[Kambale, 3(6): June 2016]

ISSN 2348 – 8034
Impact Factor-4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ATTACK PREVENTION OF SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORK BY NODE RECOVERY

Minal D. Kamble[*1] and Asst.Prof. Nutan M. Dhande[2]

[*1,2]Computer Science & Engineering, RTMNU University, A.C.E, Wardha, Maharashtra, India

ABSTRACT

The remote sensor structure is encompassed by gathering of extensive no. of sensor hubs. The sensor focus focuses have the farthest point of recognizing the weight, vibration, advancement, moistness, and sound as in and so on. In perspective of a need for liberality of checking, remote sensor structures (WSN) are frequently plenitude. Information from various sensors is totaled at an aggregator focus indicate which then advances the base station just the total qualities. Existing structure basically concentrate on affirmation of Attack in the system. This paper ranges examination of Attack Prevention by Node Recovery other than gives a thought to how to defeat the issue. Also, distinguishing the assaults by utilizing IP and MAC Based Data Injection Techniques. Besides, the SSSD dijkstra estimation for finding the briefest route from source center point to destination center point. Besides, by utilizing AES Algorithm , give more security in the framework.

Keywords: *Data collecting, Tree Approach & In Network Aggregation Approach of Data Aggregation, in-framework all out , sensor framework security, dynamic scattering , ambush adaptable.*

1. INTRODUCTION

The remote sensor framework is formed by broad number of sensor centers. Sensor centers might be homogeneous or heterogeneous. These sensor focuses includes four focal units: perceiving unit, dealing with unit, transmission unit, and force unit. For listening occasion, sensor focus focuses ere changed. Precisely when an occasion happens, by conveying remote development sensors illuminate the end point or destination node.[1] The assault strong calculation comprises of two stages. The primary thought is as per the following: (i) In the main stage, the BS infers a preparatory appraisal of the total in view of insignificant confirmation data got from the hubs. (ii) In the second stage, the BS requests more verification data from just a subset of hubs while this subset is dictated by the evaluation of the main stage.

1.1 Wireless Sensor Network

Remote Sensor Network is a social occasion of specific transducers with a correspondences base for watching and recording conditions at different territories. (Sweeping no. of sensors center). Remote sensor systems will comprise of extensive quantities of little, battery-controlled, remote sensors. Remote sensor systems are a significant headway for liberal scale checking, giving sensor estimations at high normal and spatial determination. [2] Wireless Sensor Network (WSN) is the structure which is widely utilized as a bit of benefice applications for watching and highlight perception

1.2 Data Aggregation

Information Aggregation is a fundamental methodology to achieve power profitability in the sensor framework. The assembled data must be taken care of by sensor to decline transmission. It utilized the Tree Based Approach. For accumulating the estimations of hub. What's more, produce the crossing Tree in the diagram.

1.3 Tasks in Wireless Sensor Network

- Attack Detection
- Attack Prevention
- Shortest Path Calculation

1.3.1 Attack Detection

In that detecting the two attacks based on IP Address and MAC Address. By using IP & MAC Based data Injection Technique.

1.3.2 Attack Prevention

It is fundamental part of framework, Prevent this assault from assailant. By utilizing Node Recovery taking into account Predefined Graph. furthermore utilized the SSSD dijkstra calculation for finding the other briefest way on predefined Graph.[2] It is basically focus on Attack Prevention, prevent the attacks through Node Recovery and provide more security to the system.

1.3.3 Shortest Path Calculation

After preventing attacks, then generate the alternate shortest path between source node to destination node by using SSSD Dijkstra Algorithm.

2. RELATED WORK

Sankardas Roy, Proposed [1] The once-over dispersing technique secure against the trap dispatched by managed focus focuses. Our strike strong check enrolls the genuine total by sifting through the obligations of traded off focuses in the collection chain of centrality. Essentially portray the affirmation of assault in the system. This paper areas examination of Attack Prevention moreover gives an idea to how to vanquish the issues [2] this paper ranges examination of Attack Prevention other than gives a thought to how to defeat the issues. Besides, the dijkstra count for finding the briefest route from source center point to sink center point. besides, give more security in the system.[3] Jyoti Rajput , Proposed [4] A test to information total is the strategies by which to secure assembled information from revealing amidst accumulating strategy and likewise get exact amassed results. Outlined particular conventions for securing totaled information in remote sensor systems. Nandini. S. Patil, Proposed[5] information blend which beguiling framework for information gathering in scattered structure models and part access by strategy for remote framework.

3. PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner

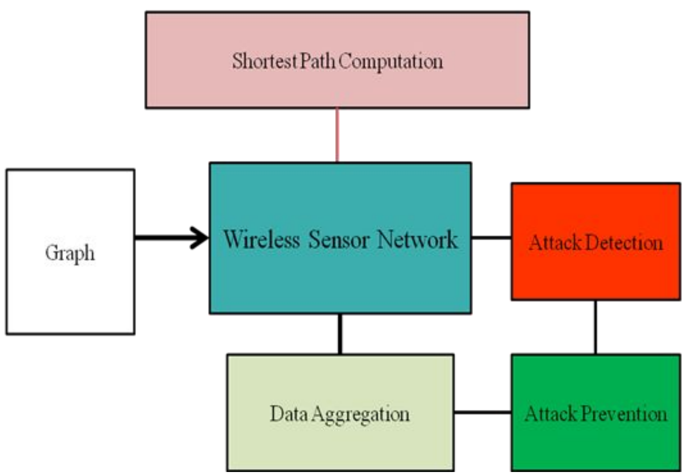

Fig 3.1: Basic System Architecture

Fig 3.1 shows the key system development displaying of proposed structure, Firstly, all the work perform on reenactment mode. It will be used the predefined graph. Bundle will be send from source center point to sink center.[2][3] To check the most constrained shower from course center point to destination center. In perspective of weight of that route beginning with one center point then onto the following center point.

3.1 METHODOLOGY

3.1.1. SSSD Dijkstra Algorithm

Step1: dist[s] $\leftarrow 0$

for all v € V – { s }

Step2: do dist[v] $\leftarrow \infty$

Step3: S $\leftarrow \varnothing$

Step4: Q $\leftarrow$V

Step5: while Q $\neq \varnothing$

Step6: do u $\leftarrow$ mindistance(Q, dist)

Step7: S$\leftarrow$ S ∪ { u }

for all v ∈ neighbors [u]

Step8: do if dist[v] > dist[u] + w(u, v)

Step9: then d[v] $\leftarrow$d[u] + w(u, v)

Step10: return dist

3.1.2. IP & MAC Based Data Injection Attack Technique

1. While Finding shortest Path the current node request for the next nodes. Then IP Address & MAC Address and its calculate the original path of the next node.

2. If the IP Address & MAC Address does not match in the routing table a false IP & MAC is detected.

MAC Address / IP Address (Node 0 To Node n) =! MAC Address / IP Address (Routing Table of Attacked Node)

3. By using Node Recovery, Recover the node then select the next node according to the path from source node S to destination node Z using SSSD algorithm.

3.1.3 Security Methodology : AES & SHA-1

In that system, provide the more security by AES and SHA-1 algorithm. AES is 256 bits for encryption and decryption. And SHA-1 used for generating the key for security.

4. SIMULATION RESULTS

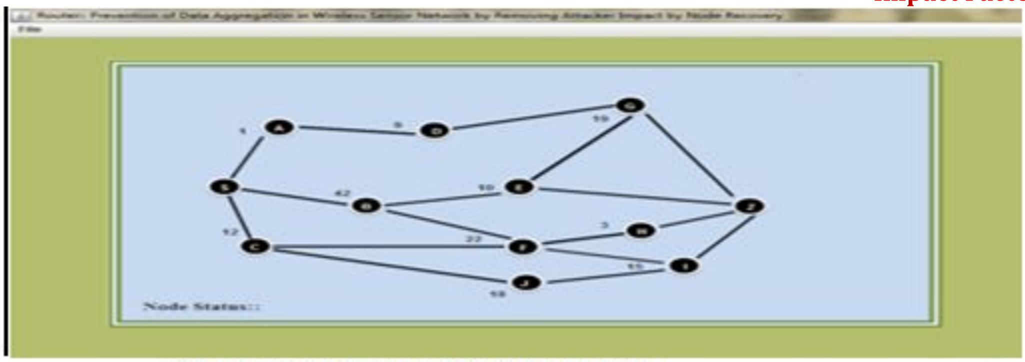

Fig 5.1: Router Form as Graph with 12 nodes

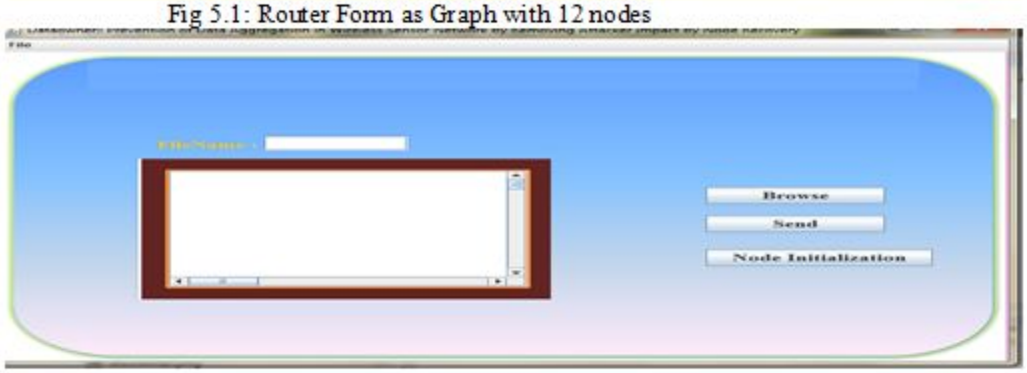

Fig 5.2 : Source Form

Fig 5.3 : Receiver Form

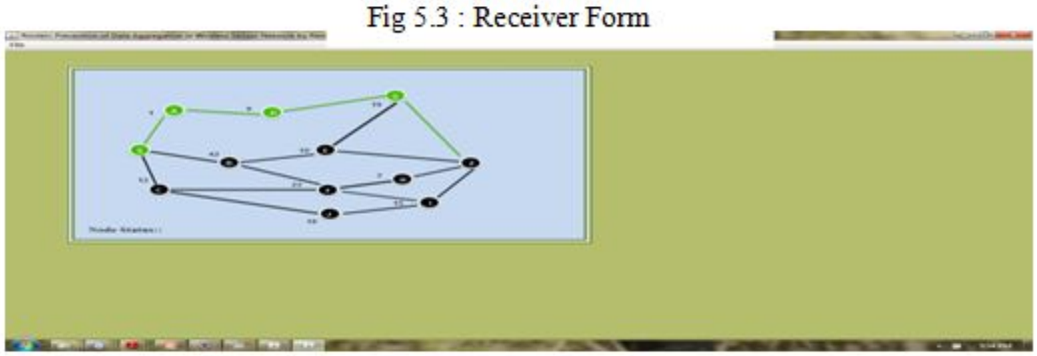

Fig 5.4 : Without Attack

ISSN 2348 – 8034
Impact Factor-4.022

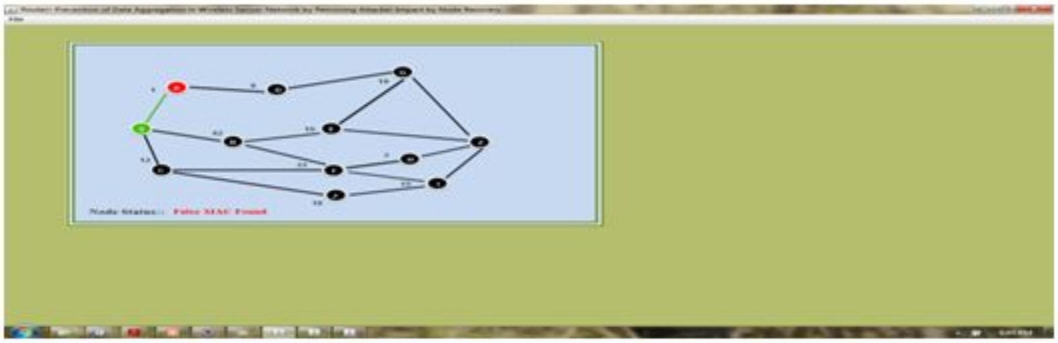

Fig 5.5 : MAC Based Data Injecton Attack

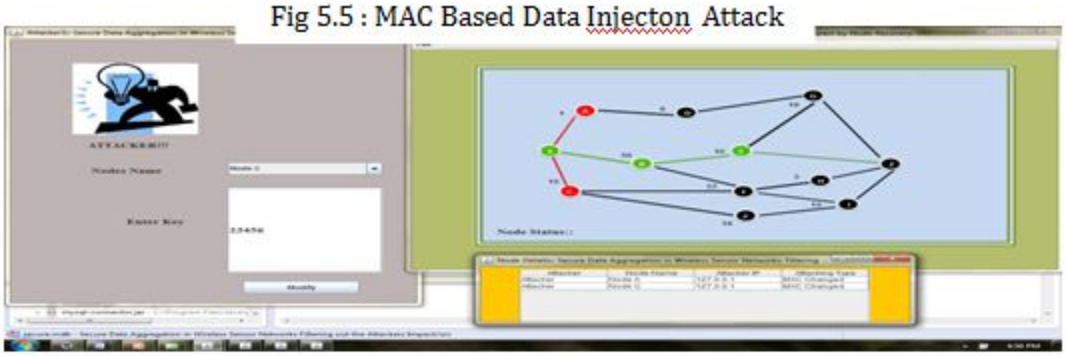

Fig 5.6 : Recover the node in MAC Based Attack Condition

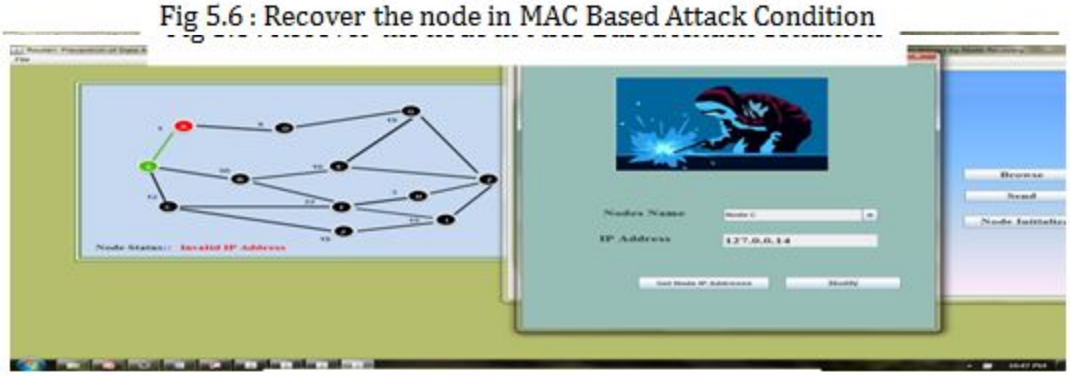

Fig 5.7 : IP Based Data Injection Attack

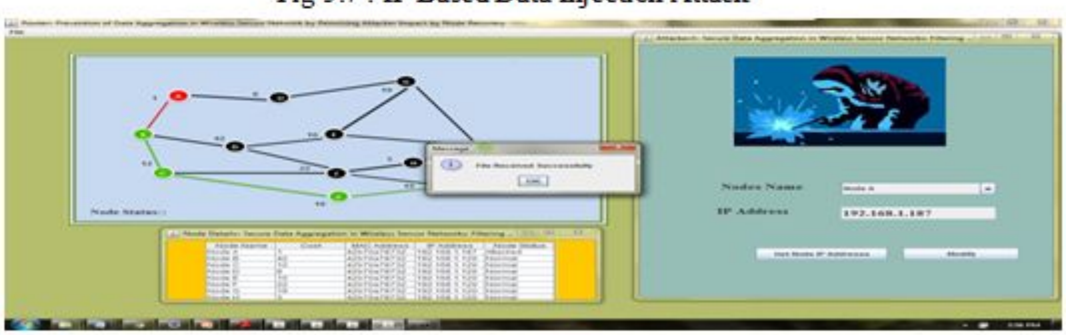

Fig 5.8 : Recover the node in IP Based Condition

ISSN 2348 – 8034
Impact Factor-4.022

The recreation considers include the deterministic arbitrary topology with 12 hubs as appeared in fig 5.1. The proposed framework actualized in the JAVA. As indicated by the proposed framework, The framework keep running on nearby host that why every one of the hubs of locations are same. That is standalone framework. we transmit the bundles from Source Node A to Destination Node Z. At that point distinguishing the Falsified sub Aggregate assault or false Data Injection Attacks taking into account IP and MAC Address. Fundamental Focus of proposed framework is the Attack counteractive action through Node Recovery. In the wake of keeping assaults parcels sends from source hub to destination hub with discovering better most limited way.

The Fig 5.1 demonstrated that reenactment of hubs. Furthermore, play out the hub initiation that is all the cost relegate to hubs. Fig 5.2 and 5.3 demonstrated that Source and Receiver Form. In source structure, scan the record for sends. Recipient Form, demonstrates that Received the documents at the destination hub Z. what's more, spare it in Database. The Fig 5.4 demonstrates that every one of the hubs are assaulted free. at that point sending the selecting record from Source Node S to Destination hub Z inside 32 ms. "Green" shading characterized that are hubs are assaulted free. The Fig 5.5 and 5.6 demonstrates that Node An and Node C are assaulted by the MAC based Attacker. That is MAC Address of that assaulted hub is changed. Utilizing MAC Based Data Injection Technique.Then "Red" shading demonstrates the hub is assaulted by the assailant. Fig 5.6 demonstrates that recuperate the following hub and the create the Better most limited way from Source Node to Destination Node. The Fig 5.7 and 5.8 demonstrates that Node An is assaulted by the IP based aggressor. Shows the assaulted hub. By utilizing IP Based Data Injection Technique. Furthermore, recoup the following hub and figure the most limited way from source hub to destination hub.

5. RESULT & DISCUSSION

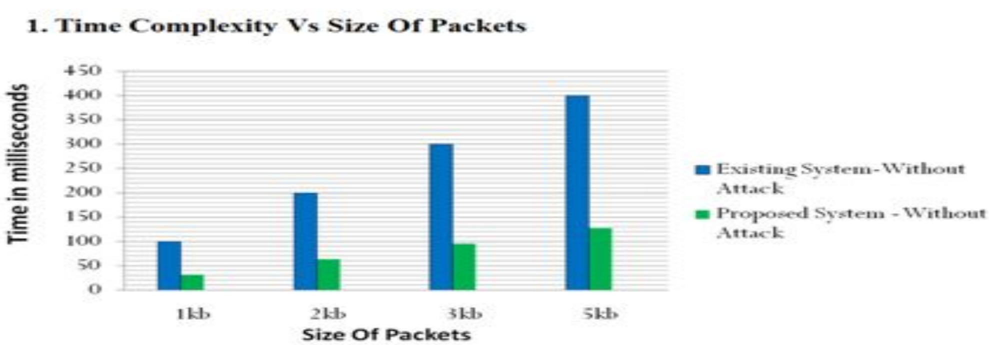

Fig 6.1 : size of packets with respect to Time

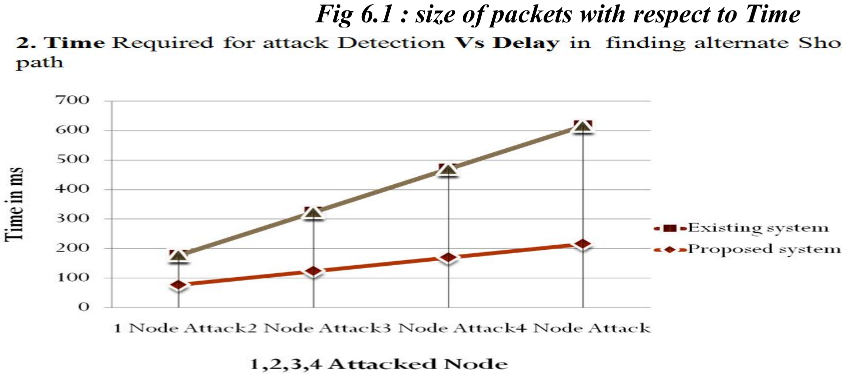

Fig 6.2 : Condition of Attacked Node as 1, 2, 3, 4

(C) Global Journal Of Engineering Science And Researches

3 . Encryption Time & Decryption Time among AES, DES and RSA Vs Size Of Packets

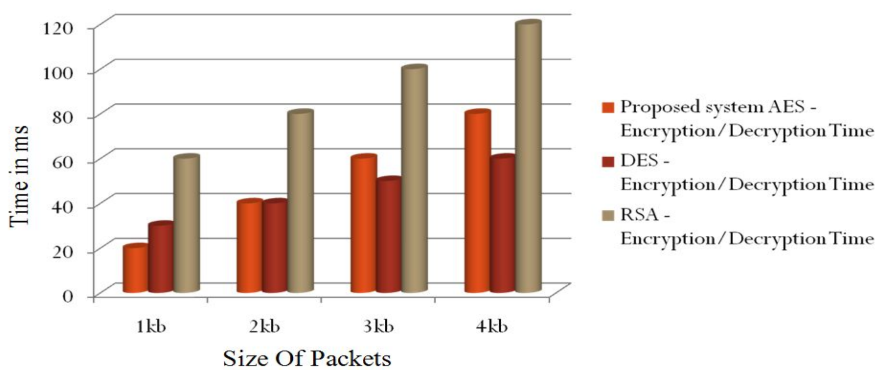

Fig 6.3 : Comparison of Proposed System AES algorithm & Prevoius Algorithm

The results are studied parameters TIME COMPLEXITY, DELAY, SECURITY of Existing System and Proposed System. The fig 6.1 shows a comparison for Time Complexity calculated for Size of packet. Proposed system required less time for sending the packet in without attacks condition. Depending upon size packets its required the time for sending packets from source node to destination node. The fig 6.2 shows time requirements for attack detection and delay in finding alternate path in the condition of no. of attacked nodes in the network. Depending upon the size of packets its required time in suppose attack detected that time delay is occurred. The fig 6.3 shows a comparison for Encryption & Decryption Time calculated among the AES with Different Algorithm. As compared to MAC Protocol and DES, RSA . More secured algorithm AES used as 256 bits , so that as this algorithm is more secure as compared to previous algorithm.

6. CONCLUSION & FUTURE SCOPE

This paper gives a proposed work of secure information blend thought in remote sensor structures. To give the inspiration driving secure information total, regardless, the security necessities of remote sensor structures are shown and the threat model and seriously orchestrated model are uncovered to adequately handle security prerequisites of WSN. The outcomes are contemplated as for Time, Size of Packets, Throughput in without assault and with assault , encryption time and decoding time of AES and MAC Protocol by Attack Detection while existing framework , Node Recovery component proposed work is worked. Given the Falsified sub Aggregate Attack identification by utilizing IP and MAC Based False Data Injection Attack procedure. Given more security at the season of send the document from Source hub to destination hub by AES calculation. Given proficient most limited way computation by SSSD Algorithm. Given Attack aversion through Node Recovery.

7. FUTURE SCOPE

- To give vitality productivity while discovery of assaults.
- Use for numerous most brief way calculations for quick preparing.
- Providing more techniques to assaults.
- Fast parcel recuperation instrument

REFERENCES

[1] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014

[2] Minal D. Kamble & Prof. D. S. Dabhade, " A Survey Paper on Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery", International Journal of Research (IJR) e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015

ISSN 2348 – 8034
Impact Factor-4.022

[3] Minal D. kamble and Prof. N. M. Dhande , " Prevention Of Data Aggregation in Wireless Sensor Network By Removing Attacker Impact by Node Recovery" IJRITCC ISSN: 2321-8169 Volume: 4 Issue : 1 14 – 19 January 2016
[4] Jyoti Rajput and Naveen Garg , "A Survey on Secure Data Aggregation in Wireless Sensor Network",International Journal of Advanced Research in Computer Science and SoftwareEngineering,Volume4 Issue5,May2014
[5] Nandini. S. Patil, Prof. P. R. Patil, "Data Aggregation in Wireless Sensor Network", IEEE International Conference on Computational Intelligence and Computing Research, 2010
[6] Peter Corke, Tim Wark, Raja Jurdak, Wen Hu, Philip Valencia, and Darren Moore "Environmental Wireless Sensor Networks", Proc. IEEE | Vol. 98, No. 11,pp.1903-1917November2010
[7] Rabindra Bista and Jae-Woo Chang, "Privacy-Preserving Data Aggregation Protocols for Wireless Sensor Networks:A Survey",Department of Computer Engineering, Chonbuk National University,Chonju,Korea,sensors,2010
[8] Haifeng Yu, "Secure and Highly-Available Aggregation Queries in Large-Scale Sensor Networks Via Set Sampling", in Proc. Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 1–12
[9] Rakesh Kumar Ranjan1, S. P. Karmore, "BIST Based Secure Data Aggregation in Wireless Sensor Network" International Journal of Science and Research (IJSR), Volume 4Issue4,April2015
[10] Sankardas Roy, Sanjeev Setia, Sushil Jajodia, "Attack Resilient Hierarchical Data Aggregation in Sensor Networks", in Proc. ACM Workshop Security Sensor Adhoc Netw. (SASN), 2006, pp. 71–82.
[11] Snehal Lonare, Dr. A. S. Hiwale, "A Data Aggregation Protocol to Improve EnergyEfficiencyinWirelessSensorNetworks",ConferenciPGCON-2015
[12]Kiran Maraiya, Kamal Kant, Nitin Gupta, "Wireless Sensor Network: A Review on Data Aggregation", International Journal of Scientific & Engineering Research Volume 2, Issue 4, April -2011
[13]Thejaswi V, Harish H.K, "Secure Data Aggregation Techniques in Wireless Sensor Network", International Journal of Innovative Research in Computer and Communication Engineering An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 5, May 2015
[14] Haowen Chan, Adrian Perrig, Dawn Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks" , ACM Trancastion , 2006
[15] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring sensor networks," in Proc. 2nd Int. Workshop Sensor Netw. Protocols Appl. 2010
[16] Afrand Agah and Sajal K.Das, "Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach", International Journal of Network Security, Vol.5, No.2, PP.145–153, Sept. 2007
[17] Arijit Ukil, "Privacy Preserving Data Aggregation in Wireless Sensor Networks", IEEE ICWCMC, Valencia, Spain , 2012
[18] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. 1st Int. Conf. Embedded Netw. Sensor Syst. (SenSys), 2010
[19] L. Buttyan, P. Schaffer, and I. Vajda, "Resilient aggregation with attack detection in sensor networks," in Proc. 2nd IEEE Workshop Sensor Netw. Syst. Pervasive Comput., Mar. 2011
[20] J. Considine, F. Li, G. Kollios, and J. Byers, "Approximate aggregation techniques for sensor databases,"inProc.IEEE20thInt.Conf.DataEng.(ICDE)2010