Secure Data Aggregation Techniques Using CPDA And SMART Algorithm For Privacy- Preserving In Wireless Sensor Network

Prajakta Waghmare[1], Anup Gade[2], Abhay Rewtkar[3]
[1]Dept of Information Technology
[2, 3]Assistant Professor, v Dept of Information Technology
[1, 2, 3] Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur

Abstract- *Latest advancements in micro-electro-mechanical-system (MEMS) and wireless communication technology, opens the way for the growth in applications of wireless sensor networks (WSNs). Data aggregation in wireless sensor networks eliminates redundancy to improve bandwidth utilization and energy efficiency of sensor nodes. WSN consists of a large number of resource- constrained sensor nodes and is usually deployed in unattended area to collect specific information. Energy consumption is always a major concern in the research field of wireless sensor network. Thus, data aggregation schemes emerged and were deployed for prolonging network lifetime by reducing data transmitted within the network. In this paper, we present two techniques for privacy-preservation of data aggregation. First is Cluster-based Private Data Aggregation (CPDA) and second is Slice-Mix- Aggregate (SMART). In these new private data aggregation algorithms– CPDA and SMART– some messages are encrypted to prevent attackers from eavesdropping.*

Keywords- WSN, Data aggregation, CPDA, SMART.

I. INTRODUCTION

A remote sensor organize (WSN) is an impromptu system made out of little sensor hubs where hubs are speak with one another remotely and associated with one sensor. WSN are developing uses of unavoidable figuring, comprising of some little, low force, and astute sensor hubs and at least one base stations. WSN utilized in extremely expansive application including both military and regular citizen use, for example, reconnaissance [1], following at basic offices [2], checking creature natural surroundings [3], wellbeing observing system[4]. Unique qualities of WSNs are asset imperatives on vitality and computational force and security of information transmission.

A. Data Aggregation

Data aggregation is refers to as the process of data gathering, aggregating and collecting the useful data for wireless network. The main goal of data aggregation is to tally the data then aggregate that data in an energy efficient privacy manner, so that the period of network lifetime is enhanced and the power is optimized. In this paper, different data aggregation technique, various privacy preserving energy-efficient algorithm and security process for data aggregation on wireless sensor networks are presented. A Wireless Sensor Network [1,2,3,4] (WSN) comprises a large number of sensor nodes deployed in the monitoring area. Each sensor node is usually a battery-powered tiny device, which is responsible for sampling some attributes like temperature, humidity, pressure, luminous intensity, voice and image from surrounding area. Sensor nodes use simple radio module to communicate with each other. The nodes' transmitting range is very limited. After being deployed, all the sensor nodes are self-organized as an Ad-Hoc network. Data exchange between two sensor nodes usually needs to relayed by many intermediate nodes. There is a data processing/storge center called sink or base station, which is responsible for receiving users' queries, distributing queries to the relating sensor nodes, gathering data from the network and return results to users. Sensor nodes are usually deployed where personnel are difficult to reach, and it is impractical to exchange batteries for them, so how to save energy to prolong the life time of each sensor node becomes the main optimizing goal of WSNs. Research results [5,6] show that among all the operations of sensor nodes, wireless communication is the dominating factor for energy consumption. Thus, in-network query processing is necessary for sake of communication efficiency. In recent years, data privacy of WSNs gets more and more attention [7,8,9,10]. Many reasons make adversaries interested about some nodes' data in a WSN. For example, in a WSN deployed in the battle filed, our enemies want to intercept the data of reporting enemies' invasion; Pharmaceutical advertisers want to get the data of people's physiological indicators collected from the sensors worn by users; To know the location of wildlife, poachers want to access the data of sensor nodes deployed in the wild for wildlife monitoring. Such application scenarios have a strong need for data privacy protection [11].In most applications of WSNs, users are more interested in the overall

situation of the data of the whole network rather than the data of a certain node. Therefore, the queries issued by users are mainly aggregation queries, e.g., query the average of the temperature sampled by all the nodes or query the minimum value of the humidity sampled by the nodes in a given area. Characteristics of WSNs determine that the processing of aggregation queries should be done in-network rather than by the sink collecting the raw data of each node. Some privacy-sensitive application scenarios require us to consider data privacy in addition to efficiency while dealing with aggregation queries. Data privacy in WSNs means that the data of any node cannot be obtained by the nodes other than the sink.

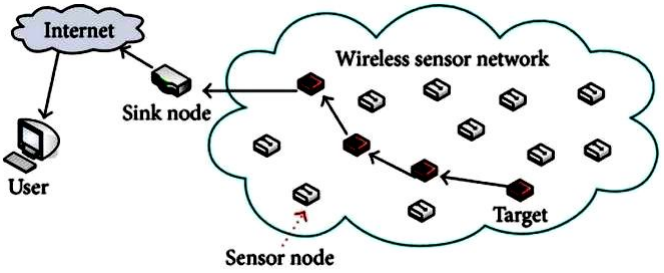


Fig.1 Wireless sensor network

II. PROBLEM DEFINITION

Giving productive information accumulation while saving information protection is a difficult issue in remote sensor systems look into. The remote sensor organize is little estimated, minimal effort sensor hubs, which detects the remote and unfriendly condition. The restriction of low power intensity of a sensor hub and constrained vitality capacity makes the remote sensor organize disappointment. In the *CPDA* scheme, sensor nodes are formed randomly into clusters. Within each cluster, our design leverages algebraic properties of polynomials to calculate the desired aggregate value. At the same time, it guarantees that no individual node knows the data values of other nodes. The intermediate aggregate values in each cluster will be further aggregated (along an aggregation tree) on their way to the data sink. In the *SMART* scheme, each node hides its private data by slicing it into pieces. It sends encrypted data slices to different intermediate aggregation nodes. After the pieces are received, intermediate nodes calculate intermediate aggregate values and further aggregate them to the sink. In both schemes, data privacy is preserved while aggregation is carrying out. We evaluate the two schemes in terms of efficacy of privacy preservation, communication overhead, and data aggregation accuracy, comparing them with a commonly used data aggregation scheme *TAG* [4], where no data privacy is provided. Simulation results demonstrate the efficacy and efficiency of our schemes.

III. PROPOSED SCHEME

In this paper, we present two techniques for privacy-preservation of data aggregation. First is Cluster-based Private Data Aggregation (CPDA) and second is Slice-Mix-Aggregate (SMART). In these new private data aggregation algorithms– CPDA and SMART– some messages are encrypted to prevent attackers from eavesdropping.

Data privacy is a challenging issue in WSNs during data transmission as well as data aggregation. In this we exists a lot of related works already in the literature. Some of the highlights of such relevant works are elaborated in the section below.

Requirements of Private Data Aggregation:

rotecting the data privacy in many WSNs applications is a major challenge. The following criteria summarize the desirable characteristics of a private data aggregation scheme:

Efficiency: The main goal of data aggregation is to reduce the number of messages transmitted within the sensor network, thus it reduces energy consumption and hence it enhances the longevity of network. In private data aggregation schemes, additional overhead is introduced to protect the privacy. However, a good private data aggregation scheme should keep that overhead as small as possible. In this paper, the proposed scheme improved the security of network and keeps the network system at low energy cost level.

Privacy: Critical security issue in the design of secure data aggregation scheme is the preservation of private data. Each node's data should be only known to itself. Hence, the private data aggregation scheme can handle some extent of attacks and collision among compromised nodes. When a sensor network is under a malicious attack, it is possible that some nodes may be uncovering the private data of other nodes. Furthermore, wireless links may be eavesdropped by attackers to reveal private data. A good private data aggregation scheme should be robust to such attacks.

Accuracy: An accurate aggregation of sensor data is desired, with no other sensors should know the exact value of any individual sensor. Accuracy should be a defined to estimate the performance of private data aggregation schemes. In a certain time, the lots of data are transmitted in the network, and then it increases the risk of data loss or transmitting collision. Hence, in this proposed scheme, we need to reduce the data traffic in network while providing the preservation of data privacy.

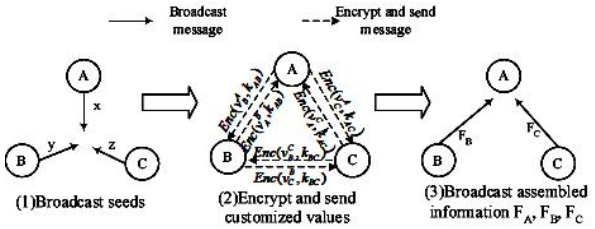


Fig 2 Formation of Clusters

A. Cluster-based approach:

In energy-constrained sensor networks of large size, it is not possible for sensors to transmit the data directly to the base station. In such scenarios, Cluster based approach is hierarchical approach. In cluster based approach, whole network is divided in to several clusters. Each cluster has cluster members then these cluster members elects the cluster head node which has high residual energy. Cluster heads do the role of aggregator which aggregate data received from cluster members and then these cluster heads communicate with base station for the transmission of that aggregated data.

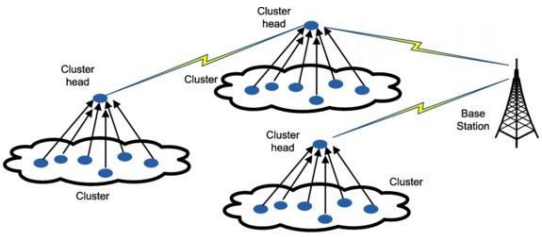


Fig3 Cluster based data aggregation

1) The network model

The basic idea of CPDA is to introduce noise to the raw data sensed from a WSN, so that an aggregator can obtain accurate aggregated information but not individual data points. The noises in CPDA are designed carefully to control the cooperation between different sensor nodes, such that the precise aggregated values can be obtained by the aggregator. It is totally different from privacy-preserving data mining in which noises are independently generated (at random) and therefore leads to imprecise aggregated results. CPDA categorizes sensor nodes as cluster members and cluster heads. Between them they have one-to-many mapping. The responsibility of the cluster head is to aggregate data from cluster members and securely transmitted to the base station. For secured communication, each pair of communication nodes uses a different shared key.

2) Key Distribution and Management

To prevent from message eavesdropping attacks the proposed scheme uses a random key distribution mechanism for encrypting messages. The key distribution scheme has three phases: [1] key pre distribution, [2] shared-key discovery, and [3] path key establishment.

These phases are described briefly as follows: For the sensor node there are k keys form a key ring. During the key-discovery phase, each sensor node identifies which of its neighbors share a common key with itself by invoking and exchanging discovery messages.

3) Cluster-Based Private Data Aggregation

The CPDA scheme works in five phases: [1]cluster formation, [2] computation of aggregate results in clusters, [3] cluster data aggregation, [4] Intermediate node, and [5] Sink. These phases are described below:

i) cluster formation: A query server Q sends a query by a HELLO message. When the HELLO message reaches a sensor node, it elects itself as a cluster head with a pre- defined probability pc. If a node becomes a cluster head, it forwards the HELLO message to its neighbors. If any HELLO message arrives at the node, it decides to join the cluster formed by its neighbor by sending a JOIN request message. This process is repeated and multiple clusters are formed so that the entire WSN becomes a collection of a set of clusters.

ii) computation of aggregate results in clusters: In this phase, aggregation is done by each cluster. The computation is elaborated with an example of a simple case in which a cluster contains three members: A, B, and C, where A is the assumed as the cluster head (aggregator), B and C is the cluster members. Let a, b, c represent the private data of nodes A, B, and C respectively.

iii) cluster data aggregation: The CPDA scheme has been implemented on top of a protocol known as 'Tiny Aggregation' (TAG) protocol .Using the TAG protocol, each cluster head node sends the sum of values in its cluster to the query server through a TAG routing tree whose root is situated at the server.

iv) Intermediate node: In this module the encrypted data is send to the sink node via intermediate node. The encrypted data is set of cipher texts. Then this

intermediate node calls forward subroutine to forward encrypted data to the sink.

v) Sink: Sink is a base station, this is a final stage, and the data are received from different wireless sensor node by this stage. In this stage sink receives the cipher texts and performs decryption process by using the private key. Once the decryption is done plain texts are generated which original message or data is sent by the source (sensor).

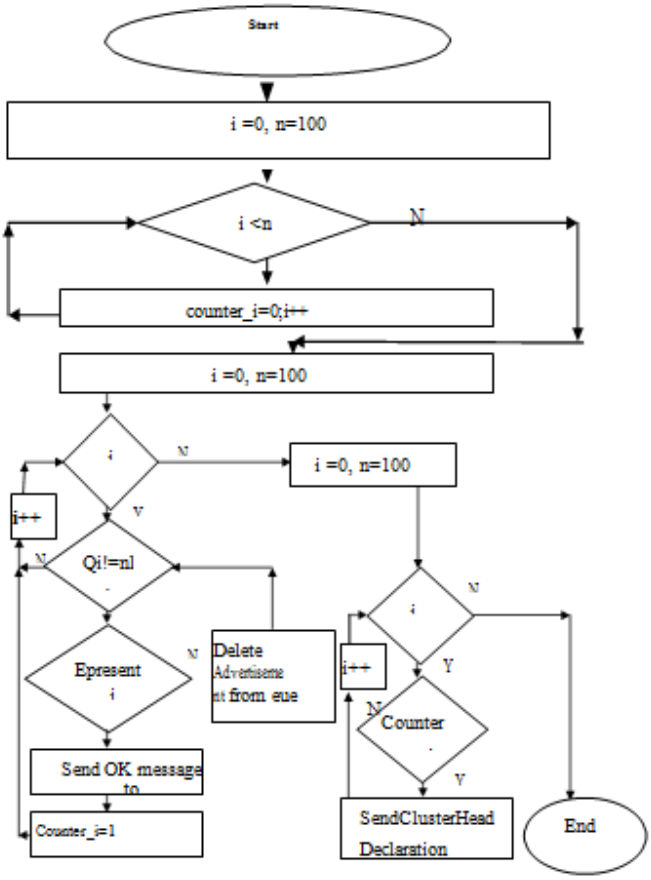
CPDA Algorithm

IDi : ID of node i.
Rf : Radius of frequency / range of communication.
Qi : Queue of sensor i.
Epresent_i : Present energy of node i.

Procedure Cluster_Formation (n)

1. For each Next iteration
2. For each IDi
3. Counter =0
4. For each IDj within Rf of IDi
5. Advertise Epresent_i
6. For each IDi
7. Put all incoming advertisements from sensors j into Qi
8. For each IDi
9. While Qi is not empty
10. If Epresent_i <= Epresent_j
11. Send ok message to IDj
12. Counter = 1
13. Else
14. Delete this advertisement from queue
15. For each IDi
16. If counter =0
17. Send cluster_head_declaration message to IDj within Rf

CPDA Flowchart



B. SMART approach:

Another scheme proposed for privacy- preservation in WSN is Slice-Mix-Aggregate (SMART). This scheme is used for individual protection of data in the aggregation of SUM. The technique used initially breaks the original data into pieces and then randomly recombines that data. This scheme involves three steps. [1] Slicing, [2] mixing, and [3] aggregating.

1) Slicing:

In this step, within h hopes j neighbor nodes are selected by each sensor node to build a set S. Then, the data is sliced into J pieces. After keeping one piece for itself, it transmits the other (J - 1) encrypted pieces to (J – 1) sensors selected at random from set S.

2) Mixing:

In this step, each sensor upon receipt of data from other sensors decrypts the data via the shared key. Every sensor waits to make certain that the process of round aggregation data slicing and receipt are finished.

3) Aggregating:

In this step, data is aggregated by intermediate sensor and transmitted to the BS. Here also for encryption of certain data, a random key distribution scheme is used.

The advantage of this scheme is the less computation overhead. In this work, both CPDA and SMART are taken as the perturbation primitives for data privacy- preservation in WSNs during data transmission and aggregation.

SMART Algorithm

Two phase protocol i-Sensor node
Rf- Range of frequency v-node under Rf
Qi : Queue of sensor i.
Cprob- Predefined probability of each sensor.
CHprob- probability of being cluster head.

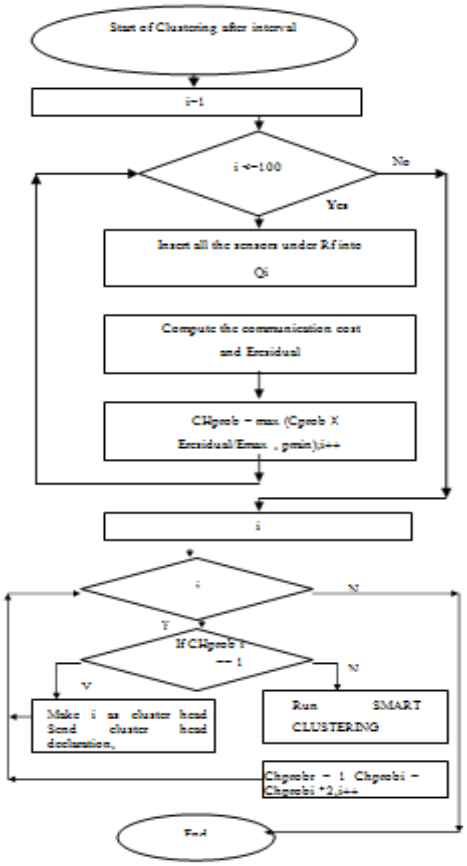
Phase I

1. For each sensor i
2. Qi <-- v: v under of Rf
3. Compute the communication cost of i after investing on Qi. And find the Eresidual
4. CHprob = max (Cprob × Eresidual/Emax , pmin)

Phase II

1. For each sensor i
2. If (Chprobi == 1)
3. cluster_head_declaration message
4. else if
5. Advertise Epresent_i each j within Qi
6. Queue all incoming advertisements from sensors j into adv_Qi
7. Compare Epresent_i with Epresent_j in adv_Qi
8. If (Epresent_i >= Epresent_j)
9. cluster_head_declaration message
10. else
11. find j in adv_Qi having Epresent_j >= Epresent_i
12. compare this Epresent_j with other sensors in adv_Qi and find the highest energy sensor let its r
13. do Chprobr = 1
14. do Chprobi = Chprobi *2

SMART Flowchart



IV. EXPERIMENTAL RESULT

Table: Simulation Result

	Max no. of node in a cluster in Proposed algorithm	Maximum number of node In a cluster in random algorithm	Number of request Proposed algorithm	Number of request Random algorithm	Total Energyin cluster formation in random algorithm	Total energy in cluster information in Proposed algorithm
Simulation 1	25	50	76	200	75.0005	51.0005
Simulation 2	27	46	68	200	73.0005	48.0005
Simulation 3	24	38	65	200	69.0005	45.0005
Simulation 4	23	29	56	200	64.5005	40.0005
Simulation 5	21	37	69	200	68.5005	45.5005
Simulation 6	22	30	59	200	65.0005	41.0005
Simulation 7	27	32	63	200	66.0005	45.5005
Simulation 8	24	39	66	200	69.5005	45.5005
Simulation 9	26	35	72	200	67.5005	49.5005
Simulation 10	24	42	68	200	71.0005	46.5005

V. RESULT

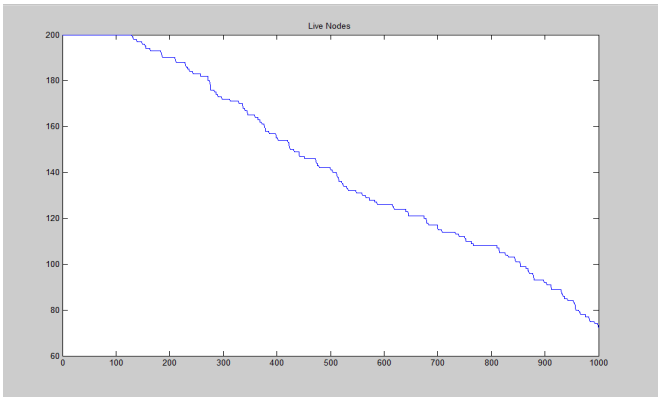


Fig3 Live nodes

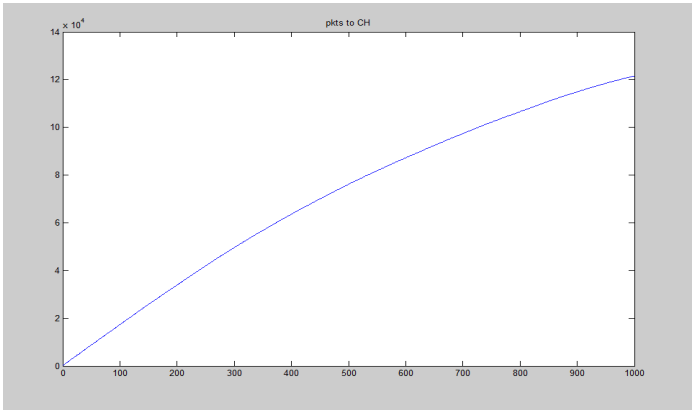


Fig3 Packets to CH

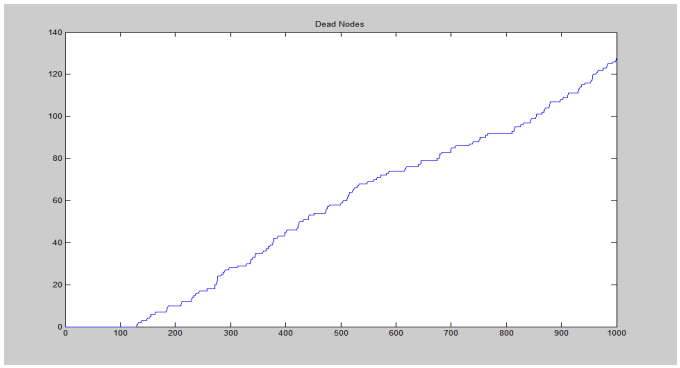


Fig3 Dead nodes

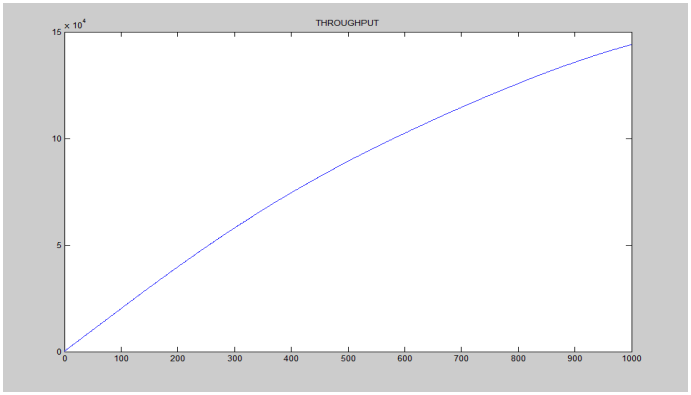


Fig3 Throughput

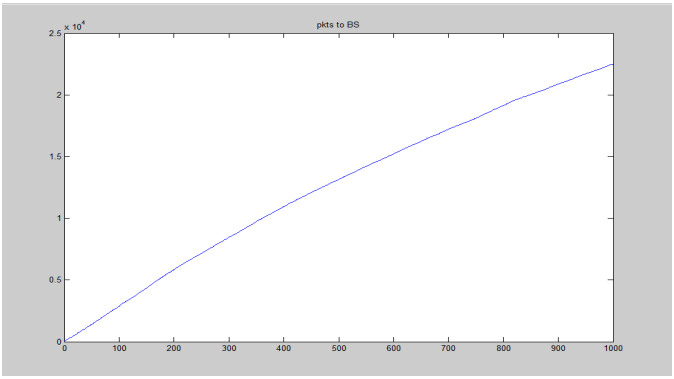


Fig3 Packets to BS

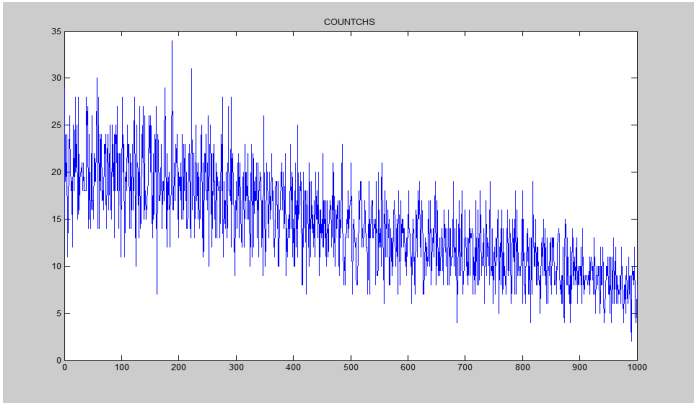


Fig3 Count CHS

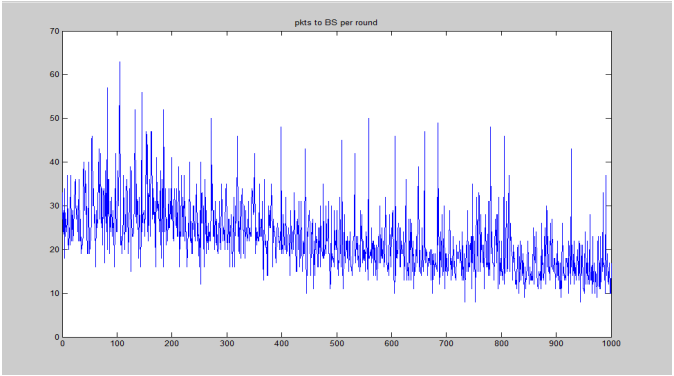


Fig3 Packets to BS per round

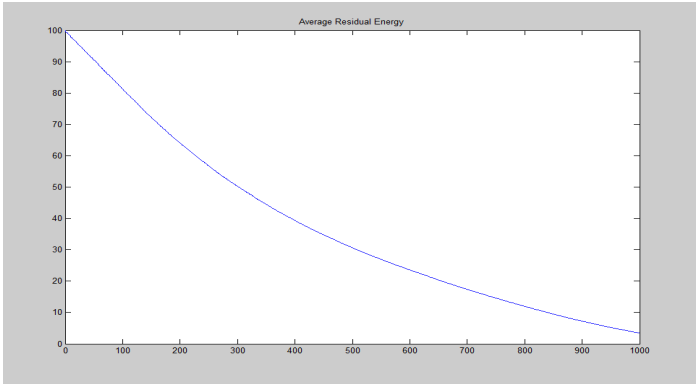
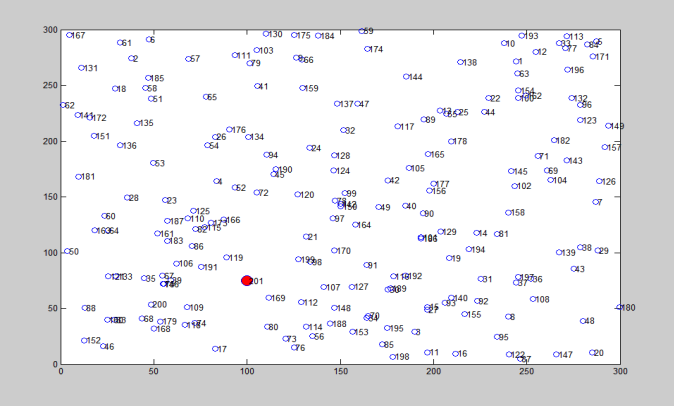
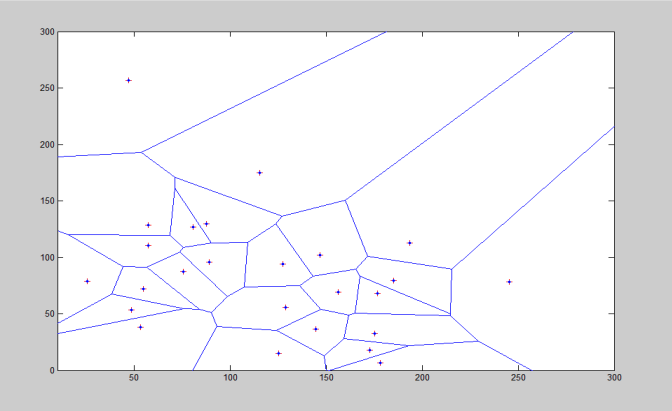


Fig3 Average residual energy





Giving effective information accumulation while safeguarding information security is a difficult issue in remote sensor systems examine. In this article, we present two protection safeguarding information conglomeration plans for added substance accumulation capacities, which can be reached out to estimated MAX/MIN total capacities. The principal plot - Bunch based Private Information Accumulation (CPDA)- - use grouping convention and mathematical properties of polynomials. It has the benefit of acquiring less correspondence overhead. The subsequent plan - Cut Blend Total (Savvy)- - expands on cutting strategies and the affiliated property of expansion. It has the benefit of causing less calculation overhead. The objective of our work is to overcome any issues between community oriented information assortment by remote sensor systems and information protection. We survey the two plans by security safeguarding adequacy, correspondence overhead, and information total exactness. We present reenactment consequences of our plans and contrast their exhibition with a common information collection plot (TAG), where no information security assurance is given. Results show the adequacy and proficiency of our plans.

VI. FUTURE WORK

The exploration work can be stretched out further to adjust the proposed calculation to expand the correspondence among sensor on diminishing the vitality utilization and henceforth to upgrade the life span of system and furthermore give protection safeguarding efficiency, communication efficiency, correspondence overhead and conglomeration exactness. In future research work, we will concentrate on the planning of secure information total plan with the capacity to ensure information uprightness and furthermore the bunching based information collection plan will be acquainted with transmit with security.

VII. CONCLUSION

Giving effective information total while saving information security is a difficult issue in remote sensor systems. Right now, propose two private-saving information collection plans – CPDA, and Keen – concentrating on added substance information total capacities. The primary driver of information total calculations is to count the information and total that information in a vitality proficient security way, with the goal that the time of system lifetime is upgraded and the force is advanced. It gives the parameters, for example, protection conservation viability, correspondence overhead, total exactness, and computational overhead. The proposed plot has no correspondence and calculation overhead and negligible preparing necessities making it appropriate for sensors with restricted assets

REFERENCES

[1] Ganesh R. Pathak, Suhas H. Patil, and Jyoti S. ryambake"Efficient and Trust Based Black Hole Attack Detection and Prevention in Wireless Sensor Networks", International Conference on Computer Science and Business Informatics, ISSN: 1694-2108, Vol.14

[2] 2014. 2. Sheela. D, Srividhya.V. R., Asma Begam, Anjali and Chidanand G. M."Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent",International Conference on Artificial Intelligence and Embedded Systems (ICAIES)July 15-16, Singapore,2012.

[3] Jaspreet Kaur, Vinod Kumar" An Effectual Defense Method Against Gray-Hole Attack in Wireless Sensor Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3, 2012, 4523- 4528.

[4] X.-Y. Xiao, W.-C.Peng, C.-C.Hung, and W.-Lee, "Using SensorRanks for in-network detection of faulty readings in wireless sensor networks," in Proceedings of the 6th

ACM international workshop on Data engineering for wireless and mobile access, ser. Morbid‟07, 2007, pp. 1–8.

[5] He, W., Liu, X., Nguyen, H. V., Nahrstedt, K., and Abdelzaher, T. 2011. “Privacy preserving data aggregation for information collection "ACM Transaction Sensor Network. Article 6 (August 2011.DOI = 10.1145/1993042.199)3048.

[6] H.-S. Lim, Y.-S. Moon, and E. Bertino, “Provenancebased trustworthiness assessment in sensor networks,” in Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, ser. DMSN ‟10, 2010, pp. 2–7.

[7] T. Arampatzis , J. Lygeros, and S. Manesis, “A Survey Of Applications Of Wireless Sensors And Wireless Sensor Networks”, In Mediterranean Conference On Control And Automation MED05, Nicosia, Cyprus, 2005.

[8] Lu Gao,Zhongmin Li,“Energy Consumption Balanced Cluster Head Selection Algorithm for Wireless Sensor Networks“International Conference on Computer Science and Applications,IEEE-2013

[9] Mahmoud M. Salim, Hussein A. Elsayed, Salwa H.El Ramly,” PR – LEACH: Approach for Balancing Energy Dissipation of LEACH Protocol for Wireless Sensor Networks",31st National Radio Science Conference (NRSC),April 28-30, 2014 Ain Shams University, Egypt.

[10] Sushant Miglani , Rajoo Pandey ,“ Optimization of Clustering Probability of LEACH Protocol for Lifetime Maximization of Wireless Sensor Networks ”2nd International Conference On Parallel, Distributed and Grid Computing, IEEE 2012 .