Attack Prevention of Secure Data Aggregation in Wireless Sensor Network by Node Recovery

Minal D. Kamble, Mr. Vikash Kumar

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 by Node Recovery besides gives an idea to how to overcome the issue. And detecting the attacks by using IP & MAC Based Data Injection Techniques. What's more, utilize the SSSD dijkstra calculation for finding the briefest way from source hub to destination hub. Furthermore, by using AES Algorithm, give more security in the system.

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 system is shaped by extensive number of sensor hubs. Sensor hubs may be homogeneous or heterogeneous. These sensor centers involves four central units: recognizing unit, taking care of unit, transmission unit, and power unit. For listening event, sensor center points ere altered. Exactly when an event happens, by delivering remote movement sensors light up the end point or destination node.[1] The attack-resilient computation algorithmconsists of two phases. The main idea is as follows: (i) In the first phase, the BS derives a preliminary estimate of the aggregate based on minimal authentication information received from the nodes. (ii) In the second phase, the BS demands more authentication information from only a subset of nodes while this subset is determined by the estimate of the first phase.

1.1 Wireless Sensor Network

Remote Sensor Network is a gathering of particular transducers with a correspondences base for observing and recording conditions at various areas.(expansive no. of sensors hub). Wireless sensor networks will consist of large numbers of small, battery-powered, wireless sensors. Remote sensor frameworks are a crucial advancement for generous scale checking, giving sensor estimations at high common and spatial determination.[2] Wireless Sensor Network (WSN) is the framework which is extensively used as a piece of bonafide applications for watching and highlight observation

1.2 Data Aggregation

Data Aggregation is a vital procedure to accomplish power productivity in the sensor system. The gathered information must be handled by sensor to decrease transmission. It used the Tree Based Approach. For aggregating the values of node. And generate the spanning Tree in the graph.

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

SankardasRoy , 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 remotesystem.

3. PROPOSED SYSTEM

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

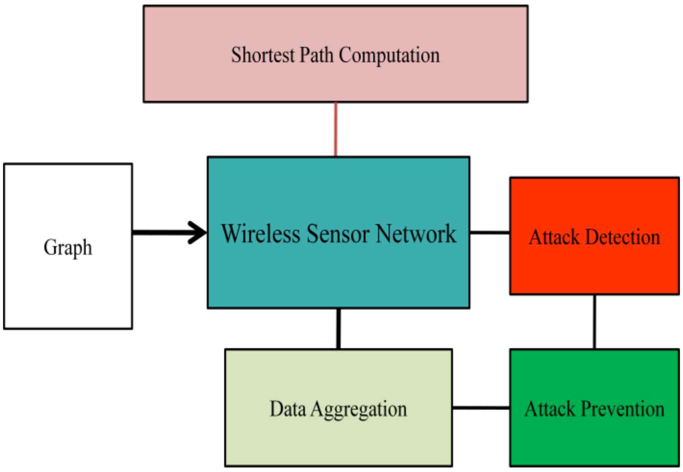


Fig 3.1: Basic System Architecture

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 pointthen onto the following center point.

3.1 METHODOLOGY

3.1.1. SSSD Dijkstra Algorithm

```
Step1: dist[s] ←0
for all v € V – { s }
Step2:          do  dist[v] ←∞
Step3: S ←∅
Step4: Q ←V
Step5:           while Q ≠ ∅
Step6:           do   u ← mindistance(Q, dist)
 Step7: S← S ∪{ u }
for all v ∈ neighbors [u]
 Step8:          do  if  dist[v] > dist[u] + w(u, v)
 Step9:           then d[v] ←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

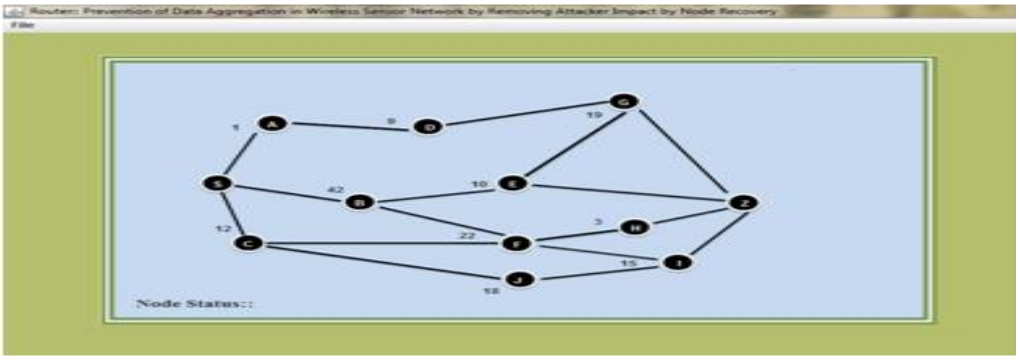

Router: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery
File
A
D
G
S
B
E
Z
C
F
H
I
J
1
9
19
42
10
12
22
3
15
18
Node Status::

Fig 5.1: Router Form as Graph with 12 nodes

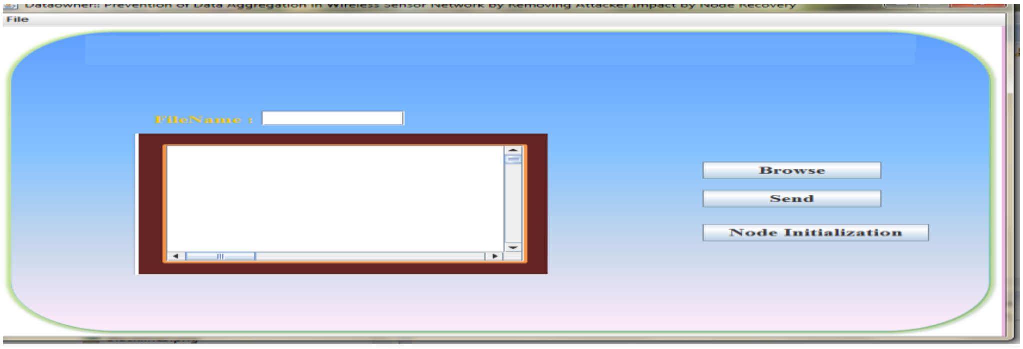
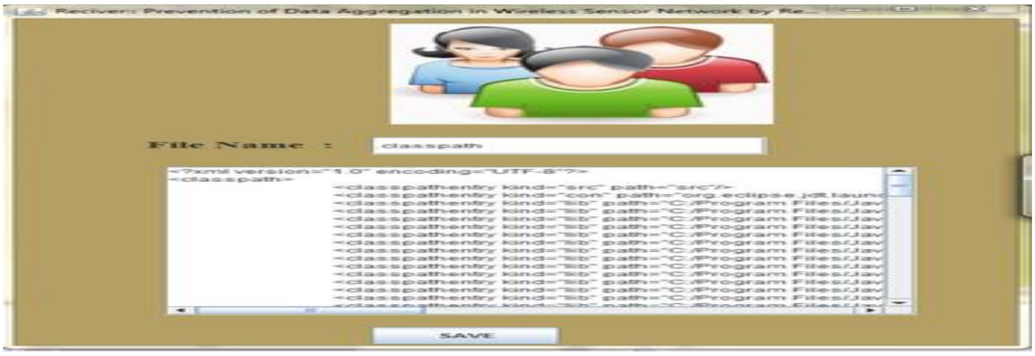

Dataowner:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery
File
FileName :
Browse
Send
Node Initialization

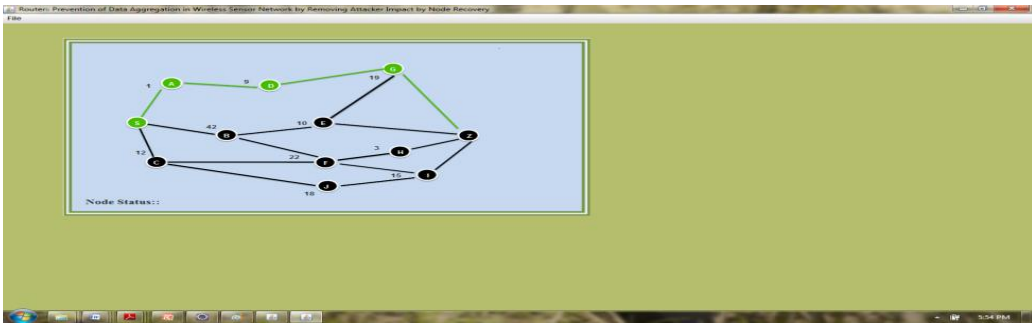
Fig5.2 :Source Form


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

File Name : classpath

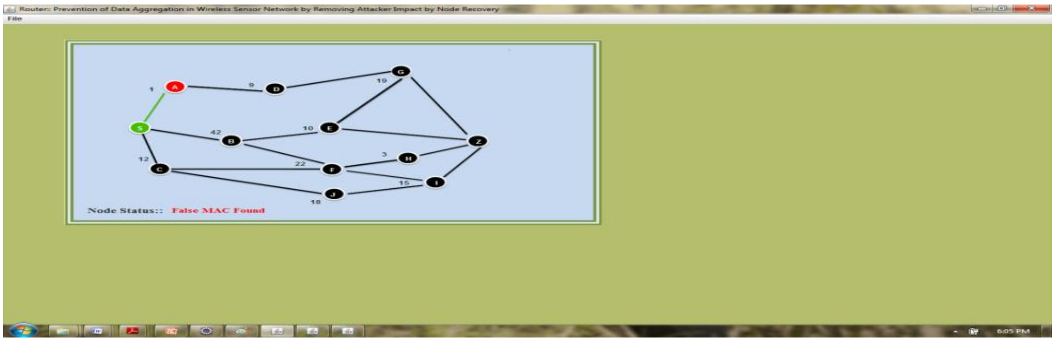
```
<?xml version="1.0" encoding="UTF-8"?>
<classpath>
		<classpathentry kind="src" path="src"/>
		<classpathentry kind="con" path="org.eclipse.jdt.launc
		<classpathentry kind="lib" path="C:/Program Files/Jav
		<classpathentry kind="lib" path="C:/Program Files/Jav
		<classpathentry kind="lib" path="C:/Program 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
		<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
File
A
D
G
S
B
E
Z
H
C
F
I
J
1
9
19
42
10
3
12
22
15
18
5:54 PM

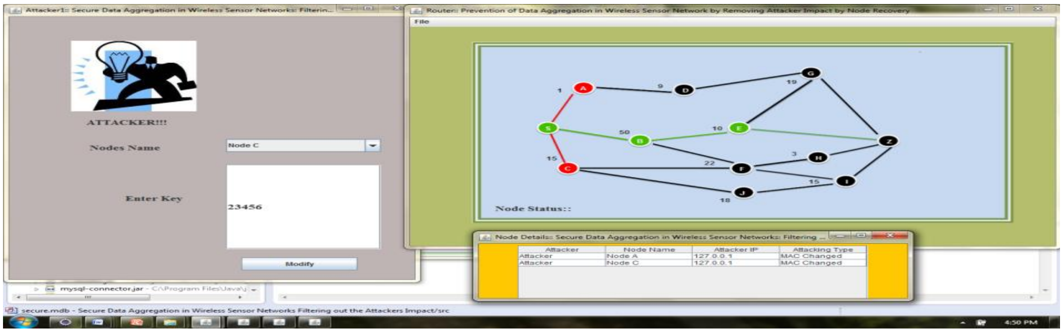
Node Status::

Fig 5.4 : Without Attack


Router:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recovery
File
A
D
G
S
B
E
Z
H
C
F
I
J
1
9
19
42
10
3
12
22
15
18
6:05 PM

Node Status:: False MAC Found

Fig 5.5 : MAC Based Data Injecton Attack


Attacker1:: Secure Data Aggregation in Wireless Sensor Networks: Filterin...
ATTACKER!!!
Modify
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
J
I
1
9
19
50
10
15
22
3
15
18
Node Details:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...
4:50 PM

Nodes Name: Node C

Enter Key: 23456

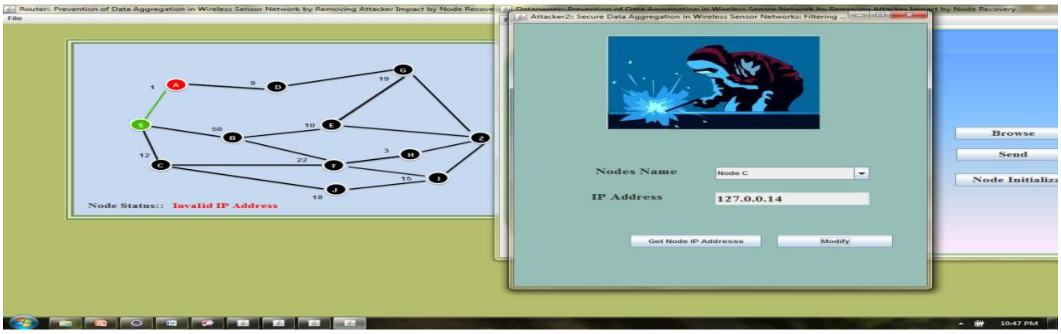
Node Status::

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\j

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

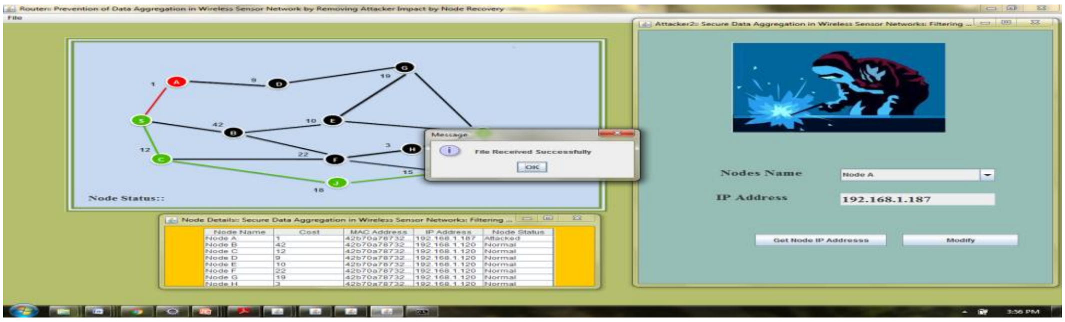

Router:: Prevention of Data Aggregation in Wireless Sensor Network by Removing Attacker Impact by Node Recove
File
A
D
G
S
B
E
Z
C
F
H
J
I
1
9
19
50
10
12
22
3
15
18
Attacker2:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...
Get Node IP Address
Modify
Browse
Send
Node Initializ
10:47 PM

Node Status:: Invalid IP Address

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
A
D
G
S
B
E
C
F
H
J
1
9
19
42
10
12
22
3
15
18
Message
OK
Attacker2:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...
Get Node IP Address
Modify
Node Details:: Secure Data Aggregation in Wireless Sensor Networks: Filtering ...
3:56 PM

Node Status::

File Received Successfully

Nodes Name: Node A

IP Address: 192.168.1.187

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

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

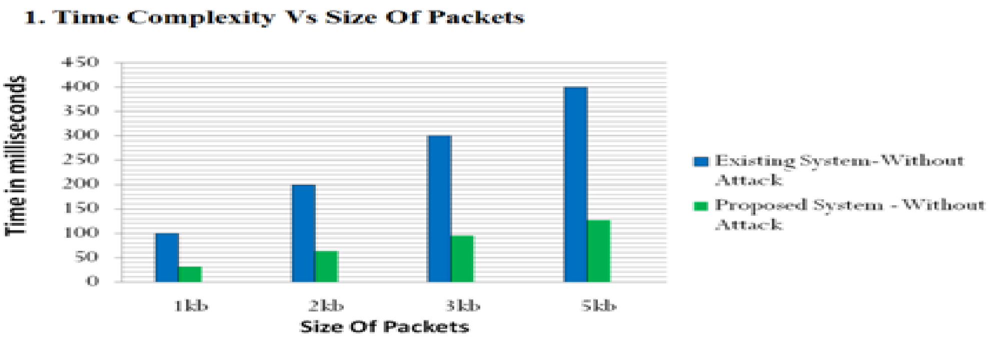

1. Time Complexity Vs Size Of Packets

Fig 6.1 : size of packets with respect to Time

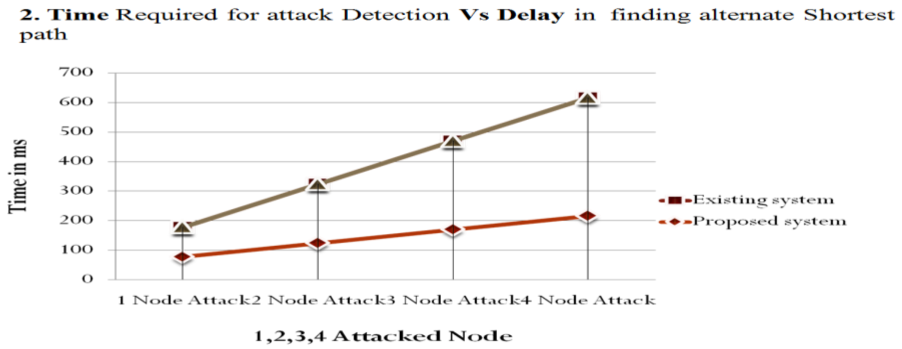

2. Time Required for attack Detection Vs Delay in finding alternate Shortest path

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

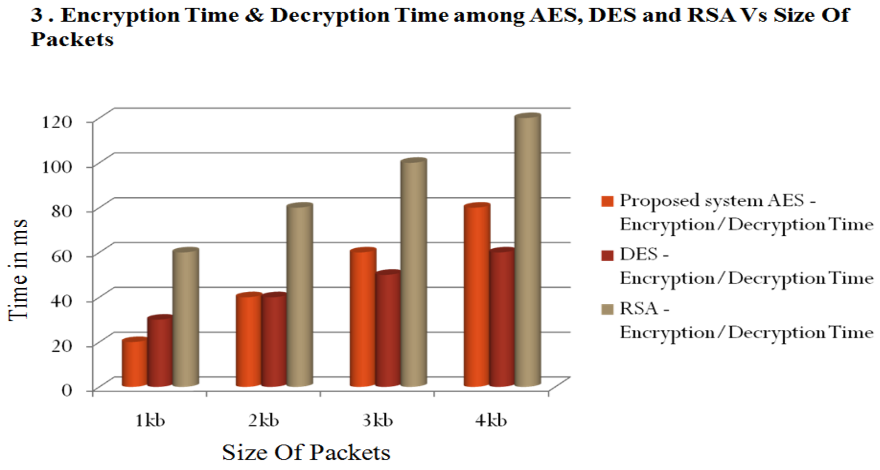

3 . Encryption Time & Decryption Time among AES, DES and RSA Vs Size Of Packets

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 AESused 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, and 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 NaveenGarg , “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] RabindraBista and Jae-Woo Chang, “Privacy-Preserving Data Aggregation Protocols for Wireless Sensor Networks:ASurvey”,*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, SanjeevSetia, SushilJajodia, “Attack Resilient Hierarchical Data Aggregation in Sensor Networks”, in *Proc. ACM Workshop Security Sensor AdhocNetw. (SASN), 2006, pp. 71–82.*

[11] SnehalLonare, Dr. A. S. Hiwale, “A Data Aggregation Protocol to Improve EnergyEfficiencyinWirelessSensorNetworks”,*ConferenciPGCON-2015*

[12]KiranMaraiya, 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] AfrandAgah and SajalK.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] ArijitUkil, “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. SensorSyst. (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*