Secure Data Aggregation in Distributed Computing: To Overcome Dishonest Nodes through PPAC Algorithm

R.Gowsalya[1], Dr.P.Thirumoorthy[2]

[1]PG Scholar, [2]Professor, Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamil Nadu

ABSTRACT: *Privacy-preserving data aggregation in network systems, e.g., Internet of Things (IoT), is a challenging problem, considering the dynamic network topology, constrained computing ability and electricity furnish of IoT devices, etc. The difficulty is now inflated when there exist dishonest nodes, and how to ensure privacy, accuracy, and robustness of the facts aggregation system in opposition to dishonest nodes remains an open issue. Different from the widely investigated cryptographic approaches, in this paper, we tackle this challenging trouble by using exploiting the allotted consensus technique. To mitigate the pollution from dishonest nodes, we propose a better impenetrable consensus-based facts aggregation (E-SCDA) algorithm that approves neighbour's to become aware of dishonest nodes, and derive the error certain when there are undetectable dishonest nodes. We prove the convergence of the E-SCDA and exhibit that the algorithm can preserve the privates related to nodes' preliminary states. The extensive simulations had proved that the proposed algorithm has a high convergence accuracy and low complexity, even when there exist dishonest nodes in the network.*

Keywords: *Privacy, Aggregation, Distributed Computing, consensus-based privacy-preserving*

I. INTRODUCTION

Wireless sensor network is ordinarily self-configurable and unattended network, which are composed of a few to heaps of light-weight and portable tiny sensing nodes. These networks are deployed in remote and adversarial environments where these nodes can sense temperature, pressure, vibration, motion, sound and even the pollutant ranges in targeted areas [2]. Wireless sensor networks (WSN) are normally set up for gathering files from insecure environment. Nearly all safety protocols for WSN agree with that the opponent can obtain entire control over a sensor node by way of direct physical access. Basically, via flooding attack, a malicious node/an attacker aim the exhaustion of the network resources (e.g. network bandwidth) as well as ingesting the sources of a true network user [4]. The data gathered from individual nodes is aggregated at a base station or host computer. In case of some restrained procedure quality and also the power resources, the aggregation of the information from multiple detector nodes dead at the aggregating node is often accomplished through easy technique called as averaging method. However such aggregation is common to be highly vulnerable to node compromising assaults Iterative filtering algorithms keep high-quality promise for such a function. Such algorithms concurrently aggregate records from more than one sources and furnish have faith evaluation of these sources frequently in a shape of corresponding weight factors assigned to facts furnished by every source. Data aggregation procedure can decorate the robustness and accuracy of information which is got by means of entire community [5].Data aggregation is an approach to mix information packets. This has the practicable to take away meaningless/redundant records and reduce the number/size of transmissions. Hence, facts aggregation technique can limit network energy consumption if it is used in a WSN. This method combines the records packets using an aggregation characteristic. It would end result in reductions of transmissions and consequently reducing the verbal exchange costs, bandwidth utilisation, network congestion, strength consumption and community prolong in WSN routing. WSN statistics aggregation routing makes verbal exchange paths between source nodes and the sink to aggregate and ahead the network traffic. Resource conservation (mainly-energy), maximizing the range of captured records and minimizing facts series prolong are three key issues that need to be regarded in data aggregation routing [7]. Every sensor hub in the network gathers records from its environment, and sends it to a base station, either from sensor hub to sensor hub i.e. multi jump, or mainly to a base station i.e. single jump. A Wi-Fi sensor network might also contain of heaps or up to a giant wide variety of sensor hubs and can be unfold out as a mass or set out one by means of one. The sensor hubs work collectively with every other over a Wi-Fi media to build up a detecting network, i.e. a wireless sensor

community [14].Information total utilising basic averaging diagram is extra presented to blames and noxious attacks. Wireless Sensor Network Data Aggregation is a essential technique to accomplish energy productivity in the sensor system. The information total is that takes out repetitive facts transmission and enhancements the lifetime of vitality in far flung sensor system. Information conglomeration is the system of one or a few sensors then gathers the discovery result from different sensor. The gathered information ought to be dealt with the aid of sensor to decrease transmission. It can be the base station or now and then an outdoor purchaser who has consent to talk with the system. Data transmission among sensor hubs, aggregators and the interrogated devours part of vitality in remote sensor network. In some application, for example, remote sensor system, records mining, distributed computing information conglomeration is broadly utilized. An aggressor can seize and bargain sensor hubs and dispatch a mixed bag of assaults through controlling traded off hubs [15].

II. RELATED WORK

The approaches for data transmission can be categorized as three classes: multipath forwarding approach, neighbour monitoring approach, and acknowledgment approach. Multipath forwarding is a widely adopted countermeasure to mitigate packet droppers, which is based on delivering redundant packets along multiple paths [16]. Alternative methodology is to yield up the observing mechanism can also be accompanied. To deal with packet modifiers, most of existing countermeasures are to filter modified messages within a certain number of hops so that energy will not be wasted to transmit modified messages [17]. The effectiveness to detect malicious packet droppers and modifiers is limited without identifying them and excluding them from the network one approach is the acknowledgment-based for identifying the problematic communication links. That can likewise be deterministically limit connections of pernicious hubs if each hub reports ACK utilizing onion report. In any case, this acquires huge correspondence and capacity overhead for sensor systems [18]. The probabilistic ACK approaches are which look for exchange offs among recognition rate, correspondence overhead, and capacity overhead. Be that as it may, these methodologies expect the bundle sources are trustable, which may not be legitimate in sensor systems [19]. As in sensor systems, base station normally is the just a single we can trust. Besides, these plans require setting up pair astute keys among normal sensor hubs in order to check the realness of ACK bundles, which may cause extensive overhead for key administration in sensor systems [20].

III. PROBLEM FORMULATION

In this paper, we study how to obtain additive data aggregation, i.e., $\sum_{i=1}^{n} x_i(0)$. The predominant graph goals are listed below. First, the aggregation purpose need to be completed in a thoroughly allotted way. Second, due to the privacy concerns, the initial nation of every node ought to not be acknowledged to others (including its neighbors and the aggregator), whilst the aggregation ought to be accurate. Third, the computation and conversation price be minimized. Lastly, there are dishonest nodes in the system, and hence dispensed safeguard mechanisms are wished to quickly discover the suspicious behaviors and sure the error in the aggregation caused by the undetectable dishonest behaviors. This includes two main problem exists during the secure data transmission. First, the overlay network be a connected, undirected graph. Second, in E-SCDA, the aggregator must have the expertise of the topology of the overlay network. A possible path is to design an incentive mechanism such that all nodes are willing to be honest so as to attain an correct privacy-preserving aggregation at a lower cost.

IV.PROPOSED MODULES

A. DATA AGGREGATION:

Data aggregation is an energy efficient approach in WSNs. Due to excessive node density in sensor networks identical records is sensed through many nodes, which outcomes in redundancy. This redundancy can be eradicated by using the usage of information aggregation strategy while routing packets from source nodes to base station.The major aim of data aggregation algorithms is to collect and mixture data in an energy environment friendly manner so that community lifetime is enhanced. Wireless sensor networks (WSN) provide a more and more alluring method of facts gathering in dispensed gadget architectures and dynamic access by using wireless connectivity. Data aggregation has emerged as a simple method in WSNs in order to reduce the quantity of transmissions of sensor nodes, and as a result minimizing the average power consumption in the network. We study foremost records aggregation in WSNs. Data aggregation is affected by various factors, such as the placement of aggregation points, the aggregation function, and the density of sensors in the network. The determination of most efficient selection of aggregation points is as a consequence extremely important. We

current precise and approximate algorithms to find the minimal wide variety of aggregation factors in order to maximize the community lifetime. Our algorithms use a constant virtual wireless backbone that is built on top of the bodily topology. We additionally study the tradeoffs between power financial savings and the manageable delay involved in the data aggregation process.

Algorithm:

Step 1: Generate random vectors functions

Step 2: Create initial state of each node

Step3: Calculating for neighbor node Distances

Step4: Calculate the corresponding Data weights

Step5: Calculating for distribution random variable

Step6: Read the corresponding neighbors Distances and transmitting to nodes

Step7: To select aggregator to monitor neighbor node

Step8: Reputation vector for the Data weights

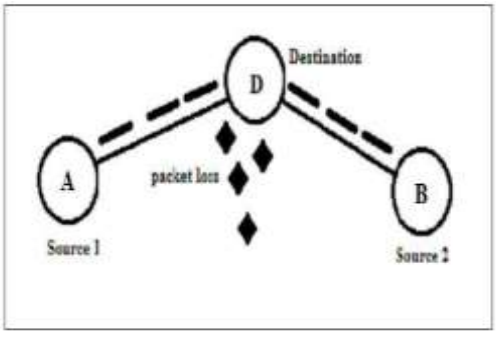
Step9: Report to the aggregator to isolate node for behaviour satisfies

Step10: Filtering for the consecutive readings

Average consensus technique is an extensively used algorithm for distributed averaging, where all the retailers in the network continuously communicate and update their states in order to attain an agreement. This approach should result in an undesirable disclosure of information on the initial state of agent i to other agents. In this paper, we propose a Privacy Preserving Average Consensus (PPAC) algorithm to guarantee the privates of the preliminary nation and the convergence to the specific preliminary values, by way of including and subtracting random noises to the consensus process. We symbolize the suggest rectangular convergence fee of the PPAC algorithm and derive upper and decrease bounds for the covariance matrix of the most probability estimate on the initial state. We further grant an algebraic situation beneath which the PPAC algorithm is (epsilon, delta)-differentially private.

B. NEIGHBOR MONITORING

The aggregator can request a neighbour node to screen a node at a random time instant. Once receiving such a request, a neighbour node i of node j exams the following three stipulations based totally on the handy statistics set the update in every generation is an average process and the introduced noise is exponentially decaying, c2 ensures that the preliminary states of dishonest nodes are bounded by the estimation error, which constrains the preliminary country choice of every dishonest node, and c3 is utilized to make certain that two parts dividing the initial states of nodes.To ensure that the dishonest node who arbitrarily selects the values of its noise manner can be detectable the two neighbour sets of every node are the input, and the output is the nodes up to date states.



The two discovery of neighboring nodes in multi-hop wireless two networks two has become key challenge Due two to tribulations in communication, two synchronization loss between nodes, disparity in transmission power etc., the connectivity of all nodes will always be experience disruptions. On the other hand, the power utilization by the nodes also became critical. In this paper, we advocate a new technique for neighbor discovery in wireless two sensor networks two (WSNs) two which can pay two an eminent consideration for electricity utilization and QoS parameters such as latency, throughput, and error rate. In the proposed method, the network routing is enhanced using AOMDV protocol which can accurately discover the neighbor nodes and power management with HMAC protocol which reduces the energy utilization significantly. The complete study is being performed to estimate how the QoS metrics varies in various consequences of power consumption in wireless networks. Now, we discuss how to estimate the distance between the two nodes and how to select the verification based on the estimated distance.

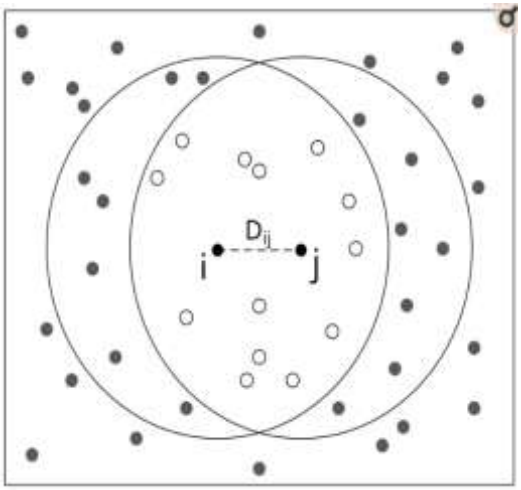
For two nodes *i* and *j*, we firstly deduce that the overlapping area between the communication area of *i* and *j* (denoted by *Sij*) is proportional to the distance between *i* and *j* (denoted by *Dij*). Next, we get the relationship between *Dij* and common neighbours of node *i* and *j* with the help of nodes' uniform deployment. *Sij* can be denoted by the equation below:

$$Sij=SAOiB+SAOjB-SAOiBOj, \quad (1)$$

Where SAOiB and SAOiB signify the region of zone AOiB and AOjB, respectively, and SAOiBOj denotes the area of rhombus AOiBOj. Then, based on geometry theory, we can without difficulty get that

$$Sij=2R^2cos-1Dij/2R-Dij\sqrt{R^2-D^2ij/4}, \quad (2)$$

Where *R* is the communication radius of node.



V. PERFORMANCE AND RESULT

A fair comparison use the same noise distribution for honest nodes in E-SCDA, and the noises will be regenerated when they exceed the decaying bound. The comparison E-SCDA and PPAC have similar convergence speed while PPAC cannot fully converge, especially when α and ρ are large. This is because unlike E-SCDA, the dishonest nodes use the normal distribution random variables as the added noises and set φ = 1 for PPAC, i.e., PPAC is more vulnerable. We also compare our algorithm with that proposed.

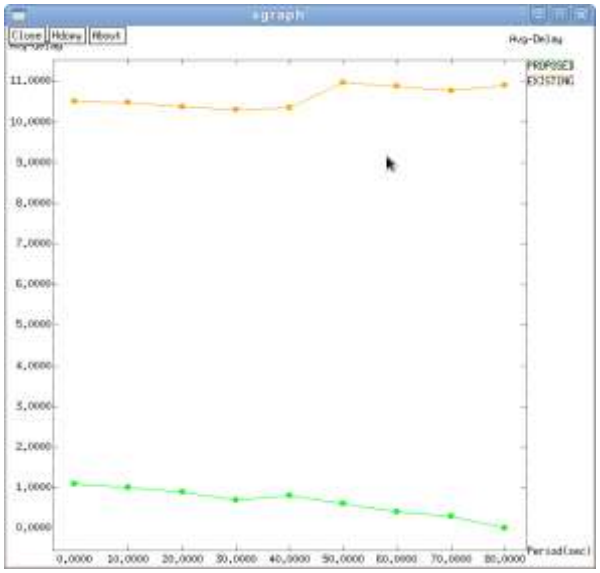


Figure 1: Average Delay

The above figure shows the average delay of the transmitted packets and also shows the best comparison between the average delay of a E-SCDA algorithm and PPAC algorithm. The average delay ofthe PPAC algorithm is minimized when compared with the E-SCDA algorithm. The energy consumption of an E-SCDA algorithm and the PPAC algorithm is fairly compared and shown in figure 2. In PPAC algorithm the energy consumed is very low than E-SCDA algorithm.

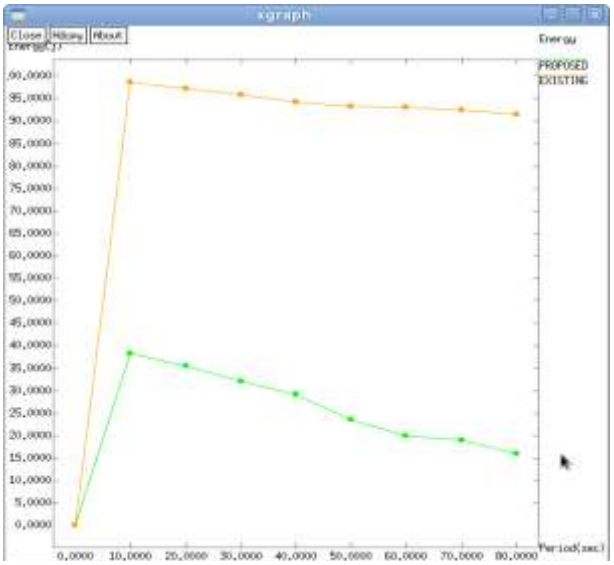


Figure 2: Energy

Figure 3: Comparison of ESDCA and PPAC

The main reason is that both of the existing algorithms add decaying and zero-sum noises to the traditional average consensus process but do not consider the presents of the dishonest nodes.

CONCLUSION AND FUTURE WORK

To moderate the contamination from untrustworthy nodes, we propose an enhanced secure consensus-based data aggregation (E-SCDA) algorithm that enables neighbours to identify unscrupulous hubs, and determine the blunder bound when there are imperceptible deceptive hubs. The underlying condition of every hub can be isolated into two sections and they will be sent with added noises to two neighbour sets. This system acquaints extra noises with the underlying state for protection conservation and hubs to screen their neighbours to distinguish any unfortunate behaviour. To accomplish it, we structure an observing procedure as a defend component, which compels the deceptive hubs for guaranteeing the exactness of total. Security safeguarding information collection answer for have such robustness and guarantee limited blunder with the nearness of unscrupulous nodes.Iterative filtering technique hold extraordinary guarantee for such a reason.

REFERENCES

[1] Rezaul Karim, Md. Hasan Furhad, Md. Khaliluzzaman and Md. Ariful Islam Khandaker," IMPROVING THE PERFORMANCE OF DATA DELIVERY IN WIRELESS SENSOR NETWORKS", JOURNAL OF TELECOMMUNICATIONS, VOLUME 8, ISSUE 2, MAY 2015

[2] Dr. Debmalya Bhattacharya," SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS", IEEE TRANSACTION, ISSN: 2248-9622, Vol. 4,

[3] Mrs. B.Vidhya, Mrs. Mary Joseph , Mr. D. Rajini Girinath , Ms. A. Malathi ,"ENVIRONMENT BASED SECURE TRANSFER OF DATA IN WIRELESS SENSOR NETWORKS",International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015

[4] S.Suresh, Giridhar. R"SECURED DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS" International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 6, June 2016

[5] O.Deepa, Dr. G. Naga Rama Devi," PROVIDING END TO END DATA SECURITY IN WIRELESS SENSOR NETWORKS", International Research Journal of Engineering and Technology, Volume: 03 Issue: 07 | July-2016

[6] Ms. Sarita V. Halde, Prof. Sucheta T. Khot," BIG DATA IN WIRELESS SENSOR NETWORK: ISSUES & CHALLENGES", International Journal of Advanced Engineering, Management and Science (IJAEMS), [Vol-2, Issue-9, Sept- 2016]

[7] Saeid Pourroostaei Ardakani, Allameh Tabataba'i , Tehran, Iran," DATA AGGREGATION ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS: A TAXONOMY", International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.2, March 2017

[8] M. Kowsigan, M.Rubasri, R.Sujithra, H.Sumaiya Banu,"DATA SECURITY AND DATA DISSEMINATION OF DISTRIBUTED DATA IN WIRELESS SENSOR NETWORKS", Int. Journal of Engineering Research and Application, ISSN : 2248-9622, Vol. 7, Issue 3, (Part -4) March 2017, pp.26-31

[9] Dr. M.Sivaram, 2Dr. Amin Salih Mohammed, 3V.Porkodi, 4V.Manikandan," SECURING THE SENSOR NETWORKS ALONG WITH SECURED ROUTING PROTOCOLS FOR DATA TRANSFER IN WIRELESS SENSOR NETWORKS",IEEE journal of selected topics on secure computing, October 2018, Volume 5, Issue 10

[10] Jinwei Liu, Haiying Shen, Lei Yu, Husnu S. Narman, Jiannan Zhai, Jason O. Hallstrom" CHARACTERIZING DATA DELIVERABILITY OF GREEDY ROUTING IN WIRELESS SENSOR NETWORKS", IEEE journal of selected topics on secure computing, Vol.5, No.3, April 2017

[11] Lokesh B. Bhajantri, Shilpa H. Rathod," DATA AWARE ROUTING IN WIRELESS SENSOR NETWORKS", International Journal on Future Revolution in Computer Science & Communication Engineering, March 2016, Volume: 4 Issue: 3

[12] Andreas Willig, Holger Karl," DATA TRANSPORT RELIABILITY IN WIRELESS SENSOR NETWORKS —A SURVEY OF ISSUES AND SOLUTIONS" EURASIP Journal on Wireless Communications and Networking, April 2016

[13] Neha Dhotre Prof. Ramesh Jadhav," A MULTI OWNER – MULTI USER DATA TRANSMISSION FOR SECURED INFORMATION IN WIRELESS SENSOR NETWORKSA MULTI OWNER – MULTI USER DATA TRANSMISSION FOR SECURED INFORMATION IN WIRELESS SENSOR NETWORKS"IJIRST –International Journal for Innovative Research in Science & Technology| Volume 3 | Issue 01 | June 2016

[14] Anu Chaudhary, Dr. Rajeev Kumar, "AN ASSESSMENT OF DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS WITH ENHANCEMENT TO THE SECURITY AND RELIABILITY", International Journal in IT and Engineering (Impact Factor- 6.341), Vol.05 Issue-01, (January, 2017)

[15] Ashvinkumar K. Selokar Arun G. Katara," IMPROVED SECURED DATA AGGREGATION IN WIRELESS SENSOR NETWORK BY ATTACK DETECTION AND RECOVERY MECHANISM", International Journal for Scientific Research & Development| Vol. 3, Issue 08, 2016

[16] Gonugunta Tulasi, R.Suresh," SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS: AGAINST PACKET DROPPING ATTACKS", International Research Journal of Engineering and Technology, Volume: 03 Issue: 07 | July-2016

[17] An Wang, Wentao Chang, Songqing Chen, Aziz Mohaisen" DELVING INTO INTERNET DDOS ATTACKS BY BOTNETS: CHARACTERIZATION AND ANALYSIS", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 7, NO. 3, JULY 2018

[18] Arham Alam Sachin Chaudhary," TRANSMISSION OF DATA IN WIRELESS SENSOR NETWORK USING ADAPTIVE CLUSTERING", International Journal for Scientific Research & Development| Vol. 5, Issue 09, 2017

[19] Guo Chen , Yuanwei Lu, Yuan Meng, Bojie Li, Kun Tan, Dan Pei , Peng Cheng, Layong Luo, Yongqiang Xiong, Xiaoliang Wang, and Youjian Zhao, "FUSO: FAST MULTI-PATH LOSS RECOVERY FOR DATA CENTER NETWORKS", IEEE/ACM Transactions on Networking (Volume: 26, Issue: 3, June 2018)

[20] Soheil Feizi, Muriel M´edard, Gerald Quon, Manolis Kellis, and Ken Duffy," NETWORK INFUSION TO INFER INFORMATION SOURCES IN NETWORKS ",IEEE Transactions on Network Science and Engineering 2018