ISSN: 2454-4248
31 - 34

Prevention of Data Aggregation in Wireless Sensor Network By Removing Falsified Sub Aggregate Attack By Node Recovery

Minal D. Kamble[1] , Prof. N. M. Dhande[2]
[1]Computer Science & Engineering, RTMNU University, A.C.E, Wardha, Maharashtra, India
[1]*kambleminal25@gmail.com*
[2]Computer Science & Engineering, RTMNU University, A.C.E, Wardha, Maharashtra, India
[2]*nutandhande@gmail.com*

Abstract: The remote sensor framework is encircled by group of large no. of sensor nodes. The sensor center points have the limit of distinguishing the weight, vibration, development, dampness, and sound as in etc. In view of a necessity for generosity of checking, remote sensor frameworks (WSN) are regularly abundance. Data from different sensors is totaled at an aggregator center point which then advances to the base station only the aggregate qualities. Existing structure simply focus on acknowledgment of Attack in the framework. This paper areas examination of Attack Prevention besides gives an idea to how to overcome the issues. What's more, utilize the SSSD dijkstra calculation for finding the briefest way from source hub to destination hub. Furthermore, give more security in the system.

Keywords*: Data collecting, different leveled aggregation, in-framework all out, sensor framework security, dynamic scattering, ambush adaptable.*

*****

1. INTRODUCTION

The remote sensor framework is molded by broad number of sensor center points. Sensor center points might be homogeneous or heterogeneous. These frameworks are incredibly passed on and contain various number of less cost, less power, less memory and self-sorting out sensor hubs. These sensor focuses includes four focal units: perceiving unit, dealing with unit, transmission unit, and force unit. For listening occasion, sensor focus focuses ere modified. Precisely when an occasion happens, by conveying remote development sensors illuminate the end point or destination node.[1] The assault flexible calculation comprises of two stages. The principle thought is as per the following: (i) In the primary stage, the BS infers a preparatory appraisal of the total in light of insignificant validation data got from the hubs. (ii) In the second stage, the BS requests more confirmation data from just a subset of hubs while this subset is dictated by the evaluation of the primary 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 ranges.(extensive no. of sensors center point). Remote sensor systems are a pivotal progression for liberal scale checking, giving sensor estimations at high regular and spatial determination. The smallest complex application is test and send where estimations are traded to a base station, yet WSNs can in like way perform in-system dealing with operations, for example, accumulation, occasion unmistakable confirmation, or actuation.[2] Wireless Sensor Network (WSN) is the structure which is widely utilized as a bit of bonafide applications for watching and highlight perception

1.2 Data Aggregation

Information Aggregation is a key methodology to finish power profitability in the sensor framework. The data aggregate is that takes out dreary data transmission and updates the lifetime of essentialness in remote sensor framework. Data aggregation is the technique of one or a couple of sensors then accumulate the revelation result from other sensor. The assembled data must be taken care of by sensor to diminishing transmission.

1.2 Tasks in Wireless Sensor Network

- Attack Detection
- Attack Prevention

Attack Detection

In that errand, In the Network, allocated the locations of the considerable number of hubs. Keep running on neighborhood host. That is every one of the locations of the hubs are same in system. Assume assaults is discovered i.e MAC ID is change of one of the hub , misrepresented hub is found.[1] at that point create the substitute way from source hub to sink hub by utilizing all source most limited way calculation. Two types of attack to be detected Detect the False Data Injection Attack in the Graph.

Attack Prevention

It is fundamental part of framework, Prevent this assault from assailant. By utilizing Node Recovery taking into account Predefined Graph. Further more utilized the SSSD dijkstra calculation for finding the other briefest way on predefined Graph.[2]

This endeavor deal with the ambushes issue from the aggressors. It is basically focus on Attack Prevention in Wireless Sensor Network. It is use the Predefined Graph. It is used for the count for finding the most concise path from source center to destination center point. Besides, the strikes. The proposed structure [3] can recognize attacker ambush moreover see the center point that is affected by the assailant. The proposed structure can in like manner right the attack center point. If a center point is seen to be harmful a choice way is taken to source to destination center point.

2. RELATED WORK

Sankardas Roy , Proposed [1] The rundown scattering procedure secure against the ambush dispatched by dealt center points. Our strike solid count enlists the real aggregate by filtering through the duties of exchanged off centers in the accumulation chain of significance. Simply delineate the acknowledgment of attack in the framework. This paper locations investigation of Attack Prevention furthermore gives a thought to how to conquer the issues [2] This paper areas examination of Attack Prevention besides gives an idea to how to overcome the issues. What's more, utilize the dijkstra calculation for finding the briefest way from source hub to sink hub. furthermore, give more security in the system.[3] Jyoti Rajput , Proposed [4] A test to data aggregate is the methods by which to secure gathered data from uncovering in the midst of hoarding technique and what's more get precise amassed results. delineated distinctive traditions for securing totaled data in remote sensor frameworks. Nandini. S. Patil, Proposed [5] data mixture which charming system for data gathering in dispersed structure architectures and component access by method for remote system. Die down Corke, Proposed [6] to speak to the inventive inconveniences and challenges that are included in meeting end-customer necessities for information gathering systems. Trustworthiness and gainfulness are key concerns and effect the setup choices for structure gear and programming.

3. PROPOSED SYSTEM

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

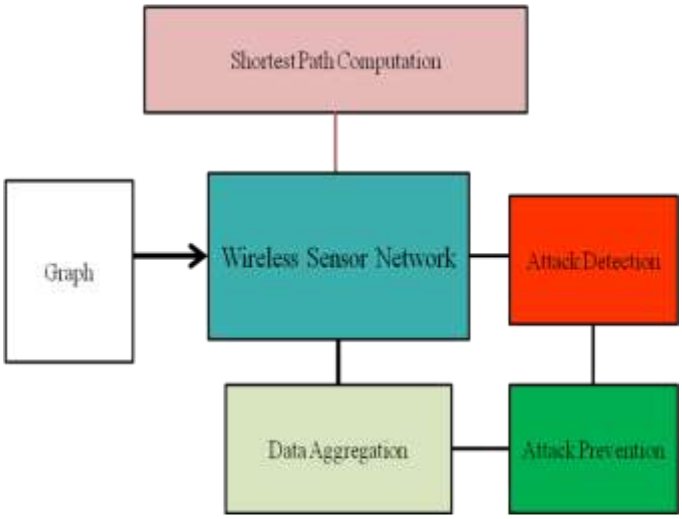

Fig 3.1: Basic System Architecture

The remote sensor framework is surrounded by immense number of sensor center points. Sensor centers might be homogeneous or heterogeneous. It involves minimal light weighted remote center points called sensor centers. The purpose of data aggregate is that wipes out abundance data transmission and enhances the lifetime of imperativeness in WSN. On a very basic level focus on ambush balancing activity in remote sensor framework.

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. 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. Twisted center is found then create the substitute route between from source center to sink center point by using specific count. To keep up the security in remote sensor framework. It used to following algorithm:

SSSD Dijkstra Algorithm

1. Input Graph
2. Assign the Weights to all the nodes
3. Define the Source Node and destination Node in the graph.
4. Calculate the shortest path between source node to destination node.

Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems - data aggregation and data trustworthiness assessment - using a single iterative procedure.

4. METHODOLOGY

1. Simulating Nodes in Wireless Sensor Network

Computer simulation is the discipline of designing a model of actual or theoretical physical system, executing the model on digital computer and analyzing the execution output.

2. Canvas Design

In module 2 , Graph will be completely design using Canvas. Assigning the MAC addresses will be done to the sensor nodes in the graph. and generate the table for storing the MAC addresses of the each nodes in the graph.

3. Attack Detection

In the Network, assigned the addresses of all the nodes. Run on local host. That is all the addresses of the nodes are same in network. Suppose attacks is found i.e MAC ID is change of one of the node , falsified node is found. then generate the alternate path from source node to sink node by using all source shortest path algorithm. It also used to kalman filtering algorithm. For detecting the attack.

4. Attack Prevention

Prevent this attack from attacker. By using Node Recovery based on Predefined Graph. Recover the falsified node on predefined graph. For avoid the detection and provide the prevention. To Recover the falsified node. And find the alternate path from source node to destination node by using SSSD Dijkstra algorithm. Successfully send the text File from source node to destination node.

5. DESIGN WORK

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

Firstly, Implemented the four algorithm for computing shortest path in network. Then I choose the SSSD dijsktra algorithm for computing shortest path because of it required less time for computing shortest path . it is best algorithm.

Secondly, Designed the Complete graph using canvas. Fig 5.1 shows that, It consists of 12 nodes in the graph. It designed the source form and receiver form. Graph shows the as router form. Graphically shows the simulation. Main aspect is the prevention of falsified sub aggregate attack or False Data Injection Attack in the graph.

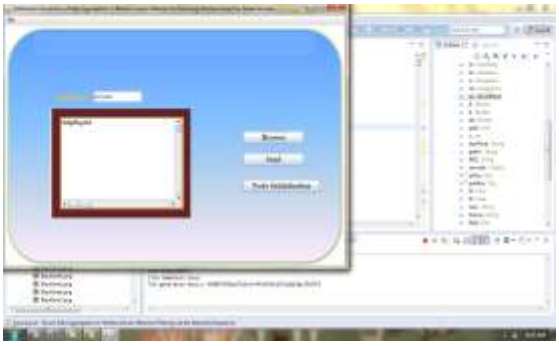

Fig 5.1: Source Form

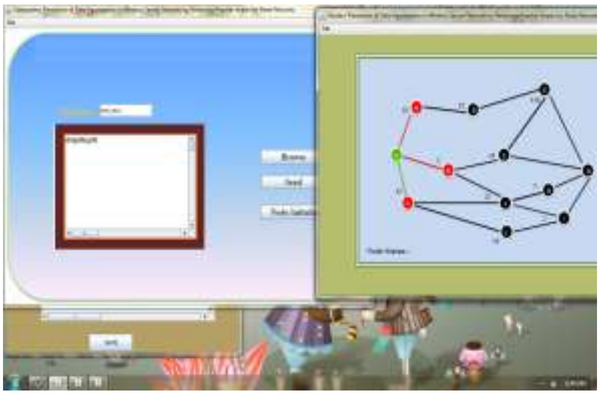

Fig 5.2 : Router Form as Graph

According to the Fig 5.2 shows the source form and router form. you select which file you send from source node to destination node.

Defined the source node and destination node. then this file as packets send from source node to destination node.

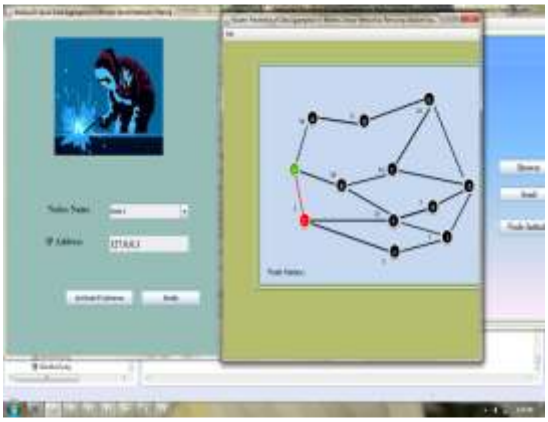

Fig 5.3 : Falsified Sub Aggregate Attack Based on IP Address

Thirdly, designed the attacker forms, one is IP Address and MAC Address of the node. designed the attacker forms, this attack is the falsified sub aggregate attack or false data injection attack is detected. Fig 5.3 shows that, In particular, compromised nodes can be used to inject false data that leads to incorrect aggregates being computed at the base station. One is IP Address and MAC Address of the node. We use the GetIp( ) function. For getting the IP Address of that node. All nodes of ip address is same because of the system is run on same system. Suppose system run on network, that time system generated the own ip address then those ip address assigned to all the nodes in graph. For detecting the attack in graph by using InjectFalsedata() , InjectFalseIp() functions. By using InjectFalseIp() function inject the false Ip of that node.

Falsified sub-aggregate attack or False Data Injection Attack based on IP Address : *Node C* just flips bit *j* in ˆ *BC* from ‘0’ to ‘1’—not having a local aggregate justifying that ‘1’ in the synopsis. ‘Red’ mark indicate that node is attacked according to the falsified sub aggregate attack based on IP Address. Used the GetIp( ) for getting the IP address of the that node whose is attacked that means that node of IP Address is changed. suppose more than node are attacked recover the node by using attack resilient algorithm. The Service provider browses the required file and uploads their data files to the Specified End User (A, B, C, D) and with their DIP (Destination IP) of End User.

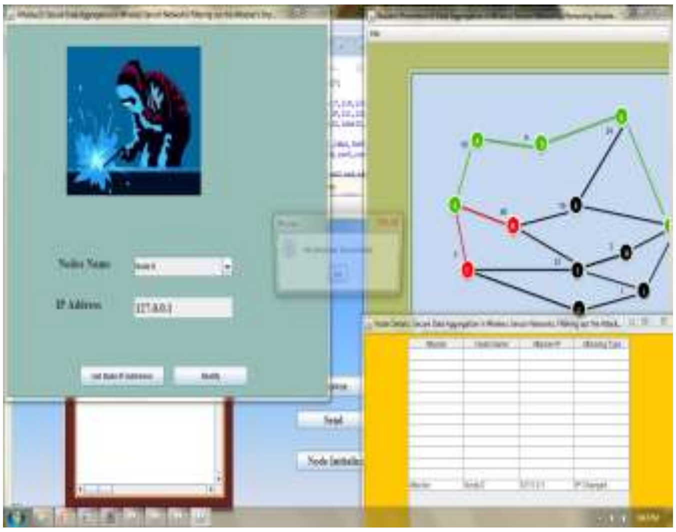

Fig 5.4: Recover the Node A and File Received Successfully

Fig 5.4 Shows the , recover the node by using attack resilient algorithm the choosed the shortest path by using SSSD Dijkstra Algorithm. Last part will be remaining of falsified sub aggregate attack or False Data Injection Attack based on MAC Address.

6. CONCLUSION

This paper gives a proposed work of secure data mixture thought in remote sensor frameworks. To give the motivation driving secure data aggregation, in any case, the security necessities of remote sensor frameworks are displayed and the danger model and badly arranged model are unveiled to sufficiently handle security requirements of

WSN. Second, an expansive outlining in order to compose study is presented the data gathering traditions. There are still open issues with WSN security essentials which maintain security for duplicate delicate combination limits in the midst of data accumulation process.

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

[3] [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 inComputerScience 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",*Conferenc iPGCON-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," *in Proc. IEEE 20th Int. Conf. Data Eng. (ICDE),2010*