Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.682 – 691

RESEARCH ARTICLE

AN IMPROVED GGP BASED CLUSTER HEAD ROUTING FOR RECOVERING AND SENSING DATA AGGREGATION INTEGRITY IN WIRELESS SENSOR NETWORKS

K.Sujana Banu[1], S.Vignesh[2], K.Banazeer[3]

[1]Assistant Professor, Department of Information Technology, Sri Eshwar College Of Engineering, Coimbatore, Tamilnadu, India

sujanakadhar2007@gmail.com

[2]Assistant Professor, Department of Information Technology, Sri Eshwar College Of Engineering, Coimbatore, Tamilnadu, India

vigneshbtech76@gmail.com

[3]PG Scholar, Department of MCA, Hindustan Institute Of Technology, Coimbatore, Tamilnadu, India

banazeer.mca@gmail.com

Abstract— In earlier works several data aggregation schemas based methods have been proposed to overcome the problems of the privacy in wireless sensor networks. These methods provides efficient result to analysis of secure data with traditional aggregation because cluster heads can straightforwardly comprehensive the cipher texts not including decryption; accordingly, reduces the transmission overhead in wireless sensor networks. But still the data aggregation schema occurs two major problems in aggregation process; the major cluster head does not receive the entire data and cannot authenticate data truthfulness and dependability via between message digest. To conquer these problems in this work first proposed a Generalized Geometric programming method to select best cluster head or aggregation of the data by finding the shortest hop inter-CH routing. For this scheme, transmission overhead reduced and improve the coverage-time maximization is created as a signomial optimization difficulty with the purpose of is capably solved using Generalized Geometric Programming (GGP) techniques. The optimal cluster sizes of the individual data aggregation are achieved beginning this examination. Experimentation results show that the transmission overhead is still concentrated even if our approach is recoverable on common sensing data. Furthermore, the design has been widespread and adopt on together homogeneous and heterogeneous wireless sensor networks data aggregation schemas while using GGP clustering (or) cluster head routing selection.

***Keywords*— Wireless Sensor Networks; Data Aggregation Using Pattern Codes; Pattern Comparison by Cluster-Head RCDA; Routing; Generalized Geometric Programming (GGP)**

I. INTRODUCTION

Wireless sensor networks (WSN) have been principally developed in numerous applications, e.g., health care, environment monitor, accident report, etc. A WSN is collected great amount of sensors which work together to

each other. Each sensor perceive a goal enclosed by its radio range, it achieve easy computations, and correspond with other sensors. Sensors are controlled in battery power, communication, and computation capability; consequently, control power consumption is a complicated disquiet for a WSN. Newly, a convenient result called information aggregation is introduced.

Data aggregation is to achieve cluster head if the complete network broken up into numerous groups recognized as clusters. For instance, in military fields, sensors are organized to examine radiation. The main station might necessitate the maximum value of each sense data to trigger the in require of consideration reaction; A well efficient methods to aggregate these schema is known as Concealed Data Aggregation (CDA) based on two process. CDA present together end-to-end encryptions as on form as in network processing in WSN. CDA be appropriate privacy homomorphism (PH) encryption with preservative homomorphism, cluster heads are predominantly consummate of complete adding up together operations on encrypted numeric information. Later, a numeral of PH-based data aggregation methods has been anticipated to get superior protection levels.

Security in data communication is an extra important issue to be calculated whereas designing WSN. Even though data aggregation moreover safeguard in WSN has been considered expansively, mostly outstanding of our information, there is no earlier investigate taking into thought of data aggregation as well as protection together. The pattern generation is well efficient method to solve the problem of the best cluster head selection for routing in WSN on both heterogeneous and homogenous pattern generation. The cluster-head also has corresponding dependability as the sensor nodes in data aggregation in WSN. It sends the model starting point frequently to each dynamic sensor nodes persist the confidentiality of the replica codes and then reception replica codes on the sensor nodes second-hand for a time period T. These sensor nodes can be position to sleep mode to safeguard authority.

The safety protocols second-hand in the sensor networks be required to be suspiciously considering the power and computational reserve constriction of WSN. Symmetric key cryptographic algorithms are working to maintain safety in WSNs. A clustering method with the intention is developed in the perspective of through hop inter-CH routing. For this system, coverage-time maximization is prepared as an optimization difficulty with the intention of professionally resolved by means of generalized geometric programming (GGP) techniques. The best possible cluster sizes are finding from this analysis. Because CDA apply privacy homomorphism (PH) encryption through preservative homomorphism, cluster heads are proficient of performing calculation operations on encrypted numeric data. It achieved better safety data aggregations than the PH encryption for RCDA.

II. INTRODUCTION

Wireless sensor networks (WSNs) are categorized through a self-motivated topology, imperfect channel bandwidth and restricted power consumption at the nodes. Since of this description, paths concerning source nodes through destinations making communication over WSNs complicated. Designing a well-organized and consistent routing protocol designed for such networks is a difficult problem [1–3]. Multipath routing addresses this difficulty by provided that additional than individual route to a target node. Source and middle nodes can make use of these routes as most important and support routes. In WSN the grouping of the nodes together, data packets send to the sender to receiver and aggregate the packets between sources to destination with less data redundancy. Consequently, energy efficiency is the most important principle of these routing protocols.

Directed Diffusion [4], and SAR [5] two data aggregation methods consistent data processing. Beginning this point onward, focal point on the multipath routing approach and the associated issues that be supposed to be well thought-out in the plan of these protocols designed for wireless sensor networks. Newly, a realistic result called data aggregation [6-8] was established. The unique conception is to aggregate numerous sensing data by the stage of arithmetical operations.

On the other way numerous studies have proposed in earlier works [9-11] challenge to provide privacy. That is, an aggregator can straightforwardly accomplish adding operations on arithmetical data or information. CDA [9] places additional importance on reactive attacks. More particularly, it regard as if challenger can eavesdrop the interactions on the atmosphere. After CDA, following explore [9], [10] have been anticipated to attain elevated security levels. They regard as the subsequent situation. If sensors inside the similar cluster encrypt their data all the way through the common secret key, and decrypt the similar data at server side. Nevertheless, the adversary can still masquerade as supplementary legal sensors to send the copied ciphertexts to the cluster head through the equivalent public key. Validity of data is not sustained. Cooperation cluster head may selectively go down a number of cipher texts and name in the combined process. This type of attack is known as forwarding attack [12]. Providentially, preceding study [13], [14] anticipated method to protect alongside this attack.

III. ROUTING AWARE OPTIMAL CLUSTER PLANNING USING GGP

Wireless sensor networks (WSN) have been principally developed in numerous applications, e.g., health care, environment monitor, accident report, etc. A WSN is collected great amount of sensors which work together to each other. Each sensor perceive a goal enclosed by its radio range, it achieve easy computations, and correspond with other sensors. Sensors are controlled in battery power, communication, and computation capability; consequently, control power consumption is a complicated disquiet for a WSN. Newly, a convenient result called information aggregation is introduced. The data aggregation and in-network dispensation move towards is to come together the data received beginning dissimilar sources at specific aggregation points eliminate redundancies by the stage simple processing at the aggregation points, and reduce the whole quantity of data communication earlier than familiar data to the exterior BS. Every one node forward sensed standards to their neighbour/close relative. Every node has to remain its family earlier than computing the collective and forward it. The quantity of the broadcasted data depends on the category of the cumulative task. Key Setup BS cannot be cooperation and it has a protected machine to confirm its broad-cast communication to everyone the nodes in the hierarchy and each nodule is able to authenticate the external broadcast communication.

Several number of data aggregation schema have been proposed in earlier works, these aggregation methods transmit aggregation outcome to everyone sensors. Then, each sensor authenticate with the purpose of its sensing data be definitely calculated. A different effort is able to essentially count up and addition constant if a small number of cooperation sensors introduce false values. Random sampling methods with the intention of make possible aggregation enquiry to not simply identify malicious sensors, however in addition to accept them. Effort to present privacy. With the intention of an aggregator can immediately complete adding together process on encrypted numeric data. But still the sensors inside the similar cluster encrypt their sensing data through a familiar secret key, an opposition might decrypt sensor node by cooperation merely single sensor. These methods have higher communication operating cost, less efficiency, intermediary node aggregation becomes difficult and it doesn't select efficient cluster head for each and every cluster formation, to overcome these problems proposed a pattern generation and GGP based CH routing for data aggregation.

1. Data Aggregation using pattern codes

The pattern generation (PG) algorithm is accomplished taking place every one sensor nodes to create the pattern codes to particular to the sensed data. It then evaluates the crucial values for every interval by means of the pattern starting point and creates the lookup tables. The time lookup table describe the series of every interval and the critical value in the lookup table that maps every interval to a crucial value.The description of sensor data are symbolized by constraint such as high temperature , dampness. When data is sensed starting the surroundings, its parameters are contrasted through the intervals distinct in the lookup table of PG algorithm and a equivalent crucial value is assigned to every restriction. Focusing on the crucial values of every one constraint of the data create the pattern code. The timestamp and the sensor ID are added to pattern codes while they are broadcasted to cluster-head.

The pattern evaluation algorithms at the cluster-head remove the superfluous pattern codes, which in revolve avoid redundant broadcast of data. In the PG algorithm, the pattern seed is second-hand to create pattern codes. While the clusters are primarily recognized in the network, sensor nodes obtain the secret pattern seed beginning their equivalent cluster-heads everywhere the pattern seed is a indiscriminate numeral generate and transmit through the cluster-head in encrypted arrangement. The pattern seed is second-hand designed for getting better the privacy of the pattern codes through not permitting the equivalent pattern codes fashioned every one the time. As the pattern seed is altered, different pattern code are produced by PG algorithm. A clustering move towards that is developed in the perspective of direct hop inter-CH routing. For this scheme, coverage-time for inter CH routing is originated as an optimization routing problem with the intention of capably resolved with Generalized Geometric Programming (GGP) techniques. The most select cluster sizes are attained beginning this examination. It presents together end-to-end encryption in WSN. Because CDA concern confidentiality homomorphism encryption through preservative homomorphism, cluster heads are proficient of implementing addition operations on encrypted arithmetical data. It attains privileged security levels and efficient cluster sizes are attained from this examination.

Generalized Geometric Programming (GGP) is a category of arithmetical solution distinguishes by purpose and restriction purpose that contain a particular structure. It leads to usual thought of posynomials function, and an expansion of GP described as generalized geometric programming. Thus, if $f_1(x)$ and $f_1(x)$are two functions for cluster head routing for each clustering process , a restriction such as a pattern polynomial variation are expanded. But the similar argument doesn't hold designed for a constriction such as,

$f_1(x)^{2.2} + f_2(x)^{3.1} \leq 1 \rightarrow (1)$
which involves fractional result for each cluster head along with patterns , initiate new variables t_1 and t_2, for cluster heads along with the inequality restriction for routing,
$f_1(x) \leq t_1$, $f_2(x) \leq t_2 \rightarrow (2)$

The new variables t_1 and t_2 act as upper bounds for cluster head for different patterns on $f_1(x)$and $f_2(x)$ correspondingly. GP, establish a novel variable t , and two new variation, to attain $t_1^{2.2} + t_2^{3.1} \leq 1$. The similar arguments as beyond demonstrate with the intention of this set of restriction is corresponding to the creative one of cluster head routing . As with positive result of the cluster head the thought can be useful recursively, and certainly, it can be assorted through the process for cluster head selection. As an instance, believe the difficulty

$$minimize \max\{x + z, 1 + \left(y + z\right)^{\frac{1}{2}}\} \; subjectto \max\{y, z^2 + \max\{yz, 0.3\} \leq 1, \frac{3xy}{z} = 1 \rightarrow (3)$$

Consider the result to more number of patterns with same cluster head .Suppose $x_1, \ldots x_n$ are pattern codes. The function $\max\{1 + x_1, 2x_1 + x_2^{0.2} x_3^{-3.9}\} \rightarrow (4)$

is a generalized best cluster head . The function

$$(0.1x_1 x_3^{-0.5} + x_2^{1.7} x_3^{0.7})^{1.5} \rightarrow (5)$$

If the patterns code becomes high then the above result are changed as ,

$$h(x) = (1 + \max\{x_1, x_2\})(\max\{1 + x_1 , 2x_1 + x_2^{0.2} x_3^{-3.9}\} + (0.1x_1 x_3^{-0.5} + x_2^{1.7} x_3^{0.7})^{1.5})^{1.7} \rightarrow (6)$$

x_1 and x_2 are pattern code variables and therefore cluster head selection routing function as so

$h_1(x) = (\max\{x_1, x_2\}) \rightarrow (7)$
$h_2(x) = \max\{1 + x_1, 2x_1 + x_2^{0.2} x_3^{-3.9}\} \rightarrow (8)$
$h_3(x) = 0.1x_1 x_3^{-0.5} + x_2^{1.7} x_3^{0.7})^{1.5} \rightarrow (9)$
$h(x) = (1 + h_1(x)(h_2(x) + h_3(x))^{1.7} \rightarrow (10)$

If f_0 is a generalized posynomial function for cluster head selection routing of k variables patterns , designed for which no patterns take place through a negative exemplar, and $f_1, \ldots, f_k$ then the composition function of different patterns with same code,

$$f_0\big(f_1(x), \ldots \ldots \ldots f_k(x)\big) \rightarrow (11)$$

$F(y) = logf(e^y) \rightarrow (12)$
is a convex task for every $y, \tilde{y}$ and every θ with $0 \leq \theta \leq 1$ after that include
$F(\theta y + (1 - \theta)\tilde{y}) \leq F(y) + (1 - \theta)F(\tilde{y}) \rightarrow (13)$
In the terms of the original generalized function f and variables x and $\tilde{x}$ the discrimination of the cluster heads are defined as
$f(x_1^{\theta} \tilde{x}^{1-\theta}, \ldots, x_n^{\theta} \tilde{x}^{1-\theta}{}_n) \leq f(\tilde{x}_1, \ldots, \tilde{x}_n)^{1-\theta} \rightarrow (14)$

For any θ with $0 \leq \theta \leq 1$. A generalized geometric program (GGP) is an optimization solution for cluster head routing of the form
$minimize \; f_0(x) \; subject \; to \; f_i(x) \leq 1, i = 1, \ldots, m \; g_i(x) = 1 \, , i = 1, \ldots . p \rightarrow (15)$
Where $g_1, \ldots . g_p$ are monomials and $f_0, \ldots \ldots . f_m$ are generalized posynomials .As a result, GGPs can be resolved extremely consistently and capably, just similar to GPs.
For example, the inequality of cluster heads
$x + y + z - \min\{\sqrt{xy}, (1 + xy)^{-0.3}\} \leq 0 \rightarrow (16)$
could be handled by a patterns first substitute the smallest amount through a variable t_1 and two *upper bounds*, to attain
$x + y + z - t_1 \leq 0, t_1 \leq \sqrt{xy}, t_1 \leq (1 + xy)^{-0.3}\} \rightarrow (17)$
Moving terms approximately obtain
$x + y + z \leq t_1, t_1 \leq \sqrt{xy} \, , t_1 t_2^{0.3} \, , 1 + xy \leq t_2 \rightarrow (18)$
The above results are capability to handle a wider diversity of patterns makes the representation are less jobs, and consequently easier. On the other hand, few patterns with more cluster head are elected for routing process would instantaneously elects the cluster head.

Then we apply RCDA homogenous and heterogeneous for WSN

2. RCDA scheme for homogeneous

RCDA-HOMO is composed of four procedures: Setup, Encrypt-Sign, Aggregate, and Verify. The Setup process is to organize and establish essential secrets designed for the BS and every sensor. When a sensor makes a decision to send sensing data to its CH result from GGP, it achieve Encrypt-Sign and sends the end result to the CH result from GGP. Once the CH receives all data from WSN then aggregation procedure is performed and then sends the concluding outcome to the BS. The final process is Verify.

Setup: In the setup procedure the base station creates the subsequent key pairs: (P_{SNi}, R_{SNi}): For every sensor SN_i, the base station generates (P_{SN}, R_{SN}) by KeyGen process anywhere $P_{SN_i,} = v_i$ and $R_{SN_i,} = x_i$ (P_{BS}, R_{BS}) These keys are created through KeyGen procedure where $P_{BS} = \{Y, E, p, G, n\}$ and $R_{BS} = \zeta$

Encrypt-Sign: This process is activating whereas a sensor make a decision to send its sensing data to the cluster head.

Encoding $d_i = m_i = d_i 10^{\beta}, \beta = 1(i-1)$

After encoding, SN_icomputes:

Signature: $\sigma_i = x_i \times h_i$, where $h_i = H(d_i)$

$\sigma_i = x_i \times h_i$

Ciphertext $c_i = (r_i, s_i) = (k_i \times G, M_i + K_i \times Y)$ where k_i is randomly assured beginning $\{0; \ldots n-1\}$, $M_i = map(m_i) = m_i \times G, n, G, Y \in P_{BS}$ S.

Aggregate: The CH receives every one results from its members, it make active Aggregate to aggregate what it acknowledged, and then sends the concluding results to the BS.

3. RCDA- Scheme for heterogeneous

RCDA-HOMO can be useful to heterogeneous WSN not including of alteration. Describe this approach as naïve RCDA-HETE. In this work H-sensors are considered as Heterogeneous sensor networks and L-Sensors are the local homogenous sensors. Thus, each and every H-sensor is act as cluster heads from GGP, naïve RCDA-HETE also attain the Recovery belongings. Effort to completely develop H-Sensors which contain higher computing capability. In addition, H-Sensors be able to be considered to be tamper-resistant, so might permit H-Sensors to accumulate the inequitable secret information if necessary. RCDA-HETE is separated into five procedures: Setup, Intracluster Encrypt, and Intercluster Encrypt, Aggregate, and Verify. In the Setup process, required secrets are loaded to every H-sensor is act as cluster heads and L-Sensor. Intracluster Encrypt process occupy while L-Sensors wish to transmit their sensing data to the subsequent H-Sensor. In the Intercluster Encrypt process, every H-sensor is act as cluster heads collective they received data and then encrypts sensor data and signs the aggregated end result. In adding together, if an H-Sensor receives data and signatures on or after other H-Sensors on top of its routing path, it stimulate the Aggregate process the Verify process certify the dependability and truthfulness of every aggregated result. Following table 1 RCDA-HETE obviously, a heterogeneous WSN thorough measures are explained.

TABLE I
THE REPRESENTATION OF SYMBOL FOR SENSOR NODES

Symbol	**Description**	**Symbol**	**Description**
H_i	H-sensor i	L_i^j	L-sensor i belongs to H_j
$E_k(m)$	Encrypt m with key k	d_i^j	Sensing data of L_i^j
δ_j	Selected data by H_j	m_j	Encoded result of δ_j
K_i^j	Pairwise key shared by L sensor i with H-Sensor j		

IV. EXPERIMENTAL RESULTS

In this work to implement this procedure using Linux open source language. It's fundamental in a heterogeneous WSN, popular of sensors such as H and L (High, Low) sensors. In our proposed, computation cost of L-Sensors is controlled by H-Sensors, consequently L-Sensors can be extremely inexpensive and easy. In fact, the generally hardware cost is cheap. Naive RCDA-HETE, MICAz nodes act as L-Sensors which collect data and execute Encrypt-Sign the similar technique as RCDA-HOMO. Therefore, the processing delay generation is equal to RCDA-HOMO. For data aggregation delay, the ZB32 nodes are selected as cluster head for H sensors, which are additional authoritative. So the delay of the WSN is reduced to 3.371 ms, and compared with RCDA-HOMO, aggregation performance is roughly 21.9 times quicker than in RCDA-HOMO. RCDA-HETE has been modifying from naive RCDA-HETE to improve the result of L-Sensors. The processing delay of the L-sensor nodes are decreases 2.97 ms, because *Intra-encrypt* leverages symmetric cryptography. In this method where every H-Sensor aggregates the received data and receives signatures beginning former H-Sensors on its routing pathway. To run every node in the network using the network simulation tool, it can start the process with command 'nam <nam-file>' is the name of a nam trace file that was created by ns which you desire to imagine. Below Fig. 1 you can notice a screenshot of a NAM window.

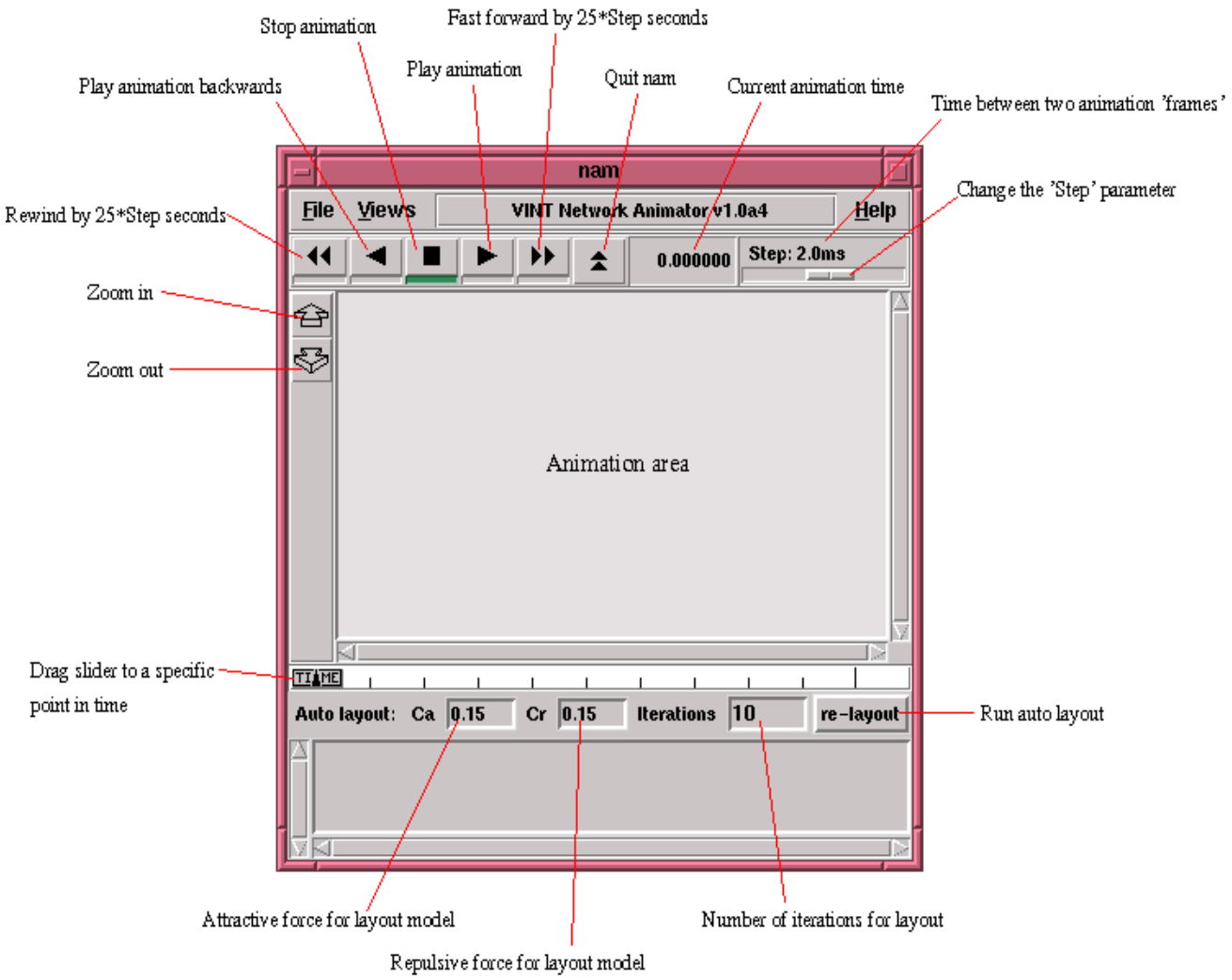

Fig 1 : Network Animating Window

The following figures show the result of nodes formation, RCDA HOMO, Naïve RCDA-HETE before and after cluster head routing result.

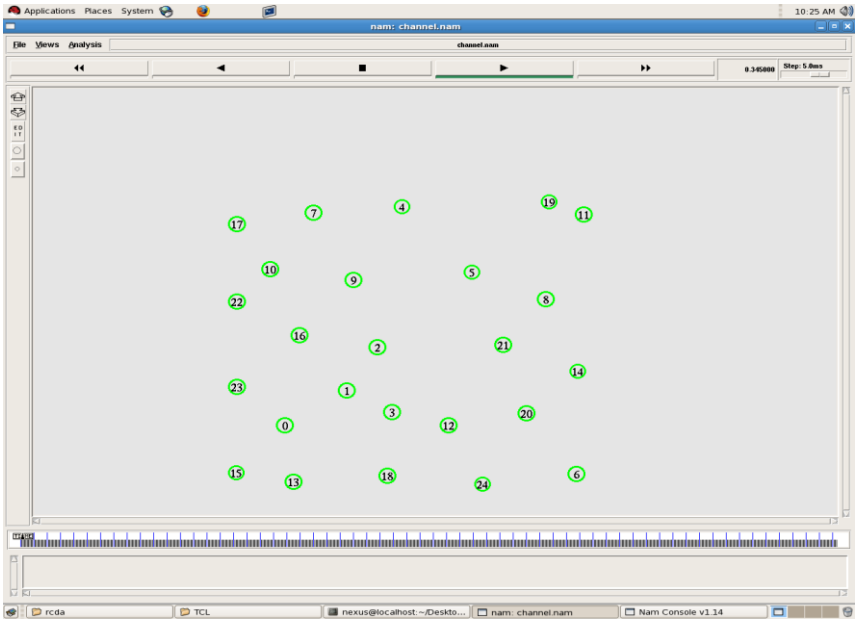

Fig 2: Number of nodes in WSN

The Fig 2 shows the result of number of nodes used for data aggregation process in WSN.

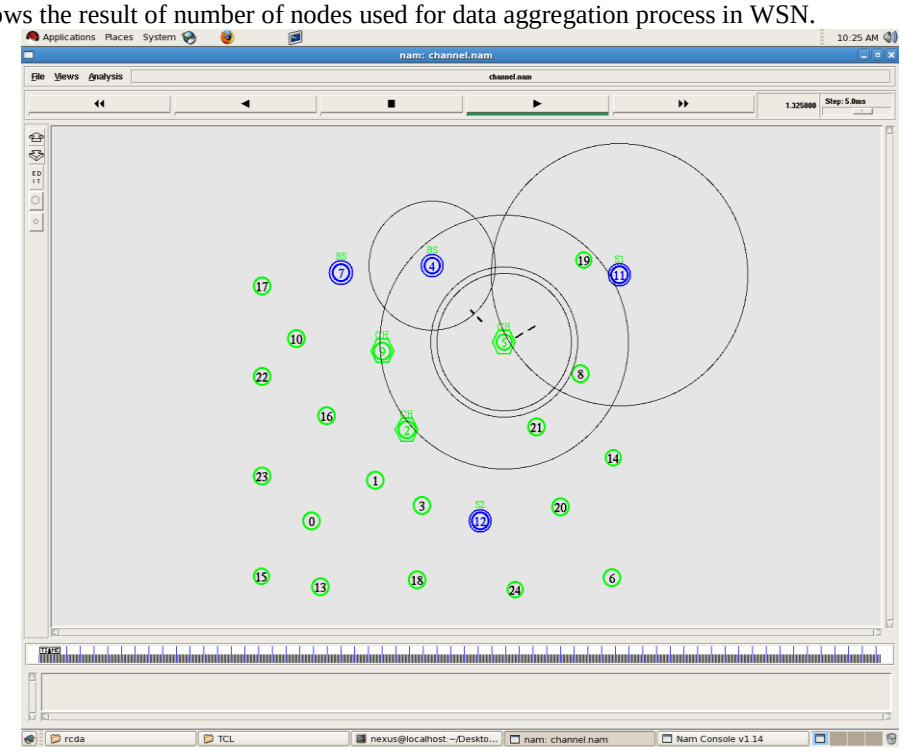

Fig 3: RCDA-HOMO in WSN

In the Fig 3 shows the RCDA data aggregation procedure for inside the cluster where node 11 aggregates the nodes information to 19 only.

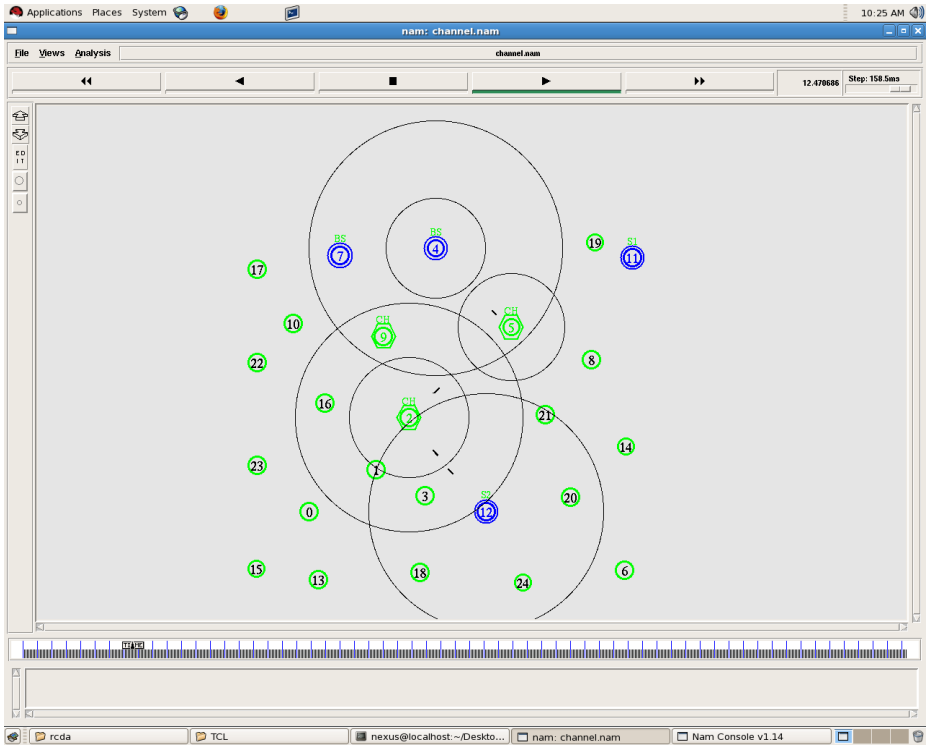

Fig 4: Naïve RCDA-HETE in WSN

In the Fig 4 shows the Naïve RCDA-HETE data aggregation procedure for inside and outside the cluster where node 9,4 aggregates the nodes information to several nodes.

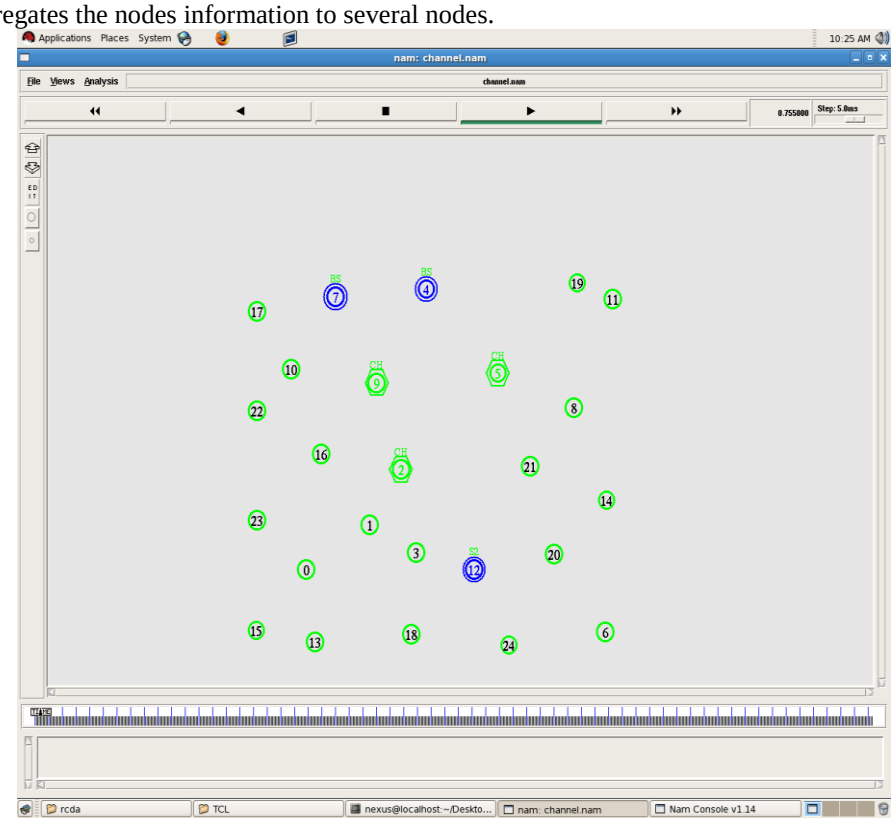

Fig 5: GGP Cluster Head in WSN

In the Fig 5 shows the result of better cluster head selection based on GGP for routing .

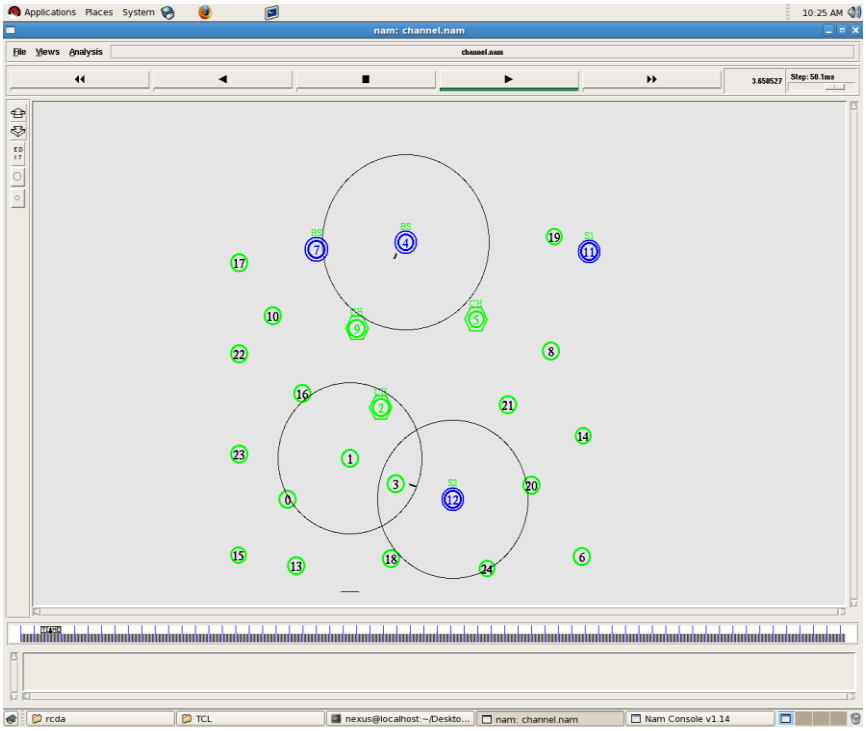

Fig 6: RCDA-HOMO after GGP in WSN

In the Fig 6 shows the result of RCDA data aggregation procedure for inside the cluster after the best cluster head was selected where node 12 aggregates the nodes information to 20,24 only.

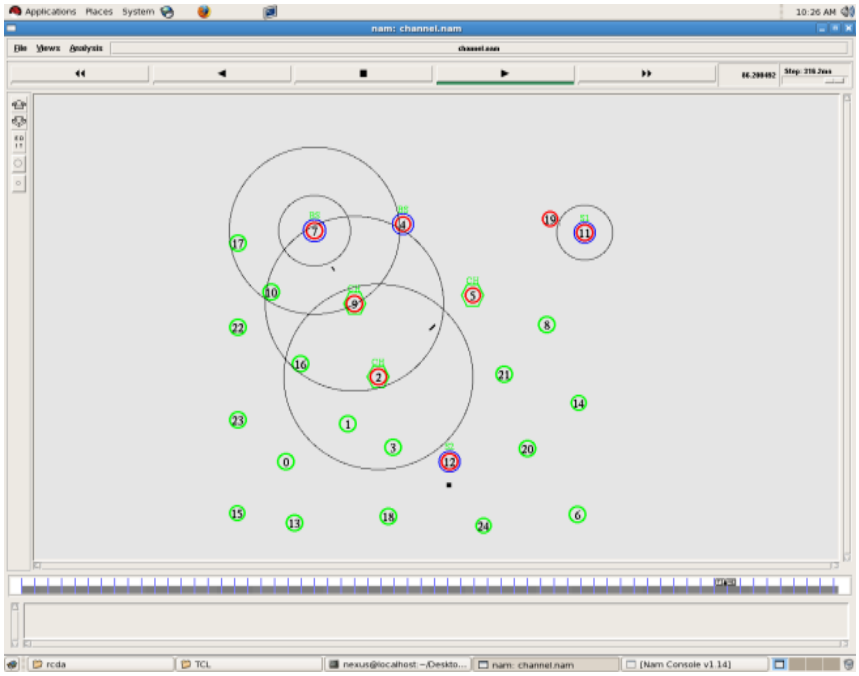

Fig 7: Naïve RCDA-HOMO after GGP in WSN

In the Fig 7 shows the Naïve RCDA-HETE data aggregation procedure result for inside and outside the cluster after CH routing selected where node 9, aggregates 4,16,19,17 and to many nodes .

V. CONCLUSIONS AND FUTURE ENHANCEMENT

In this paper solves the problem of coverage time cluster head routing schema for data aggregation and consumes less power to balance the different cluster head are elected in a clustered WSN is considered. GGP methods are well efficient methods to solve the problem of cluster head routing in WSN models were investigated. The proposed recoverable concealed data aggregation schemes with GGP methods to select best cluster head and optimal routing schema for each homogenous and heterogeneous wireless sensor network routing. A particular characteristic is that the base station can steadily make progress every one sensing data somewhat than aggregated results, but the communication overhead is still suitable. Furthermore, incorporate the aggregate signature system to guarantee data dependability and reliability in the design. It demonstrates the consequence of concurrently accounting for the collision of intra and intercluster traffic in the propose of clustering strategies. Taking into consideration a large WSN also performed simulations on the projected schemes.

Because sensor nodes may produce important redundant information, in several applications comparable packets from numerous nodes can be summative consequently that the numeral of transmissions would be reduced. Data aggregation is the groupings of data from diverse sources by with functions such as removing duplicates, min, max and average. In future work we need add these functions in either partially or fully in each sensor node, by permitting sensor nodes to accomplish in-network data diminution.

REFERENCES

[1] B. L. Sun, C. Gui, and Y. Song, "Energy Entropy On- Demand Multipath Routing Protocol for Mobile Ad Hoc Networks", *China Communications*, Vol. 8, No. 7, 2011, pp. 75–83.

[2] B. L. Sun, S. C. Pi, C. Gui, et al., "Multiple Constraints QoS Multicast Routing Optimization Algorithm in MANET based on GA", *Progress in Natural Science*, Vol. 18, No. 3, 2008, pp. 331–336.

[3] B. L. Sun, X. C. Lu, C. Gui, et al., "Network Coding-Based On-Demand Multipath Routing in MANET", *Proceedings of 26th IEEE International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW)*, Shanghai, China, May 21-25, 2012, pp. 1520–1524.

[4] Intanagonwiwat, C.; Govindan, R.; Estrin, D,"Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks", *In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00),* Boston, MA, USA, 6–11 August 2000; pp. 56–67.

[5] Sohrabi, K.; Gao, J.; Ailawadhi, V.; Pottie, G.J,"Protocols for Self-Organization of A Wireless Sensor Network", *IEEE Person. Commun*. 2000, 7, 16–27.

[6] R. Rajagopalan and P. Varshney, "Data-Aggregation Techniques in Sensor Networks: A Survey," *IEEE Comm. Surveys Tutorials*, vol. 8, no. 4, pp. 48-63, Oct.-Nov. 2006.

[7] S. Madden, M.J. Franklin, J.M. Hellerstein, and W. Hong, "TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks," *Proc. Fifth Symp. Operating Systems Design and Implementation*, 2002.

[8] J.-Y. Chen, G. Pandurangan, and D. Xu, "Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Randomized Algorithms and Analysis," *IEEE Trans. Parallel Distributed Systems*, vol. 17, no. 9, pp. 987-1000, Sept. 2006.

[9] D. Westhoff, J. Girao, and M. Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation," *IEEE Trans. Mobile Computing*, vol. 5, no. 10, pp. 1417-1431, Oct. 2006.

[10] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," *Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems*, pp. 109-117, July 2005.

[11] E. Mykletun, J. Girao, and D. Westhoff, "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Comm*., vol. 5, pp. 2288-2295, June 2006.

[12] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications*, pp. 113-127, May 2003.

[13] B. Yu and B. Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," *Proc. IEEE 20th Int'l Symp. Parallel and Distributed Processing (IPDPS' 06),* Apr. 2006.

[14] T.H. Hai and E.-N. Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-Hops Neighbor Knowledge," *Proc. IEEE Seventh Int'l Symp. Network Computing and Applications,* pp. 325-331, July 2008.

