Improved Secured Data Aggregation in Wireless Sensor Network by Attack Detection and Recovery Mechanism

Mr. Ashvin Selokar & Prof. Parul Bhanurkar
TGPCET Mohgoan NAGPUR

Abstract: *The remote sensor system is enclosed by gathering of substantial no. of sensor hubs. The sensor focus focuses have the point of confinement of recognizing the weight, vibration, advancement, suddenness, and sound as in and so forth. In perspective of a need for liberality of checking, remote sensor structures (WSN) are routinely 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 territories examination of Attack Prevention by Node Recovery other than gives a thought to how to defeat the issue. What's more, distinguishing the assaults by utilizing IP and MAC Based Data Injection Techniques. Besides, the SSSD Dijkstra estimation for finding the briefest path from source center point to destination center. Moreover, by utilizing AES Algorithm , give more security in the framework.*

Keywords: **IP Injection; Mac Injection; AES**

1. INTRODUCTION

The remote sensor framework is molded by broad number of sensor centers. Sensor center points 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 versatile calculation comprises of two stages. The primary thought is as per the following: (i) In the principal stage, the BS determines a preparatory assessment of the total in light of insignificant verification 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 controlled by the assessment of the primary stage.

1.1 Wireless Sensor Network

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

1.2 Data Aggregation

Information Aggregation is an essential methodology to fulfill power efficiency in the sensor framework. The accumulated data must be taken care of by sensor to reduction transmission. It utilized the Tree Based Approach. For totaling the estimations of hub. What's more, produce the spreading over Tree in the chart.

2. RELATED WORK

Sankardas Roy , Proposed [1] The once-over dissipating strategy secure against the snare dispatched by managed focus focuses. Our strike strong number enrolls the genuine total by sifting through the obligations of traded off focuses in the collection chain of hugeness. Basically 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 zones examination of Attack Prevention other than gives a thought to how to beat the issues. Besides, the dijkstra estimation for finding the briefest route from source center to sink center. 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 storing method and likewise get exact amassed results. depicted unmistakable customs for securing totaled information in remote sensor structures. Nandini. S. Patil, Proposed[5] information blend which enchanting framework for information gathering in scattered structure models and segment access by strategy for remote framework.

3. PROPOSED SYSTEM

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

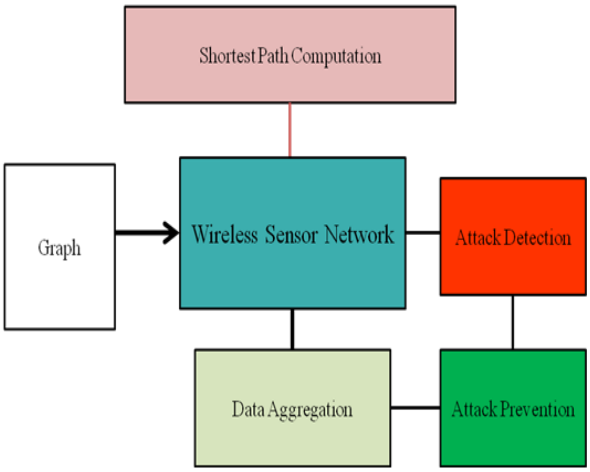


Fig 3.1: Basic System Architecture

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: $S \leftarrow \emptyset$
Step4: $Q \leftarrow V$
Step5:          while $Q \neq \emptyset$
Step6:          do   $u \leftarrow mindistance(Q, dist)$
 Step7: $S \leftarrow S \cup \{ u \}$
                    for all $v \in neighbors [u]$
 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

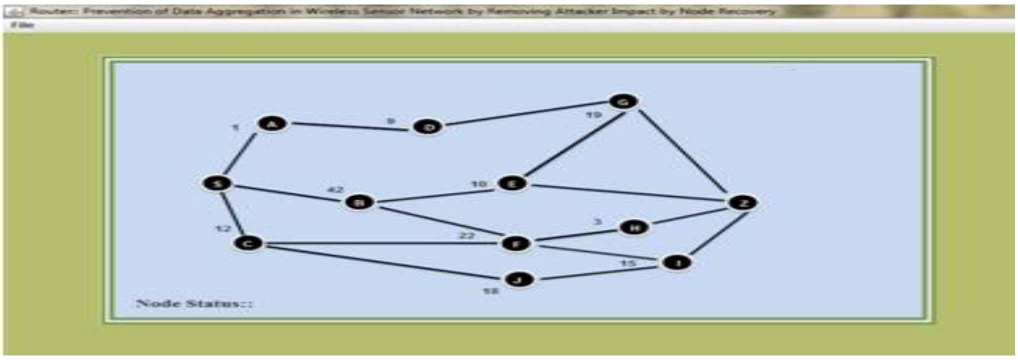

Router:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery
File
A
D
G
S
B
E
Z
C
F
H
I
J
1
9
19
42
10
12
22
3
15
18
Node Status::

Fig 5.1: Router Form as Graph with 12 nodes

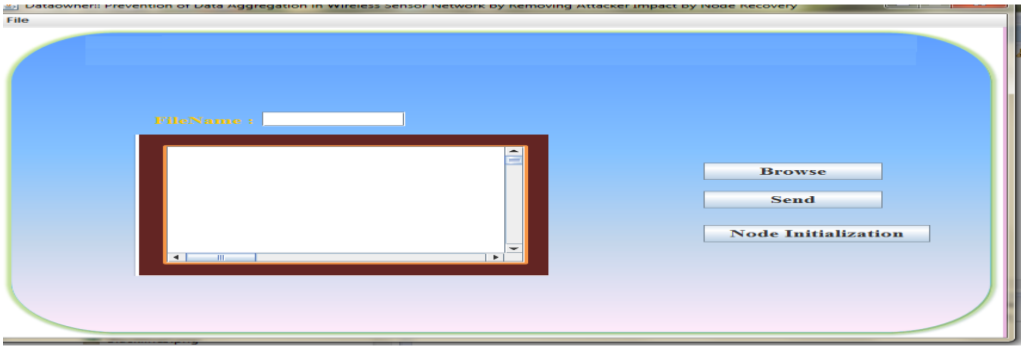
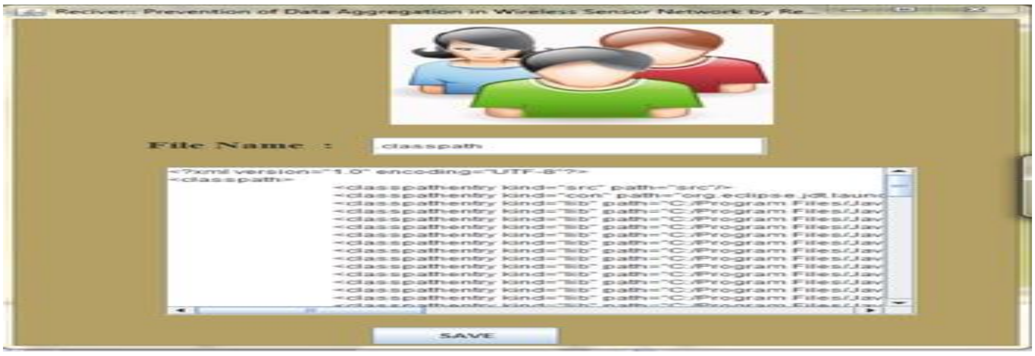

Dataowner:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery
File
FileName :
Browse
Send
Node Initialization

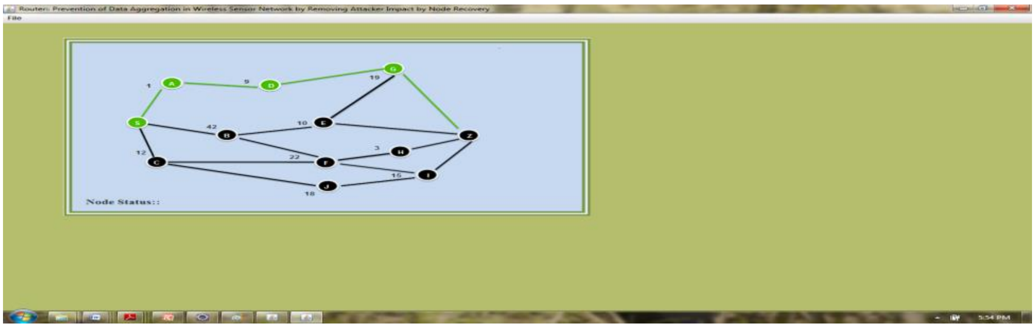
Fig 5.2 : Source Form


Reciver:: Prevention of Data Aggregation in Wireless Sensor Network by Re...
SAVE

File Name : classpath

```
<?xml version="1.0" encoding="UTF-8"?>
<classpath>
                    <classpathentry kind="src" path="src"/>
                    <classpathentry kind="con" path="org.eclipse.jdt.launc
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
                    <classpathentry kind="lib" path="C:/Program Files/Jav
```

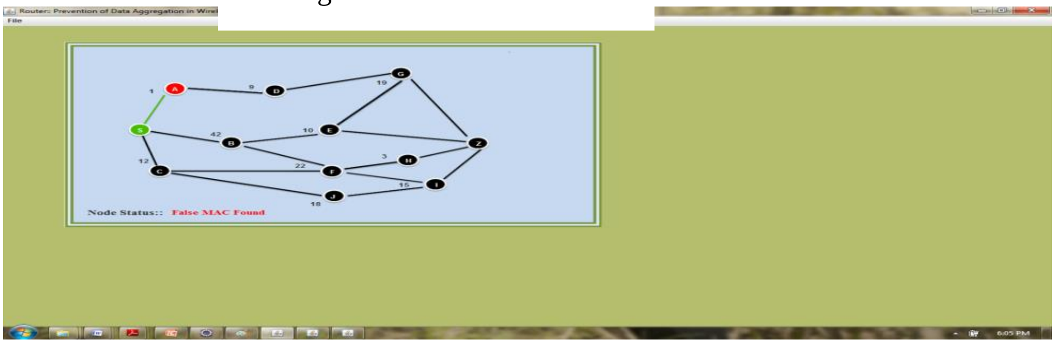
Fig 5.3 : Receiver Form



Router:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery

Node Status::

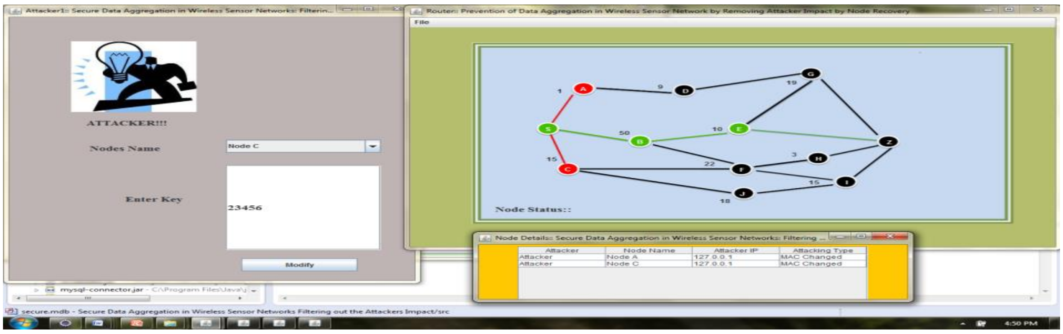
Fig 5.4 : Without Attack



Router:: Prevention of Data Aggregation in Wirel

Node Status:: False MAC Found

Fig 5.5 : MAC Based Data Injecton Attack



Attacker1:: Secure Data Aggregation in Wireless Sensor Networks: Filterin...

ATTACKER!!!

Nodes Name: Node C

Enter Key: 23456

Router:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery

Node Status::

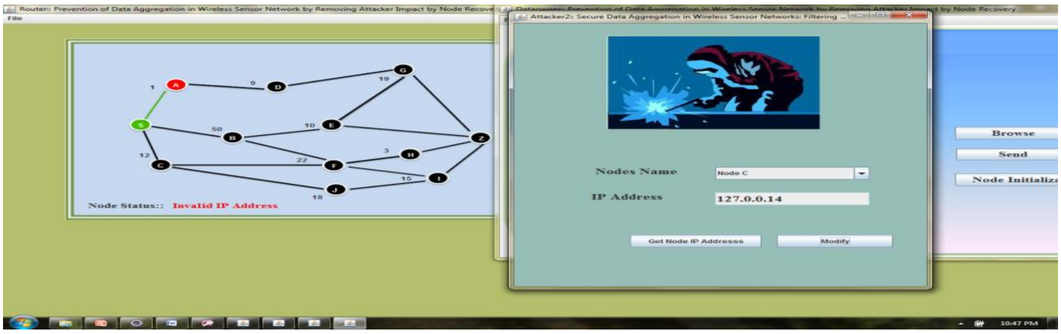
Node Details:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...

Attacker	Node Name	Attacker IP	Attacking Type
Attacker	Node A	127.0.0.1	MAC Changed
Attacker	Node C	127.0.0.1	MAC Changed

mysql-connector.jar - C:\Program Files\Java\

secure.mdb - Secure Data Aggregation in Wireless Sensor Networks Filtering out the Attackers Impact/src

Fig 5.6 : Recover the node in MAC Based Attack Condition



Router:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recove

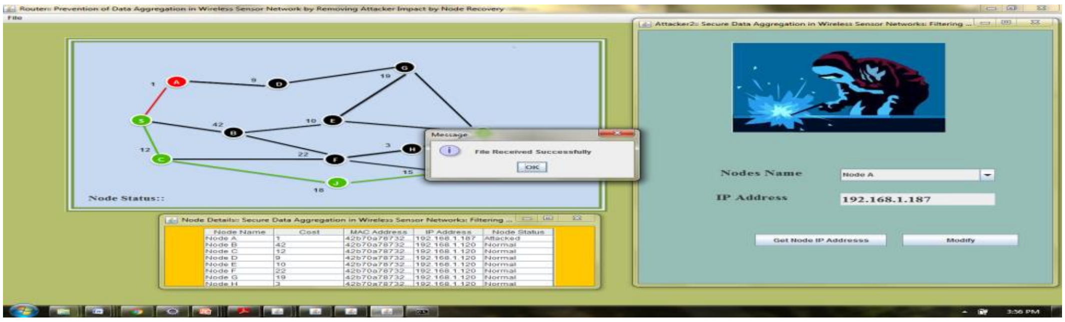
Node Status:: Invalid IP Address

Attacker2:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...

Nodes Name: Node C

IP Address: 127.0.0.14

Fig 5.7 : IP Based Data Injection Attack



Router:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery

File

Node Status::

Message

File Received Successfully

OK

Node Details:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...

Node Name	Cost	MAC Address	IP Address	Node Status
Node A	1	42b70a78732...	192.168.1.187	Attacked
Node B	42	42b70a78732...	192.168.1.120	Normal
Node C	12	42b70a78732...	192.168.1.120	Normal
Node D	9	42b70a78732...	192.168.1.120	Normal
Node E	10	42b70a78732...	192.168.1.120	Normal
Node F	22	42b70a78732...	192.168.1.120	Normal
Node G	19	42b70a78732...	192.168.1.120	Normal
Node H	3	42b70a78732...	192.168.1.120	Normal

Attacker2:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...

Nodes Name: Node A

IP Address: 192.168.1.187

Fig 5.8 : Recover the node in IP Based Condition

The simulation studies involve the deterministic random topology with 12 nodes as shown in fig 5.1. The proposed system implemented in the JAVA. According to the proposed system, The system run on local host that why all the nodes of addresses are same. That is standalone system. we transmit the packets from Source Node A to Destination Node Z. Then detecting the Falsified sub Aggregate attack or false Data Injection Attacks based on IP & MAC Address. Main Focus of proposed system is the Attack prevention through Node Recovery. After preventing attacks packets sends from source node to destination node with finding better shortest path.

The Fig 5.1 shown that simulation of nodes. And perform the node inilization that is all the cost assign to nodes. Fig 5.2 & 5.3 shown that Source & Receiver Form. In source form, browse the file for sends. Receiver Form, shows that Received the files at the destination node Z. and save it in Database. The Fig 5.4 shows that all the nodes are attacked free. then sending the selecting file from Source Node S to Destination node Z within 32 ms. 'Green' color defined that are nodes are attacked free. The Fig 5.5 & 5.6 shows that Node A & Node C are attacked by the MAC based Attacker. That is MAC Address of that attacked node is changed. Using MAC Based Data Injection Technique.Then 'Red' color indicates the node is attacked by the attacker. Fig 5.6 shows that recover the next node and the generate the Better shortest path from Source Node to Destination Node. The Fig 5.7 & 5.8 shows that Node A is attacked by the IP based attacker. Indicates the attacked node. By using IP Based Data Injection Technique. And recover the next node and calculate the shortest path from source node to destination node.

5. RESULT & DISCUSSION

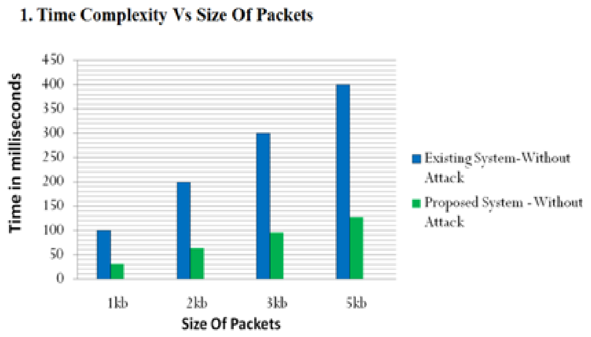


Fig 6.1 : size of packets with respect to Time

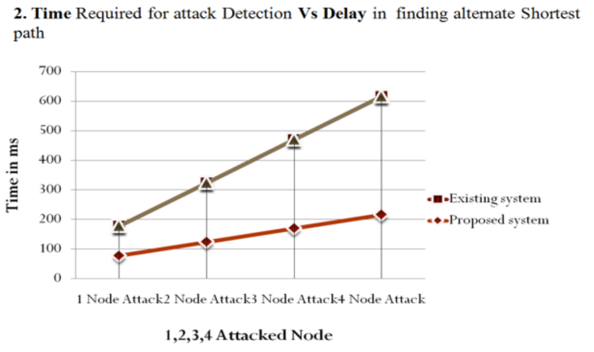


Fig 6.2 : Condition of Attacked Node as 1, 2, 3, 4

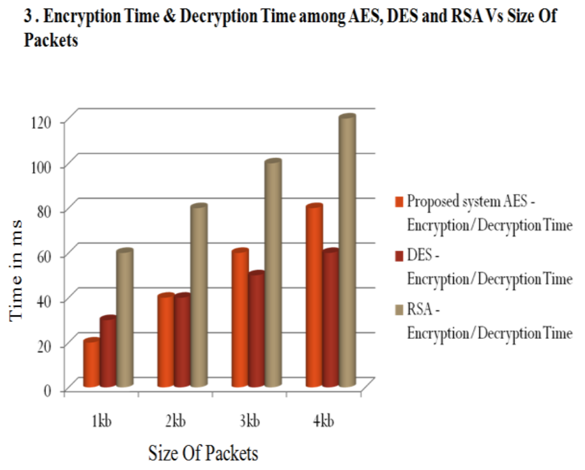


Fig 6.3 : Comparison of Proposed System AES algorithm & Prevoius Algorithm

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 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. The results are studied with respect to Time, Size of Packets, Throughput in without attack and with attack , encryption time and decryption time of AES and MAC Protocol by Attack Detection when existing system , Node Recovery mechanism proposed work is operated. Provided the Falsified sub Aggregate Attack detection by using IP and MAC Based False Data Injection Attack technique. Provided more security at the time of send the file from Source node to destination node by AES algorithm. Provided efficient shortest path calculation by SSSD Algorithm. Provided Attack prevention through Node Recovery.

FUTURE SCOPE

- To provide energy efficiency while detection of attacks.
- Use for multiple shortest path algorithms for fast processing.
- Providing more methods to attacks.
- Fast packet recovery mechanism

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] 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*