International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Secure Data Aggregation Protocol with Efficient Energy in Sensor Networks

M Selvi, P M Joe Prathap

Abstract*: *In the current secure data aggregation strategies, decrease within the energy utilization isn't greatly talked about and consolidated answer for both trustworthiness and confirmation isn't tended to. In this paper, we propose to structure an Energy Efficient Secure Data Aggregation Protocol for wireless sensor networks. In this protocol, we fuse the confirmation as well as protection to keep up the productivity of the data aggregation. Initially the network been partitioned into bunches, every group is going through an aggregator also the aggregators are associated with sink each straightforwardly otherwise by different aggregators. The aggregator has been chosen dependent taking place the closest separation toward a lot of sensor hubs as well as its energy level. Detached inputs has been circulated toward the two points i.e., sensor hub to the aggregator as well as aggregator to the sink. At whatever point a sensor hub needs to mail information toward an additional hub; former the sensor hub scrambles the information utilizing a input also mails it toward the aggregator. For honesty of the information parcel, a MAC support confirmation policy is utilized. Reenactment outcome confirm so as to our planned protocol have decreased energy utilization though achieving great bundle conveyance proportion.

Keywords: Efficient Energy, Secure Data Aggregation, Wireless Sensor Networks and Network Simulator.

I. INTRODUCTION

In wireless sensor networks, data aggregation is measured as one of the basic distributed data handling approach for thrifty the energy as well as preventing the intermediate get to level conflict [1, 2]. Data aggregation is demonstrated as a significant model for steering within the wireless sensor networks. The essential idea is to consolidate the information commencing different resources, redirect it by the end of the repetition consequently lessening the quantity of broadcasts as well as sparing energy [3]. The inherent excess inside the crude information assembled commencing different sensors could be anticipated through the in-network data aggregation. Furthermore, these activities are likewise helpful to separate function explicit data as of crude information. Toward keeping the energy inside the framework in favor of keeping up extended duration within the system, it is significant in favor of the system to keep up the fast rate of the in-network data aggregation [4].

II. SECURE DATA AGGREGATION

The concern identified with the protection in the data aggregation of WSN is as per the following [5-8]:

Data Confidentiality: Specifically, the basic protection concern is the information confidentiality which shields the broadcasted information that is delicate as of inactive assaults similar to spying. The importance of the information secrecy lies within the threatening condition, while the wireless control is increasingly defenseless toward listening stealthily. Despite the fact that cryptography has given a lot of strategies, the activity identified with convoluted encryption and unscrambling, as particular augmentation of huge numbers in broad daylight key based cryptosystems, utilizes the sensors control rapidly.

Data Integrity: Data Integrity counteracts the alteration of the final aggregation esteem through the undermined resource hubs otherwise aggregator hubs. Sensor hubs be capable of effectively undermined since the absence of the costly altering safe equipment. Something else, utilized equipment may not be dependable now and again. An undermined hub is equipped for changing, manufacturing and disposing of the messages.

When all is said in done, on behalf of secure data aggregation in wireless sensor networks, two strategies is utilized. They are bounce by jump scrambled data aggregation and start to finish encoded data aggregation.

Hop-by-Hop encrypted data aggregation: In this method, the encryption of the information has been done via detecting hubs as well as decoding via aggregator hubs. The aggregator hubs total the information also again scrambles the aggregation outcome. Towards ending, the sink hub by getting the last encoded aggregation outcome decodes it.

End to End encrypted data aggregation: here, the aggregator hubs within the middle don't have unscrambling inputs as well as know how to just execute aggregation on top of the encoded information.

III. RESEARCH METHODOLOGY

Herein exploration effort, energy efficient secured data aggregation protocol for wireless sensor network is projected, which would reduce the hub bad conduct.

The protocol includes:

Manuscript published on November 30, 2019.
* Correspondence Author
M Selvi*, Research Scholar, Sathyabama Institute of Science and Technology, Chennai, India.
P M Joe Prathap, Associate Professor, Department of Information Technology, RMD Engineering College, Chennai, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

- Method for energy efficient aggregator choice
- Method for efficient hub choice on behalf of enhancing the system duration as well as lessening the deferral
- Source hub confirmation by the sink
- Aggregator confirmation according to recorded in the parcel header, by the sink. Parcel header is recorded in Figure 1.

Packet-ID	Source-Address	Destination-Address	List-of-Visited-Sensor-Nodes	TTL

Fig.1 Packet Header Format

Where:

- Packet-ID: is a one of a kind number used to recognize copy.
- Source-Address: contains the IP address of the transmitter of bundle.
- Destination- Address: contains the IP address of the goal hub.
- List-of-Visited-Sensor-Nodes: contains rundown of addresses of recently call-on hubs.
- Time-To-Live (TTL): includes a tally of numeral moderate hubs navigated.

The projected protocol knows how to develop over the prior key dissemination and encryption plots in the wireless sensor networks.

IV. SYSTEM OVERVIEW

Within a clustered WSN, the network is assembled as groups. Every group has an aggregator comprising of an amazing wireless handset so as to equip for broadcasting the information legitimately toward the internal server. It is expected to facilitate every sensor plays out the broadcast of the information just toward the aggregator. Thus, every sensor will have the option to lessen the transparency within broadcasting the information parcels. Consequently, everyone accepts with the aim of the sensor hubs don't contain some versatility, i.e., the sensor hubs have altogether connected toward a location as well as can't progress.

The confirmation data has been worked through the resource utilizing the common input. Check data has been incorporated by information parcel through the broadcast. By gathering parcel, the resource is checked through the aggregator utilizing the common input. If there should arise an occurrence of disappointment in the check, the bundle would be disposed of; else, would be sent. By gathering information parcel through the sink, the resource would be tried once more on behalf of its legitimacy. On the off chance that the legitimacy of the resource comes up short, at that point it would be disposed of.

A MAC supported confirmation policy is utilized so that keeps up the trustworthiness of the information bundle. The sink is able to distinguish some progressions done by the aggregator together with the confirmation data, through examining of the MAC esteem utilizing its mutual input. In the event that the information bundle has seen as adjusted, at that point it will be disposed of.

The power utilization is diminished because of choice of the aggregator's dependent happening energy point, alongside the support of the mystery as well as protection. In the event of the mystery, encryption is done through every sensor hub also this encoded information been then broadcasted toward the aggregator. Thus, the foes won't be able to peruse the data parcel.

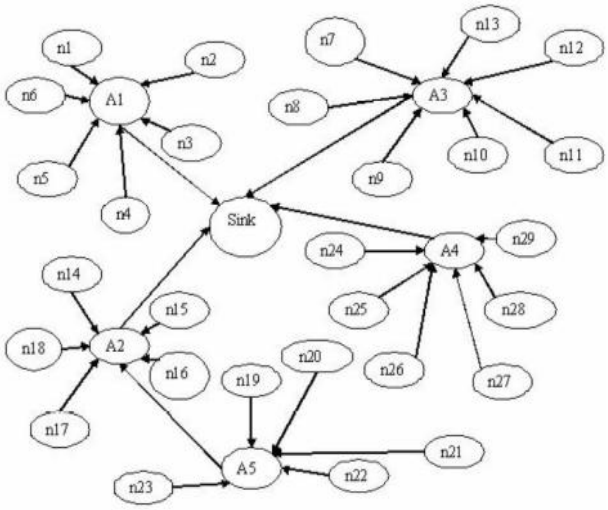

Fig.2 System Architecture

In the framework engineering of WSN, appeared inside Fig 2, n1, n2.., be signified like hubs also A1, A2.., be meant like aggregator. At first system is separated as bunches, all the group be going through an aggregator also the aggregators be associated with sink moreover straightforwardly otherwise by different aggregators.

V. RESULTS AND DISCUSSION

Recreation depends analyses were led in this exploration to assess the exhibition of the proposed calculation. These days, PC based discrete-occasion reenactment has generally acknowledged to be a significant tool in numerous territories where explanatory techniques are not relevant and experimentation isn't doable. The standard methodology in the WSN investigate network for the most part pursues the improvement, reproduction, and distributes procedure, and WSN productions regularly incorporate execution recreations that look at changed protocols. In this examination likewise, recreations were additionally done for assessing the projected aggregator calculation as well as hub catch assaults.

Network Simulator: Network Simulator2 (NS2) be a distinct-occasion reenactment stage coded in C++ programming language as well as Scripting language Object oriented Tool Command Language (OTCL). Client composes an OTCL content that characterizes the system (numeral hubs, connects), the congestion in the system (resources, goals, kind of congestion) also the protocol is utilized. This content been utilized through NS2 in recreation. The consequences of the recreation be a yield follow record so as to utilize for information handling (ascertain productivity, holdup also so on.) and visualize the reproduction by coding named Network AniMator (NAM). NAM is a perception tool which imagines the parcel like it spreads by the system.

A review of the reproduction been done in NS2 is showed in Fig. 3.

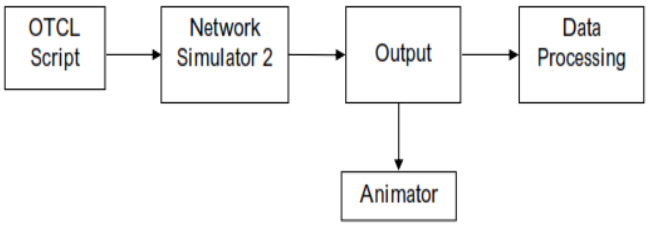

Fig.3 Network Simulator-2

Reproduction Overview: Recreation in NS2 Showed in Fig 4 consists of generating the associated info records toward NS2.

- Circumstances documentation depicts the expansion scenario of hubs.
- Associated document depicts the traffic within the network.

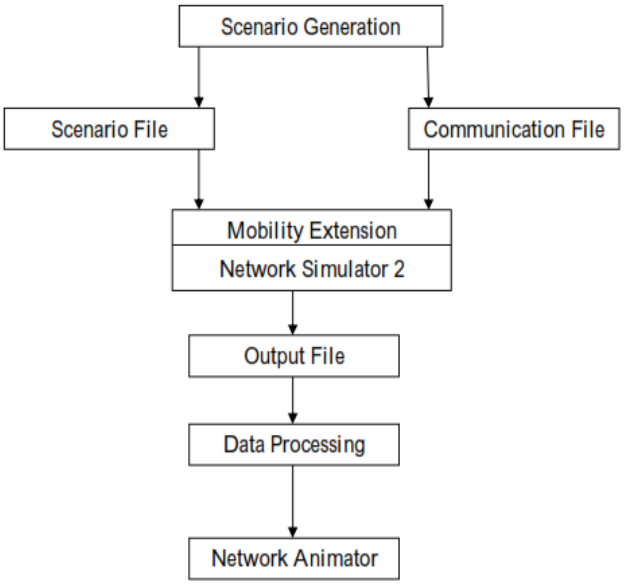

Fig.4 Simulation Overview

This documentation could be formed through creating entirely casual progress also associated plan by subject. They are subsequently used on behalf of the simulation also therefore on or after this; a pursue record is produced as a result. Before the simulation, the attributes which is tracked during the restoration should be selected. The track record can subsequently sort out as well as verified in favor of various attributes which should be anticipated. It should be used like data meant for designs and to picture the reproduction run with NAM.

Execution Metrics: The presentation of EESDA is contrasted and the CPDA protocol, as indicated by the accompanying measurements.

- Average end-to-end Delay (ms): It is arrived at the midpoint of over every single enduring datum parcels commencing the resource toward the goals.
- Average Packet Delivery Ratio (%): This is stated as the proportion of the quantity of bundles got effectively by the all out numeral parcels broadcasted.
- Energy Consumption (Joules): Energy Consumption is the normal energy utilization of each and every hub in transmitting, accepting also promoting tasks.

Based on Attackers: In introductory reproduction, number of aggressors is differed as 5, 10, 15, 20, 25 and 30

Table.1 Attackers Vs Delay for CPDA and EESDA

Attackers (No's)	CPDA (ms)	EESDA (ms)	Percentage (%)
5	5.5008	3.3059	39.90175
10	6.8549	4.1644	39.24973
15	6.9879	5.1963	25.63872
20	7.2358	5.3486	26.08224
25	7.8603	5.7725	26.56159
30	8.2980	6.5928	20.54968
Average	7.1228	5.0633	29.663

Table 1 portrays the normal start to finish holdup on behalf of the two protocols while the quantity of aggressors be expanded. In the fig, it tends to be viewed that the normal start toward finish postponement of the current CPDA protocol is 7.1228 ms as well as the projected EESDA protocol is 5.0633 ms. Subsequently as of the reproduction investigation it is surmised to the postponement is under 29.66% while contrasted and surviving CPDA protocol.

Table 2 Attackers Vs Delivery Ratio for CPDA and EESDA

Attackers (No's)	CPDA (%)	EESDA (%)	Percentage (%)
5	47.940	70.737	32.22830
10	38.2340	63.164	39.46789
15	25.9888	50.687	48.72609
20	20.8976	47.836	56.31338
25	19.2732	42.018	54.13024
30	12.46599	33.0577	62.29013
Average	27.466	51.249	48.859

Table 2 characterizes the packet delivery proportion of existing CPDA protocol be 27.466% also the projected EESDA protocol which is 51.249%. Since unwavering quality is accomplished utilizing the connection solidness, EESDA accomplishes great conveyance proportion 48.85%, contrasted with existing CPDA protocol.

Table 3 Attackers Vs Energy for CPDA and EESDA

Attackers (No's)	CPDA (Joules)	EESDA (Joules)	Percentage (%)
5	99.346	90.013	9.394233
10	83.372	74.679	10.42669
15	77.409	64.646	16.48825
20	63.362	48.564	23.3559
25	60.286	34.316	43.07898
30	48.574	30.346	37.52703
Average	72.057	57.093	23.378

Table 3 shows the consequences of energy utilization for the current CPDA protocol be 72.057 joules also the proposed EESDA protocol be 57.093 joules. As of the outcomes, it tends to be viewed that EESDA protocol have low energy utilization by 23.37% than the current CPDA protocol, because this protocol have the energy efficient way.

Table 4 Attackers Vs Overhead for CPDA and EESDA

Attackers (No's)	CPDA (Packets)	EESDA (Packets)	Percentage (%)
5	15281	5055	66.92409
10	16954	8915	47.41935
15	18029	9421	47.74796
20	20340	11044	45.7054
25	23877	13430	43.75525
30	24935	14924	40.16
Average	19901.6	10463.8	48.6169

Table 4 portrays the aftereffects of Overhead in favor of the current CPDA protocol be 19901.6 parcels as well as the projected EESDA protocol be 10463.8 bundles. As of the outcomes, it is viewed that EESDA protocols have fewer Overhead 48.61% contrasted with the current CPDA protocol.

VI. CONCLUSION

In this research, a Secure Data Aggregation protocol with efficient energy in sensor networks has been created to keep up energy productivity. For data aggregation, the framework is gathered with the end goal that each gathering is going by an aggregator. This aggregator goes about as a connection between the sensor hubs and the sink. During the transmission of the data, first encryption is performed by the sensor hubs while moving information toward the aggregator. The aggregator on gathering of the information decodes it utilizing the input and understands it. The aggregator at that point decides the MAC esteem utilizing hash capacity toward verifying the legitimacy of the resource sensor. In the event that the assessed MAC esteem is substantial, at that point the source is validated. Second encryption is performed by the aggregator while moving data alongside the MAC incentive to the sink. Consequently respectability of the framework is kept up. Because of the twofold encryption of the information through data aggregation, enemies can't influence the framework. Henceforth the framework stays secure even in the wireless condition. Reenactment outcomes explain that the projected protocols of EESDA have diminished energy utilization while accomplishing great packet delivery proportion.

REFERENCES

1. Bhoopathy, V. and Parvathi, R.M.S. "Energy Efficient Secure Data Aggregation Protocol for Wireless Sensor Networks", European Journal of Scientific Research, Vol. 50, Issue 1, pp.48-58, February 2011.
2. Zhenzhen Y, A Abouzeid, A, Jing A "Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks, Proceedings of the workshop on Draft Infocom, pp. 1676-1684, December 2006.
3. Krishnamachari, B., Estrin, D, Wicker S, "The Impact of Data Aggregation in Wireless Sensor Networks", Proc. of the 22nd Int. Conf. on Distributed Computing Systems, Vienna, Austria, IEEE Computer Society, pp. 575-578, July 2002.
4. Kai-Wei F, Sha L, Prasun S, "Structure-free Data Aggregation in Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 6, No. 8, pp. 929-942, August 2007..
5. Yingpeng S, Hong S, Yasushi I, Yasuo T, Naixue X, "Secure Data Aggregation in Wireless Sensor Networks: A Survey", Proc. of the 7th Int. Conf. on Parallel and Distributed Computing, Applications and Technologies, pp. 315-320, December 2006.
6. M Selvi, P M Joe Prathap, "WSN Data Aggregation of Dynamic, Routing by QoS Analysis", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9. Sp– 18 / 2017, pp. 2900-2908.
7. M Selvi, P M Joe Prathap, "Analysis & Classification of Secure Data Aggregation in Wireless Sensor Networks", International Journal of Engineering and Advanced Technology, Volume-8 Issue-4, April 2019, pp.1404-1407.
8. M Selvi, P M Joe Prathap, "Performance Analysis of QoS Oriented Dynamic Routing for Data Aggregation in Wireless Sensor Network", International Journal of Pharmacy & Technology, Vol.9, Issue.2, 2017, pp.29999-30008.