International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

EN-ROUTING FILTERING SCHEME FOR WIRELESS NETWORK

Namrata P. Mishra[1], Samadhan D. Mali[2]

PG student, Digital Systems (Electronics), SCOE, Pune, India[1]

Assistant Professor, E&TC, SCOE, Pune, India[2]

ABSTRACT

In any wireless sensor network detection of compromised node is very important. It has affected the reliability and efficiency of wireless sensor network. False report will be inserting in the network via compromised nodes, which can prompt false alerts as well as the exhaustion of restricted energy assistance in a battery fuelled system. The false information infusion in a CPNS is achieved by using cluster network. In this paper, we have reviewed and analyzed different methods which detect faults results created by compromised nodes. Therefore it is very important to find out the route which maximize end to end throughput. Therefore Spatial Reusability Routing is discussed.

Keyword- Multipath, SAAR routing protocol, Spatial Reusability Routing, wireless sensor network, etc.

I. INTRODUCTION

Wireless sensor network made up of large number of sensor nodes. Now days in various applications the sensors and actuators are used to monitor the physical systems. The cyber physical network system is made up of sensors, actuators and wireless network. In wireless sensor network it is very important to select the route which gives the maximum throughput and with minimum overall number of transmission. In this proposed methodology the polynomial based compromised resilient en-routing filtering with implementation of single path routing and any path routing is discussed. In the proposed methodology the different parameter such as end to end throughput, Delay chart, Packet loss ratio and Packet Delivery ratio are analyzed.

II. LITERATURE SURVEY

The overview of various routing protocols such as Statistical En-Routing Filtering (SEF), Location Based Resilient Security Solution (LBRS), Location- Aware End to End Data Security (LEDS) and Random Perturbation Based (RPB) are used in wireless sensor network. In [1] the cyber physical network systems to avoid false data injection attack multiple en- routing scheme are proposed. To deal with false data injection, the Polynomial-based Compromised-Resilient En-route Filtering scheme (PCREF) is implemented. This method can filter false injected data efficiently and gain a high resilience to the number of compromised nodes. In [2] this scheme, a legal report is generated by multiple sensing nodes using their different authentication keys from one way hash chains. Cluster head uses approach to disseminate the authentication keys of sensing nodes along multiple paths toward the base station. There is another scheme which is implemented [3] a mixed hop by hop

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

authentication scheme that assures the base station will find any injected false data packets when no more than a fix en number sensor nodes are vulnerable to attacker. This work [4] proposes some research activities in WSN, including networking issues and coverage and deployment issues. Then, we review some CPS network systems that have been designed for, including health care, navigation, rescue, intelligent transportation, social networking, and gaming applications

III. IMPLEMENTATION DETAILS

3.1 System Overview

In this proposed system, en route filtering technique which can be used in wireless networks, with which the intermediate nodes checks the correctness of the data that is being transmitted along the route from source to the sink with the help of intermediate nodes . This intermediate node exists in wireless sensor network to route data packet from source to sink node or destination node. The intermediate node not only checks the correctness of the data but also can filter the false data effectively. The intermediate node continuously check packet received with valid detail. If sink node or trust node receive data packet without filtered, the sink can filter packet detail for attacked or data forgery from packet. To carry out these above operations the polynomial based compromised resilient en-route filtering is adopted in the proposed system. In addition to this, by considering spatial reusability of the wireless communication the multipath routing scheme are also available for packet forwarding to the destination or sink node. The multipath routing scheme based on spatial reusability aware single path routing (SAAR) any path routing (SAAR) protocols and the remaining part of polynomial based compromised resilient en-route filtering is implemented in proposed methodology.

Fig. 1. Shows the proposed system architecture of proposed system. As shown in architecture the polynomial based compromised resilient en-routing filtering with implementation of single path routing and any path routing are implemented

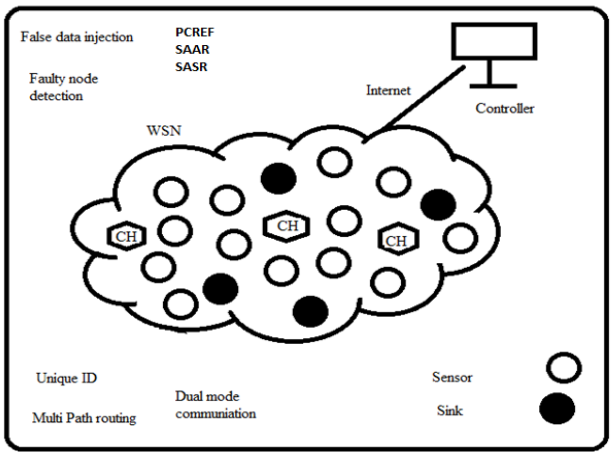

Fig. 1. Shows the proposed system architecture of proposed system.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

3.2 Mathematical Model

False data injection with multipath routing

Let us consider S as a set en-routing scheme to avoid false data injection,

S= { }

Input

1. Identify the inputs as number of nodes
2. F= {f_1, f_2, f_3 ....., f_n| 'F' as set of functions to execute to routing model
3. I= {i_1, i_2, i_3…|'I' sets of inputs to number of nodes/ sensor
4. O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets}

   S= {I, F, O}

Where,

I = {Number of nodes}

O = {false data injection filtering, multipath route}

F = {Shortest Path algorithm, SAAR, SASR}

3.3 Algorithm

The algorithm implemented for the for packet transmission in wireless packet transmission is given below. This is request and response model for packet acknowledgement.

Input : - Number node, neighbors, connection Links

Output: - Network scheduling with distributed network

Step1 :- Calculate Weight for each connection

Step2 :- Break connection with similar weight

Step3 :- Find node which having multiple connection with Free neighbor

Step4:- While Links. Size Do

{

If links. Match(request) Then

{

Matched link

}

Else

{

Send matching request to node

}

}

Step5:-IF request. Match (link) then

{

Send matched reply to node

Send drop message to free neighbors

}

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

Step6:- If Matched reply from neighbor Then

{

Send drop message to free neighbors

}

Step7:- If Drop message Then

{

Acknowledge matched link

neighbors. Remove (node)

}

Step8:-

End

IV. IMPLEMENTATION STATUS

The Polynomial-Based Compromised-Resilient En-route Filtering scheme is implemented by designing graphical user interface (GUI) as shown in fig.2. At any time a user will be able to create wireless sensor network by using graphical view with the help of clicking on a button. The GUI consists of number of key factors such as total nodes, source node and destination node as shown in the fig.3.

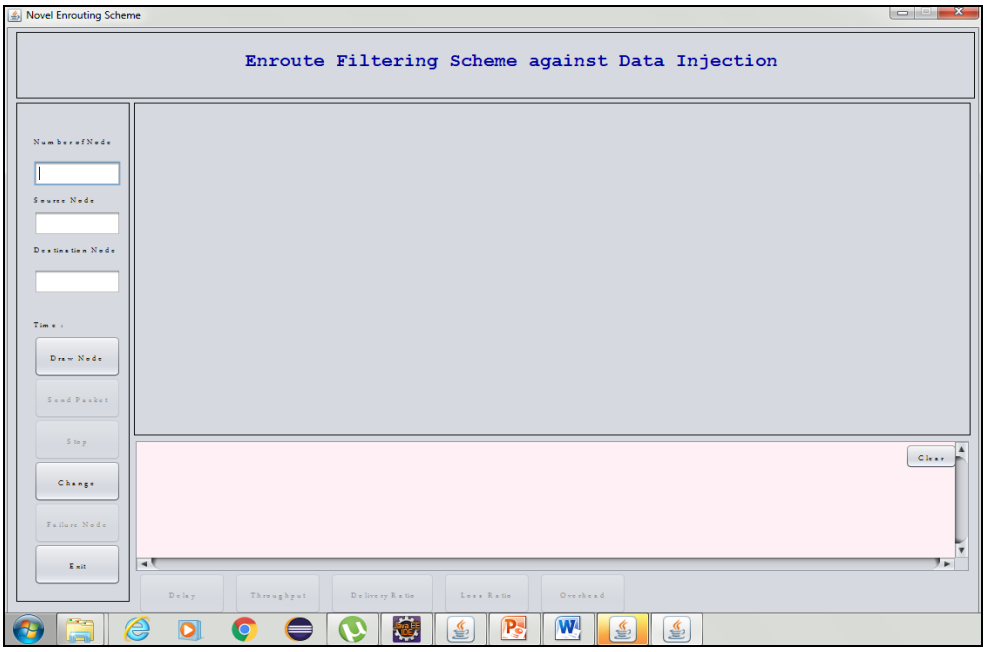

Fig.2: En-route filtering scheme using Graphical User Interface.

In the GUI, user will enter no. of total nodes and source node and destination node and after click on draw node button. The network simulator creates wireless sensor network by using graphical view and displays no. of sensor nodes, sink node.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

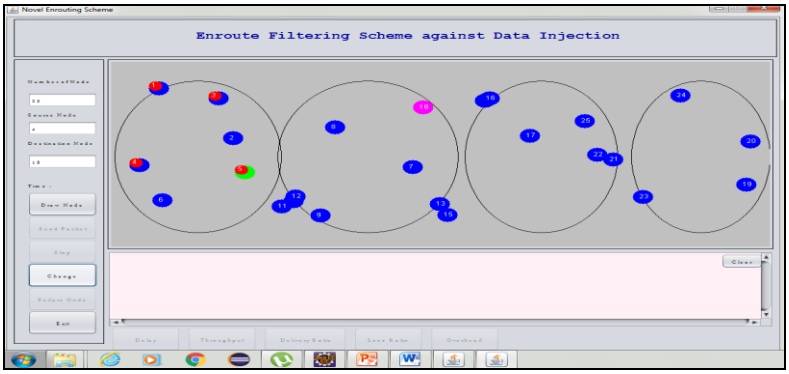

Fig.3: Example of Number of sensor nodes and destination node.

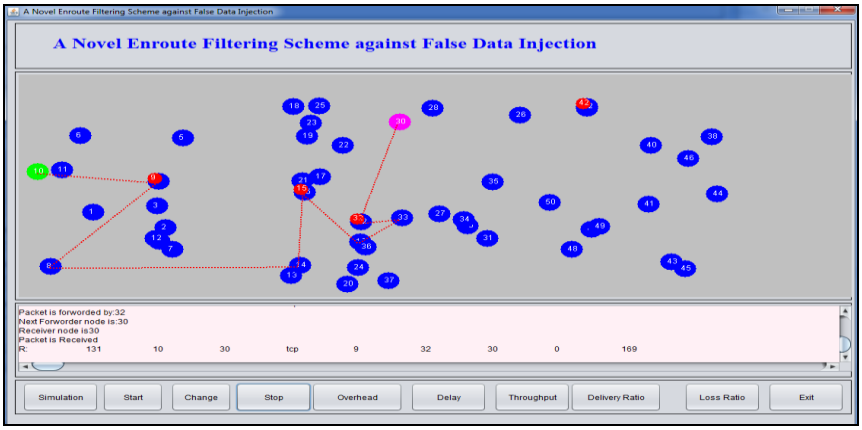

Fig.4: En-route filtering scheme.

V. SYSTEM ANALYSIS

In the proposed methodology the PCREF is used to filter false injected data and achieve high resilience to attack over data. Following graph shows throughput for packet transmission after polynomial authentication and check polynomials over encrypted data. Additionally, this system implements SAAR and SASR to reduce overhead and improve throughput maximization. The throughput computation results are shown below in fig.5.

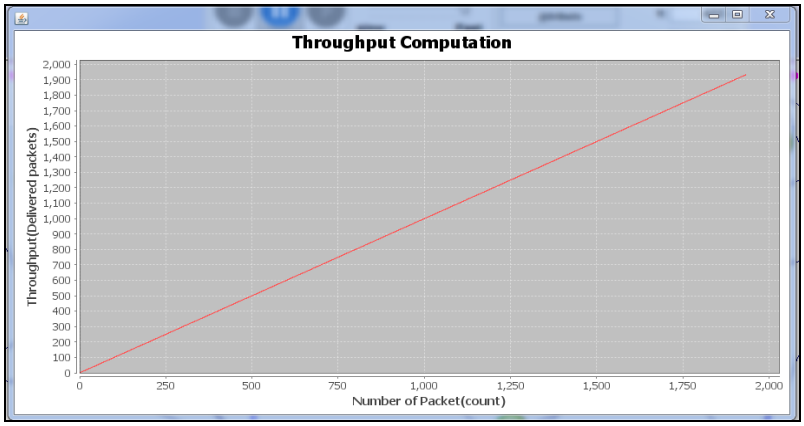

Fig.5: Throughput Chart

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

5.1 Delay Ratio.

This graph shows packet transmission delay ratio. This delay is reduced due to energy efficient packet data transmission using spatial available routing.

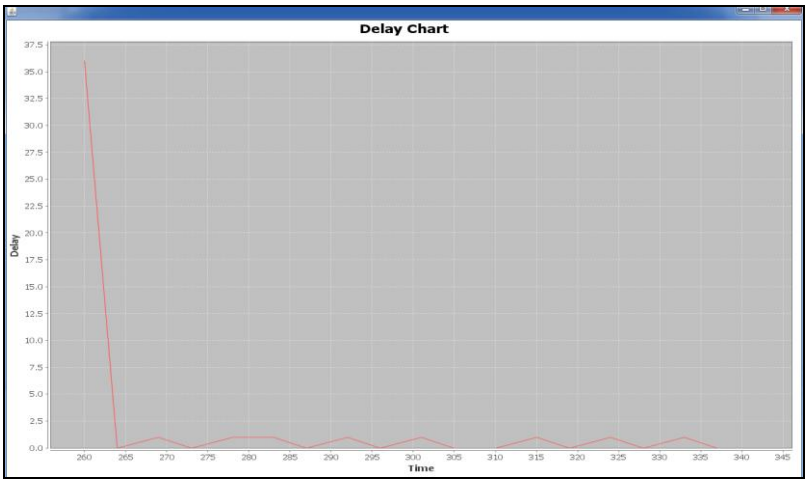

Fig.6: Delay Chart

5.2 Packet Loss Ratio

An en-route filtering scheme reduces packet loss ratio in WSN with energy efficient packet transmission by avoiding false data injection.

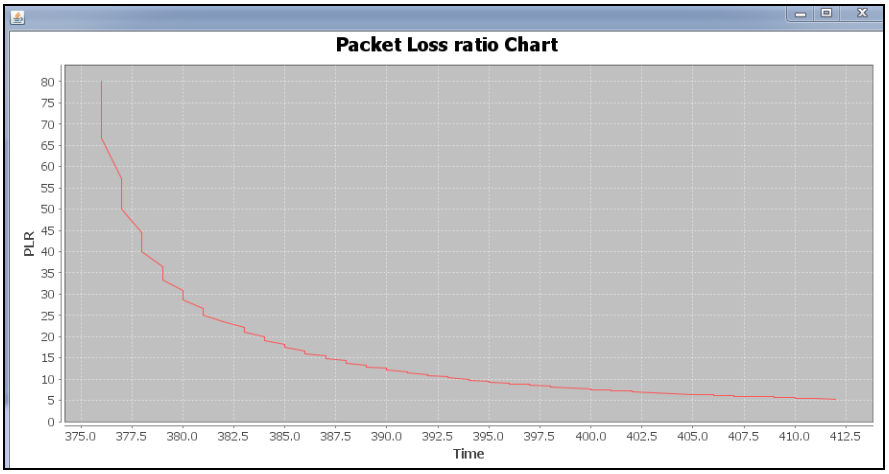

Fig.7: Packet Loss Ratio Vs Time.

5.3 Packet Drop Ratio (Before)

This graph shows that packet delivery before false data injection attack in wireless network.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

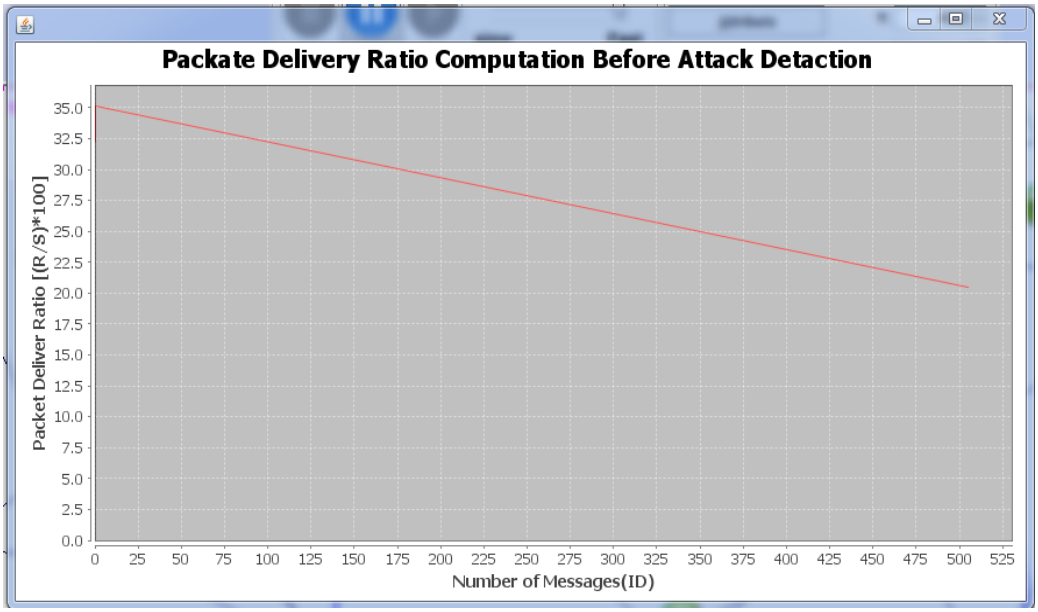

Fig.8: Packet Delivery Ratio Vs Time.

5.3 Packet Drop Ratio (After)

Following graph shows packet delivery ratio after false data injection avoidance and high resilience for data collection.

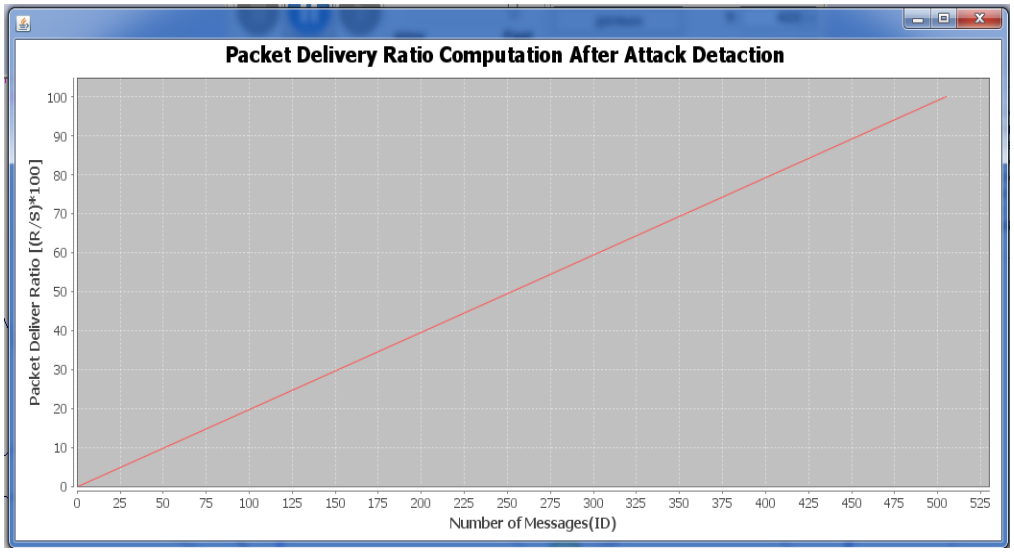

Fig.8: Packet Delivery Ratio Vs Time.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

5.4 Overhead

Novel en-route filtering scheme for data collection to avoid false data injection in wireless sensor network uses polynomial based authentication and authorization of data and sensors. These sensors are authorized in terms of digital signature verification to avoid overhead for authentication each time. Spatial routing helps to reduce overhead between network nodes to transfer packet.

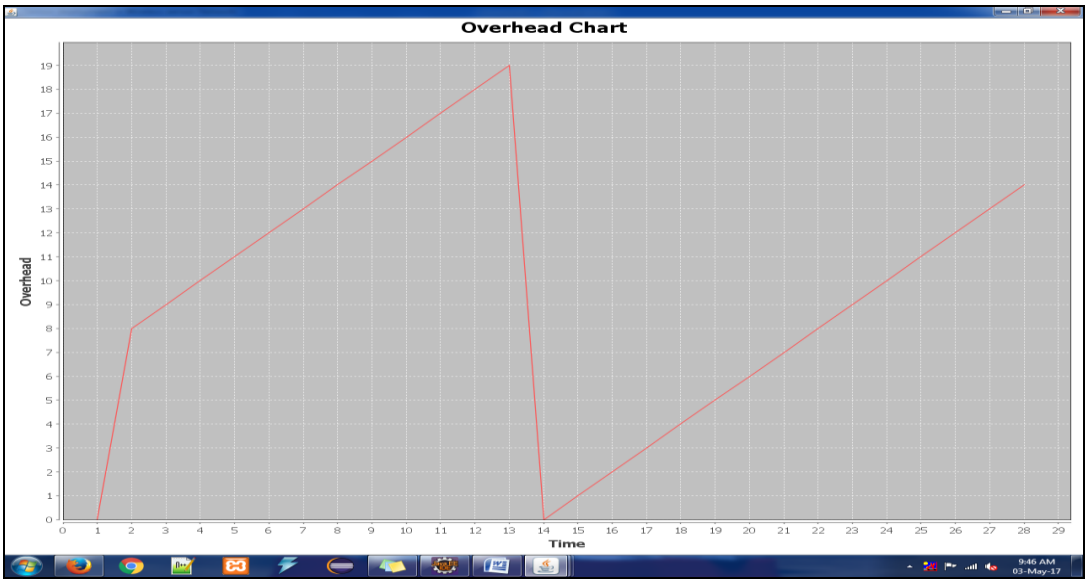

Fig.9: Overhead Vs Time.

5.4 File Transfer

In the proposed methodology for packet transmission after polynomial authentication and check polynomials over encrypted data and file is transfer from source to destination, the file is verified then it transfer to destination. The verified file is shown below.

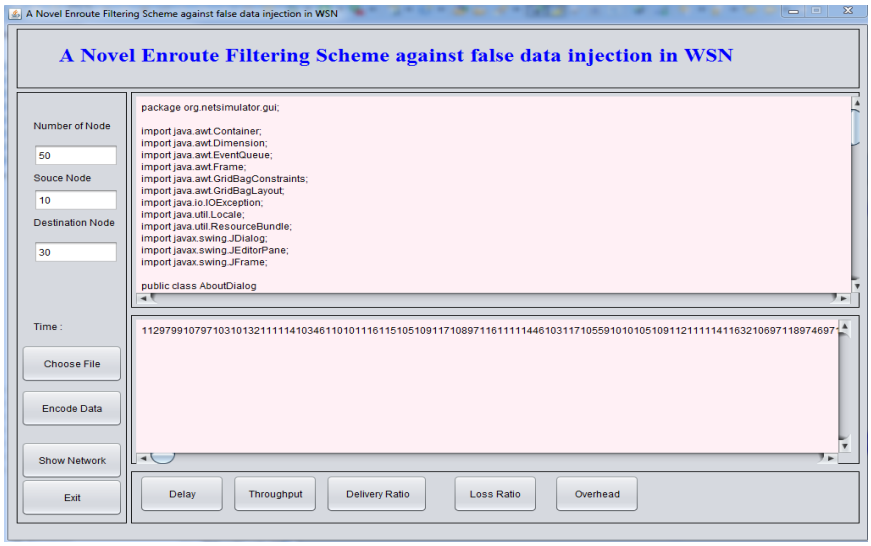

Fig.9: File Transfer in wireless Network.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

5.5 Comparison of Performance Parameters.

In the polynomial based compromised resilient en-routing filtering and in proposed system the performance parameters are given in the tabular form.

Goals	Existing System	Proposed System
Network	Unicast- Hop by Hop	Clustering based
Security	Authentication Polynomial and Check Polynomial	PCREF + Digital Signature based authentication and authorization
Methodology	Hop to Hop data collection	Cluster wise data collection
Routing	DSR	Radio Resource Control
Algorithm	Shortest Path Routing	SAAR and SASR

VI. CONCLUSION

In the wireless sensor network to avoid false data injection the en-route filtering scheme is implemented. To avoid false data injection in wireless, data collection uses authentication polynomial and check polynomial attributes about the sensor nodes. The Proposed system used in this paper demonstrates signature based data authentication to avoid misuse of information collected. Since wireless network can be easily compromised with faulty nodes, to avoid sensor nodes are encrypted with digital signature generated for data transmission across the network. Wireless sensors are filtered by different attributes like energy, packet transmission capacity. The proposed SAAR and SASR communication scheme reduces delay for packet delivery during clustered communication for data transmission and improves end to end throughput.

VII. ACKNOWLEDGMENT

I express my sincere thanks to my research guide **Prof. S. D. Mali** Department of Electronics & Telecommunication Engineering, for his valuable guidance and continuous support. Without his inspiration and help it would not have been possible for me to complete this paper. I take this opportunity to thank my PG Co-ordinator Dr**. (Mrs.) S.O. Rajankar** for her helpful suggestions. I would like to thank all my teaching and non teaching staff and my classmates for their direct or indirect co-operation in the successful completion of this project report. I would also like to express my gratitude's to those who were directly or indirectly guiding me.

REFERENCES

[1] Xinyu Yang_, Jie Lin, Paul Moulemay,WeiYuy, XinwenFuz and Wei Zhaox "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems" IEEE Transaction on computers, VOL. 64, No. 1, January 2015.

[2] Z. Yu. And Y. Gaun, "A dynamic en-route filtering scheme for data reporting in wireless sensor networks," IEEE Trans networking, Vol. 18, pp. 150-163, 2010.

[3] S. Zhu, S. Setia, "An interleaved hop-by-hop authentication scheme for filtering of injection false data in

sensor networks," ACM Trans sensor Network, Vol. 3, no. 4, pp. 259-271, 2007.

[4] F. Wu, Y. Kao, and Y. Tseng, "from wireless sensor networks towards cyber physical system," Pervasive mobile comput., Vol. 7, no. 4, pp. 397-413, Aug. 2011

[5] H. Yang and S. Lu. "Commutative cipher based en-route filtering in wireless sensor networks". In Proc. of 60th IEEE VTC, 2004.

[6] Y.-S. Chen and C.-L. Lei. Filtering false messages en-route in wireless multi-hop networks. In *Proc. of IEEE WCNC*, 2010.

[7] K. Ren, W. Lou, and Y. Zhang. Leds: Providing location-aware end-to end data security in wireless sensor networks. *IEEE Transactions on In Mobile Computing (TMC)*, 7(5):585–598, 2008.

[8] N. Subramanian, C. Yang, and W. Zhang. Securing distributed data storage and retrieval in sensor networks. In *Proc. of the 27th IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2007

[9] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh. Toward resilient security in wireless sensor networks. In *Proc. of the 6th ACM MobiHoc*, 2005.

[10] F. Ye, H. Luo, S. Lu, and L. Zhang. Statistical en-route filtering of injection false data in sensor networks. In *Proc. of the 23th IEEE INFOCOM*, 2004.

[11] L. Yu and J. Li. Grouping-based resilient statistical en-route filtering for sensor networks. In *Proc. of the 28th IEEE INFOCOM*, 2009.

[12] W. Zhang, N. Subramanian, and G. Wang. Lightweight and compromise resilient message authentication in sensor networks. In *Proc. of the 27th IEEE INFOCOM*, 2008.

[13] W. Zhang, M. Tran, S. Zhu, and G. Cao. A random perturbation-based pair wise key establishment scheme for sensor networks. In *Proc. of the 8th ACM MobiHoc*, 2007.

[14] S. Zhu, S. Setia, S. Jajodia, and P. Ning. An interleaved hop-by-hop authentication scheme for filtering of injection false data in sensor networks. In *Proc. of the 25th IEEE Symposium on Security and Privacy (S&P)*, 2004.