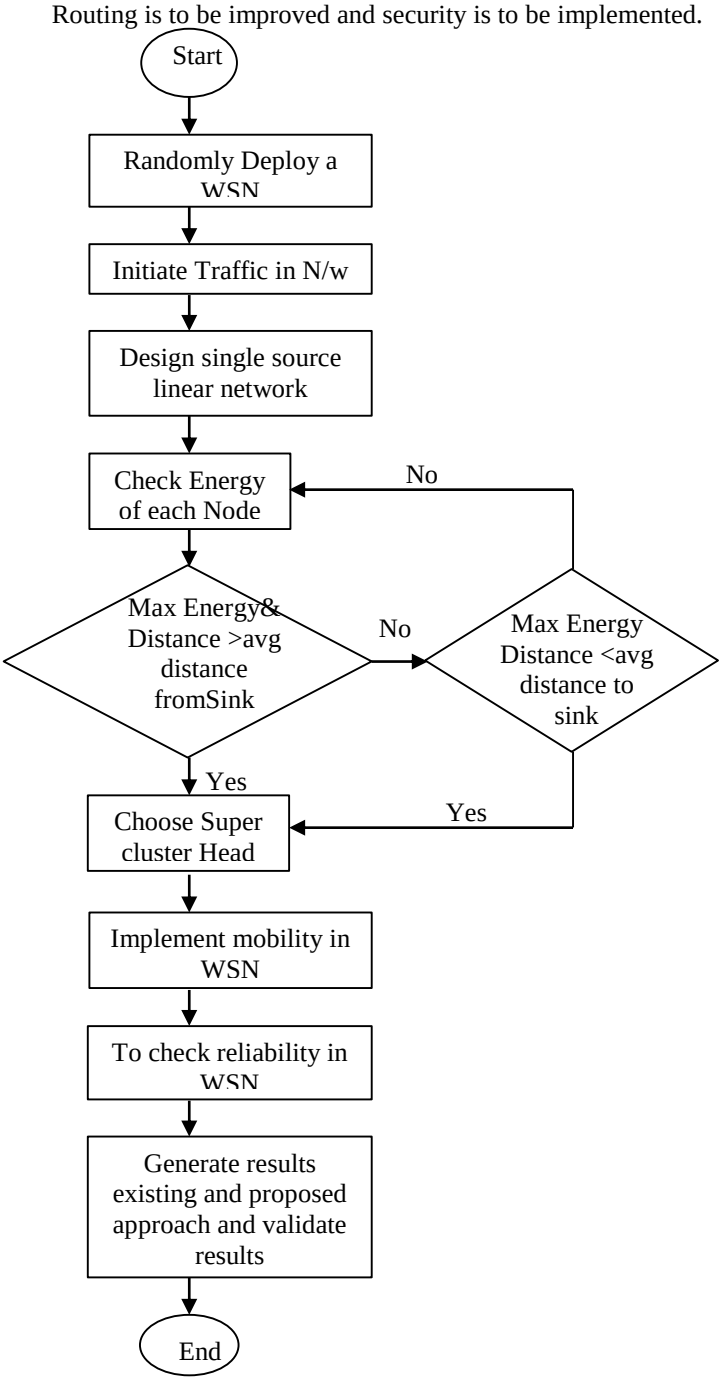

Fig 2: Flow chart

Algorithm

- **Begin:**
  - **Deploy nodes in an area of 100*100**
  - **Select cluster head on basis of residual energy.**
  - **Select secondary cluster head on basis of residual energy and distance from base station.**
  - **If(REsc>AVGenergyof network and REsc>Et)**
  - **No tertiarty cluster head**
  - **Generate cluster by using CSMA/CA. This step is for advertising of cluster head formation using CSMA/CD**
  - **Nodes transmit data according to TDMA scheme to CH.**
  - **CH transmit data to secondary cluster head and then to tertiary to make it to sink.**
  - **Energy Consumption is:**
  - **Etc = Eadvertisement+Esetup+Edatatransmission**

Designing and Development: In this phase the main emphasis is on the designing and development of the improved routing protocol that is to be proposed in this research. In the designing phase, an optimization scheme and cryptographic technique is to be implemented. With the help of an optimization algorithm the performance of the Phantom Routing algorithm will be enhanced and the various drawbacks will be overcome. With the help of cryptographic techniques the efficiency of Phantom routing will be maintained.

Modeling and Simulations: Simulation is the process of modeled the behavior of the network by calculating the interaction b/w the different network components using mathematical formulae. The simulation process can be modeled by using MATLAB Modeler. In the simulation phase the result will be generated and the validation is to be done. From the simulation phase a fair comparison may be done with which one can judge the improvements done in the Phantom Routing algorithm.

In this research different scenarios are taken into consideration with varying number of nodes against constant simulation time. Comparison is drawn between two coverage techniques on the basis of delay, load, throughput, data dropped and retransmission attempts.

Simulation Time: The time taken for each simulation to run or it can be said as the time between start and end of it.

Delay: Delay of network specified how long it takes for a bit/packet of data to travel across the network from one node to another.
Load: It refers to the amount of data that is carried by a network. It is expressed as bits/sec or packets/sec.
Throughput: It is an average rate of successful message delivery over a network. It is measured in Bits/sec or packets/sec.

VIII. RESULTS AND DISCUSSION

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

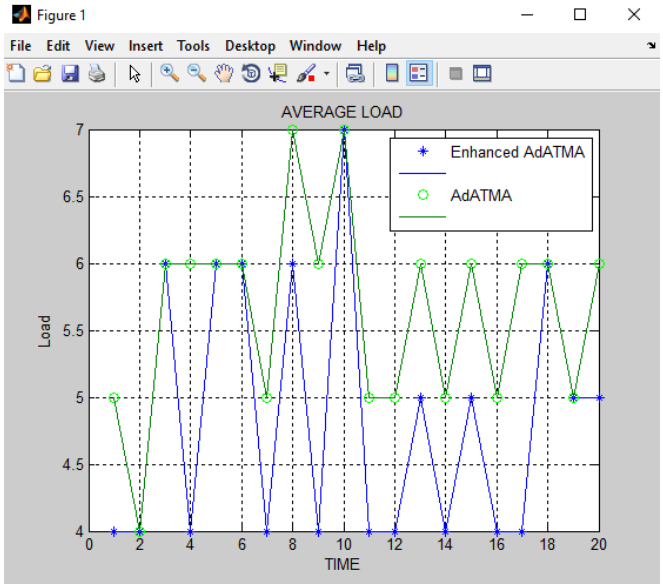

Fig 3: Average load

Load: The load in two WSN protocols called ADATMA and enhanced ADATMA in 25 nodes. From the above graph it is shown that the load in proposed approach is less than that of existing approach.

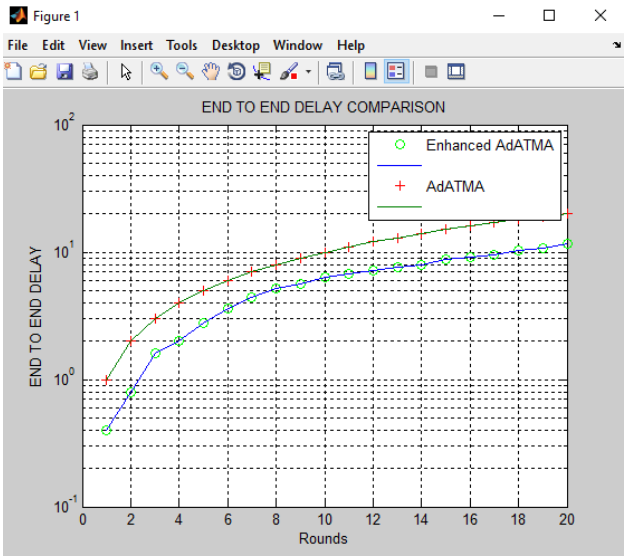

Fig 4: Delay

Delay: Delay in enhanced ADATMA and ADATMA in WSN in 25 nodes. From the graph it can easily depicted that the delay in enhanced ADATMA is less than that of existing ADATMA protocol.

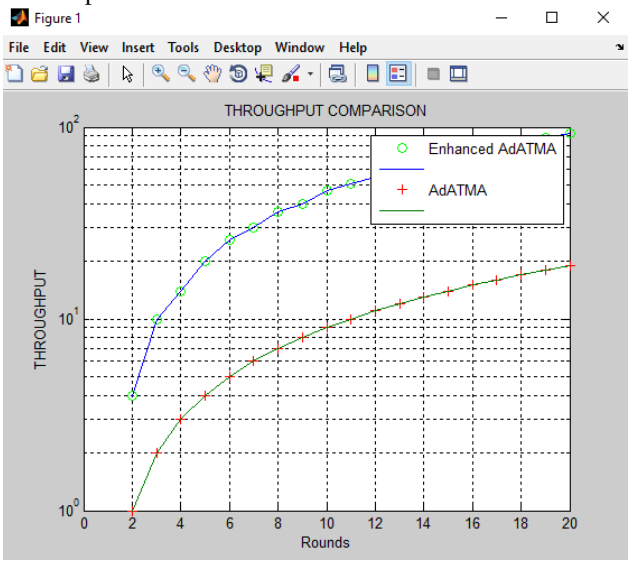

Fig 5: Throughput

Throughput: Throughput in enhanced ADATMA and ADATMA in WSN in 25 nodes. From the graph it can easily depicted that the throughput in enhanced ADATMA is less than that of existing ADATMA protocol. Throughput in case of proposed case is approx 110 packets and in existing case it is approx 100 packets.

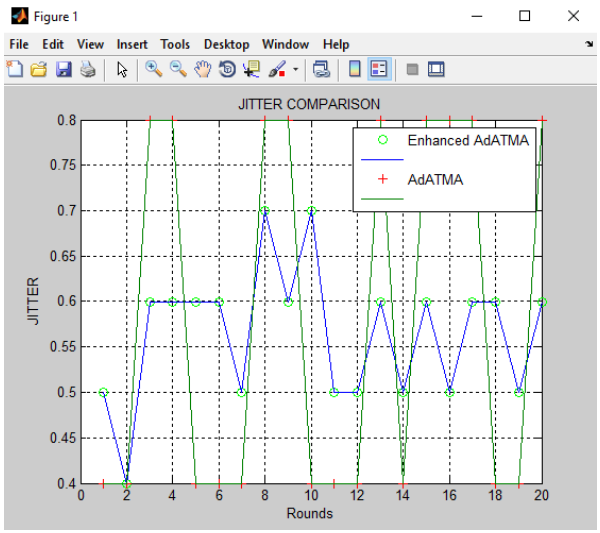

Fig 6: Jitter

Jitter: Jitter in enhanced ADATMA and ADATMA in WSN in 25 nodes. From the graph it can easily depicted that the jitter in enhanced ADATMA is less than that of existing ADATMA protocol. Jitter in case of proposed case is approx 3.5 sec and in existing case it is approx 7 sec.

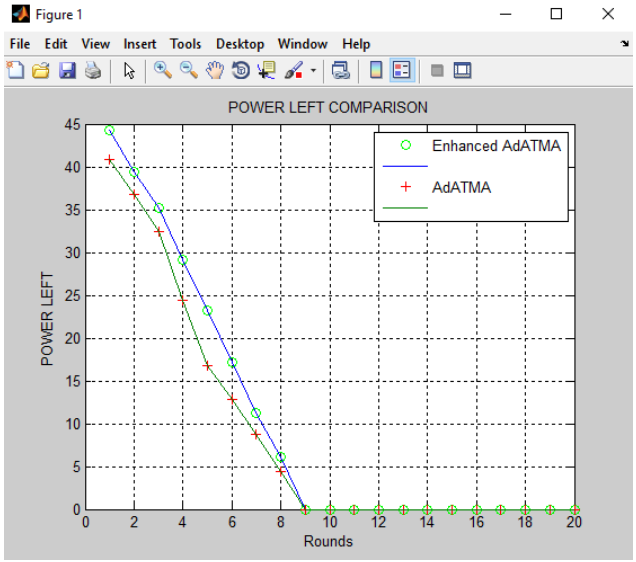

Fig 7: Power Left

Power Left: Power Residual in enhanced ADATMA and ADATMA in WSN in 25 nodes. From the graph it can easily depicted that the residual power in enhanced ADATMA is more than that of existing ADATMA protocol. Residual power in case of proposed case is retained upto approx 10 rounds and in existing case it is approx 8 rounds.

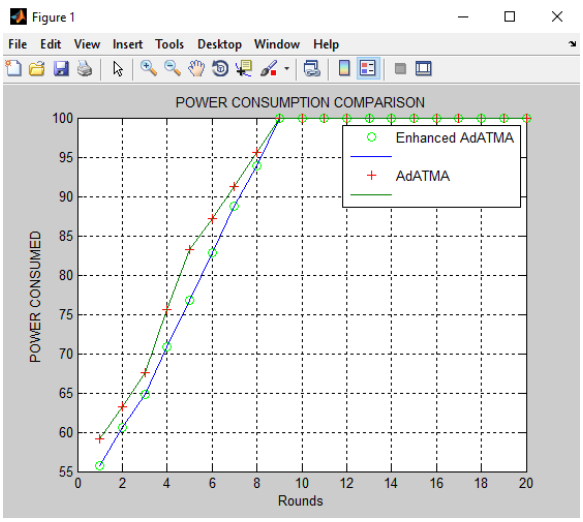

Fig 8: Power Consumption

Power Consumption: Power Consumption in enhanced ADATMA and ADATMA in WSN in 25 nodes. From the graph it can easily depicted that the residual power in enhanced ADATMA is more than that of existing ADATMA protocol. Residual power in case of proposed case is retained upto approx 10 rounds and in existing case it is approx 8 rounds.

Algorithm Parameters	Existing	Proposed
Delay(sec)	400	300
Residual power	8 rounds	10 rounds
Power Consumption	8 Rounds	10 rounds

Table 1: Comparative Study of Existing and Propsoed Approach

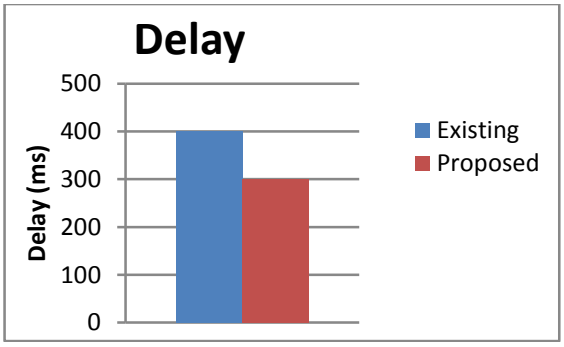

Fig 9: Delay (ms)

Fig 9 is representation of delay in 200 nodes. From above results it is clear that the proposed algorithm is better as compare to the existing approach i.e. delay in case of existing approach is more as compare to the proposed approach.

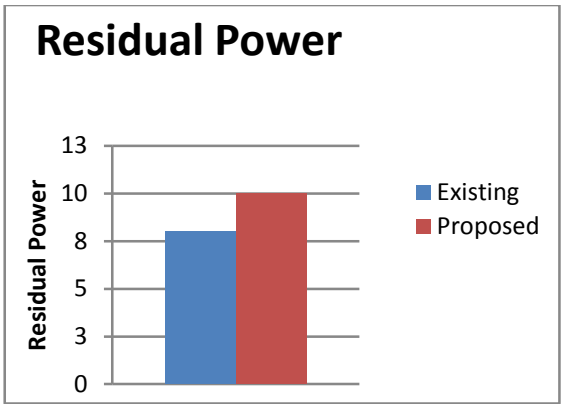

Fig 10: Residual Power Comparison

Fig 10 is representation of residual power in case of 200 nodes. From above results it is clear that the proposed algorithm is better as compare to the existing approach i.e. residual power in case of existing approach is less as compare to the proposed approach.

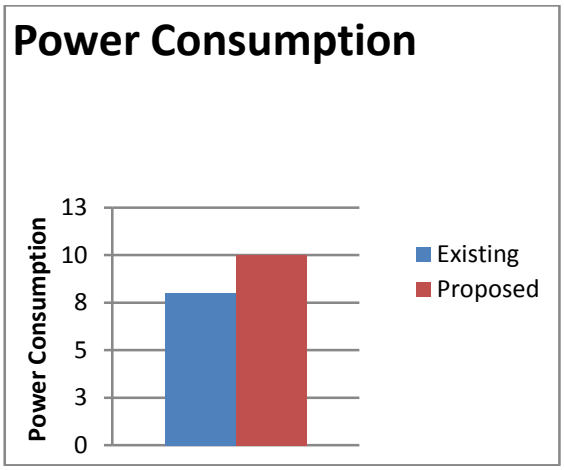

Fig 11: Power Consumption Comparison

Fig 11 is representation of power consumption in case of 200 nodes. From above results it is clear that the proposed algorithm is better as compare to the existing approach i.e. power consumption in case of existing approach is more as compare to the proposed approach.

IX. CONCLUSION

In the proposal an approach is defined for energy efficiency and reduction in data dropped in the WSN network. In Data Aggregation algorithm a subset is defined, in which if a single node in that subset is died out then the whole subset have to be replaced. A modification in the data aggregation algorithm is made to achieve the objectives of the research in which energy efficiency is improved and security algorithm is embedded. In this scheme the optimization is done in the existing data aggregation scheme so that the drops in the network may be reduced. In this way the data dropped due to energy dissipation is reduced. Using this approach the data dropped and other Quality parameters are also improved like, delay, load and throughput etc as defined in results and discussion. From the above defined results it may be clear that the proposed algorithm is more secure and efficient as compare to existing algorithms of data aggregation. In case of scalability the proposed results are better than that of the existing data aggregation technique.

X. REFERENCES

1. Akilandeswari, N.; Santhi B.; Baranidharan, B.;(2013) “A Survey on Energy Conservation Techniques In Wireless Sensor Networks”, ARPN Journal of Engineering and Applied Sciences, ISSN 1819-6608, Volume. 8, No. 4, pp: 265-269

2. Brar G.S., Rani S., Chopra V., Malhotra R., Song H., Ahmed S.H., (2016) “Energy Efficient Direction-Based PDORP Routing Protocol for WSN”, IEEE Access, Special Section On Green Communications And Networking For 5G Wireless, ISSN: 2169-3536, Volume 4, pp: 3182-3194

3. Chen Y.B., Lin G.Y., Wei H.Y., (2016) "A Dynamic Estimation of the Unsaturated Buffer in the IEEE 802.11 DCF Network: A Particle Filter Framework Approach", IEEE Transactions on Vehicular Technology, ISSN: 0018-9545, Vol: 65, No: 7, pp: 5397-5409

4. Gawali, S. E.; Mantri, D. S.;(2010) “Lifetime Energy Efficient Optimization for WSN”, 2nd International Conference, Computer Technology and Development, E-ISBN :978-1-4244-8845-2, Print ISBN:978-1-4244-8844-5, pp: 235-239

5. Guravaia; K.; Velusamy, R. L.; (2015) “RFD: River Formation Dynamics based Multi-Hop Routing Protocol for Data Collection in Wireless Sensor Networks”, Eleventh International Multi-Conference on Information Processing, Volume: 54, pp: 31-36.

6. Hayes, T.; Ali, F.H.; (2015), “Proactive Highly Ambulatory Sensor Routing (PHASeR) protocol for mobile wireless sensor networks”, Pervasive and Mobile Computing, Volume: 21, pp: 47-61

7. Huang H., Gong T., Chen P., Malekian R., Chen T., (2016) “Secure Two-Party Distance Computation Protocol Based on Privacy Homomorphism and Scalar Product in Wireless Sensor Networks”, Tsinghua Science And Technology, ISSN: 1007-0214l, Volume: 21, No: 4, pp: 385-396

8. Joshi, G. P., Nam, S. Y., Kim, S. W. (2013) “Cognitive Radio Wireless Sensor Networks: Applications, Challenges and Research Trends”, Sensors, ISSM: 1424-8220, Vol.13, No: 9, Aug 12, pp: 11196-11228

9. Khan, A. W.; Abdullah, A. H.; Razzaque, M. A.; Bangash, J. I.; (2015) “VGDRA: A Virtual Grid-Based Dynamic Routes Adjustment Scheme for

Mobile Sink-Based Wireless Sensor Networks", IEEE Sensors Journal, Volume: 15, Issue: 1, pp: 526-534

10. Kumar, N., Kumar, M., Patel, R. B.(2012) "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks", International Journal of Network Security, Vol.15, No.6, pp.490-500

11. Li, X, Merrett, G. V., White, N. M. (2013) "Energy-efficient data acquisition for accurate signal estimation in wireless sensor networks", Journal on wireless Communications and Networking, Vol. 230, Issue.1, pp: 1-15

12. Long, J.; Dong, M.; Ota, K.; Liu, A.; Hai, S.; (2015) "Reliability Guaranteed Efficient Data Gathering in Wireless Sensor Networks", IEEE, ISSN: 2169-3536, Volume: 3, 2015, pp: 430-444

13. Mishra, N. K., Jain,V., Sahu, S.(2013) "Survey on Recent Clustering Algorithms in Wireless Sensor Networks", International Journal of Scientific and Research Publications, ISSN 2250-3153, Vol. 3, Issue.4, pp: 1-4.

14. Patil, P., Kulkarni, U. P.(2013) "Energy Efficient Aggregation With Divergent Sink Placement For Wireless Sensor Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.4, No.2, pp: 47-58

15. Prabha, K. A., Hemapriya, K. (2013) "Energy Saving In Wireless Sensor Network Using Optimal Selective Forwarding Protocol", International Journal of Advancements in Research & Technology, Vol. 2, Issue: 1, pp: 1-6

16. Qi J., Hu X., Ma Y., Sun Y., (2015) "A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme", Special Section On Industrial Sensor Networks With Advanced data management: design and security, IEEE Access, ISSN: 2169-3536, Volume: 3, pp: 718-724

17. Riyami A.A., Ning Zhang, John Keane,(2016) "An Adaptive Early Node Compromise Detection Scheme for Hierarchical WSNs", IEEE Access, ISSN: 2169-3536, Volume: 4, pp: 4183-4206

18. Saini, M.; Saini, R. K.; (2013) "Solution of Energy-Efficiency of sensor nodes in Wireless sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 5, pp: 353-357

19. Seada, K.; Zuniga, M.; Helmy, A.; Krishnamachari, B.;(2004) "Energy Efficient Forwarding Strategies for Geographic Routing in Lossy Wireless Sensor Networks", Proceedings of the 2nd international conference on Embedded networked sensor systems, USA, ISBN:1-58113-879-2, pp: 108-121

20. Singh, S.; Meenaxi, (2013) "A Survey on Energy Efficient Routing in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Volume 3, Issue 7, pp: 184-189

21. Sun L., Ren P., Du Q., Wang Y., (2016) "Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks", IEEE Transactions on Industrial Informatics, ISSN: 1551-3203, Volume: 12, No: 1, pp: 291-300

22. Usman M., Gebremariam A.A., Raza U., Granelli F., (2015) "A Software-Defined Device-to-Device Communication Architecture for Public Safety Applications in 5G Networks", Special Section on Recent Advances In Software Defined Networking for 5g networks, IEEE Access, ISSN: 2169-3536, Volume: 3, pp: 1649-1654

23. Wu J., Ota K., Dong M., Li C., (2016) "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities", IEEE Access, ISSN: 2169-3536, Volume: 4, pp: 416-424

24. Ye, W.; Heidemann, J.; Estrin, D.; (2002), "An Energy-Efficient MAC Protocol for Wireless Sensor Networks", INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, ISSN: 0743-166X, Volume: 3, pp: 1567-1576

25. Zhao Z., Feng J., Peng B., (2016) "A Green Distributed Signal Reconstruction Algorithm in Wireless Sensor Networks", Special Section On Green Communications And Networking For 5g Wireless, IEEE Access, ISSN: 2169-3536, Volume: 4, 2016, pp: 5908-5917