IJRRECS/December 2013/Volume-1/Issue-8/1764-1768 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFICIENT STRATEGY OF AGGREGATE SECURE DATA TRANSMISSION

K.Anusha[1], K.Sudha[2]

[1]M.Tech Student, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India

[2]Associate Professor, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India

ABSTRACT:

In large amount of sensor network, especially in case of data aggregation it should reduces the amount of communication and energy consumption. Recently, the research community has proposed a robust aggregation framework called synopsis diffusion which combines multipath routing schemes with duplicate-insensitive algorithms to accurately compute aggregates (e.g., predicate Count, Sum) in spite of message losses resulting from node and transmission failures. But these aggregation frameworks aggregation frameworks does not solve the problems which are appearing at base station side. In this paper, we make the synopsis diffusion approach secure against attacks in which compromised nodes contribute false sub aggregate values. Thorough theoretical analysis and extensive simulation study show that our algorithm outperforms other existing approaches. These problems may occur due to the irrespective of the network size, the per node communication overhead. In this paper, we make the synopsis diffusion approach secure against attacks in which compromised nodes contribute false sub aggregate values. In this paper, we develop mechanisms that generate dynamic dispersive routing algorithm. Under our design the routes taken by the "shares" of different packets change over time. So even if the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet. Besides randomness, the routes generated by our mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost. Extensive simulations are

conducted to verify the validity of our mechanisms.

Keywords: Aggregation of the data, Base station, Aggregation hierarchy, Aggregation in network, Security of the network sensor, Computational complexity respectively.

1. INTRODUCTION:

There is a lot of advancement takes place in the system with respect to the strategy of the transmission of the data in the wireless environment in a well efficient fashion respectively [1]. Here the networks related to the sensor oriented with the wireless phenomena in which there is a number of the applications included in it and some of them are monitoring wild habitat, detection of the forest fire followed by the surveillance of the military is a major concern respectively. As per the deployment oriented scenario by which organization of the nodes with respect to the sensor oriented with the sensor of the multi hop strategy is a well efficient related to the control of the central point base station is a major concern respectively [3][4].

BLOCK DIAGRAM

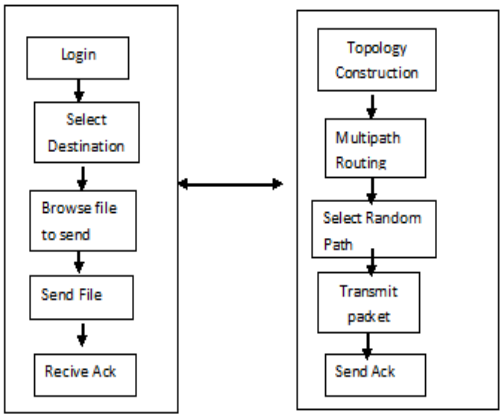


Fig 1: Shows the architectural representation of the present method respectively

2. METHODOLOGY:

In this paper a method is designed based on the well effective frame work oriented strategy in a well efficient manner respectively[2][5]. Here the implementation of the present technique followed by the analysis oriented aspect related to the architecture based strategy is shown in the below figure in terms of the block diagram based approach respectively. Here the

present method completely overcome the drawbacks of the several previous methods in a well efficient manner respectively [6][7][9]. Here the present implemented technique is designed in such a way in which there should be an accurate analysis is made on the lot of the previous methods oriented failures followed by the accurate analysis based aspect in a well efficient manner and improve the performance of the system followed by the improvement in the accurate outcome oriented strategy in a well effective manner respectively [8][10]. Therefore the present designed method is effective and efficient in terms of the performance based strategy followed by the outcome oriented pattern respectively.

3. EXPECTED RESULTS

A lot of analysis has been made between the present method to that of the several previous methods in a well efficient manner respectively. A comparative analysis is made between the present method to that of the several previous methods and is shown in the below figure in the form of the graphical representation respectively. There is a huge challenge for the present method where it is supposed to implement the technique in a well efficient manner where it is supposed to improve the performance of the present system respectively. There are a number of experiments have been conducted on the large number of the data sets in a well effective manner respectively. There is a huge challenge for the present method where it is supposed to control the degraded performance of the previous methods in a well efficient manner followed by the accurate outcome of the system based aspect towards the accuracy related analysis of the entire system respectively.

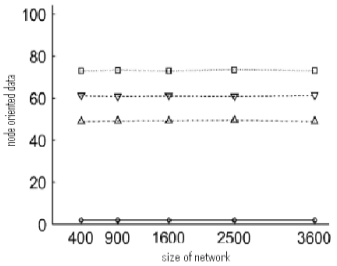


Fig 2: Shows the graphical representation of the present method respectively

4. Algorithm:

Step1: when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares, according to a (T,M)

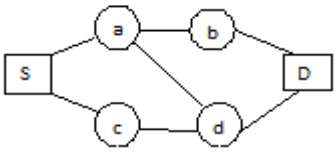
Ex: packet length - 20kb

T-2

Then (2kb,10)

(T, M)

Step2:



In this network available paths are 3

1.S-a-d-D

2.S-a-b-D

3.S-c-d-D

Step 3:

In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random paths.

TTL value=M=10

Step 4:

After receiving the one share to list, the TTL field is reduced by 1.

TTL=TTl-1

Step 5:

When the TTL value reaches 0, Once the Destination collects at least M shares, it can reconstruct the original packet.

5. CONCLUSION

In this paper a method is designed with a well efficient framework oriented strategy where there is an efficient improvement in the performance followed by the outcome in a well respective fashion in the entire system respectively. Here a new strategy is designed with a well effective framework in which related to the aggregate of the network based strategy in which issues of the security aspect by which aggregation of the computational phenomena includes the sum and count respectively. Here a huge research takes place in the system by which it is related to the phenomena of the corruption of the node compromization plays a major role in its implementation aspect followed by the aggregate base station estimation respectively. Here in which the algorithms are related to the phenomena of the hierarchical approach oriented ring based scenario is a major concern respectively. Here in order to overcome the above problem an algorithm is designed by the verification of the light weight strategy in which base station enabling takes place in the system followed by the followed by the effective verification of the valid aggregate computations respectively. In this paper, we develop mechanisms that generate Dynamic Dispersive Routing Algorithm.s Here we finally conclude that the present method is

effective in terms of the performance followed by the outcome in a well oriented fashion respectively.

REFERENCES

[1] P. Flajolet and G. N. Martin, "Probabilistic counting algorithms for data base applications," J. Computer Syst. Sci., vol. 31, no. 2, pp. 182–209, 1985.

[2] D. Wagner, "Resilient aggregation in sensor networks," in Proc. ACM Workshop Security of Sensor and Adhoc Networks (SASN), 2004.

[3] L. Buttyan, P. Schaffer, and I. Vajda, "Resilient aggregation with attack detection in sensor networks," in Proc. 2nd IEEE Workshop Sensor Networks and Systems for Pervasive Computing, 2006.

[4] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in Proc. 1st Int. Conf. Embedded Networked Sensor Systems (SenSys), 2003.

[5] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in Proc. ACM Conf. Computer and Communications Security (CCS), 2006.

[6] K. B. Frikken and J. A. Dougherty, "An efficient integrity-preserving scheme for hierarchical sensor aggregation," in Proc. 1st ACM Conf. Wireless Network Security (WiSec), 2008.

[7] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A secure hop-by-hop data aggregation protocol for sensor networks," in Proc. Seventh ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), 2006.

[8] S. Nath, H. Yu, and H. Chan, "Secure outsourced aggregation via one-way chains," in Proc. 35th SIGMOD Int. Conf. Management of Data, 2009.

[9] L. Hu and D. Evans, "Secure aggregation for wireless networks," in Proc. Workshop Security and Assurance in Ad hoc Networks, 2003.

[10] H. Yu, "Secure and highly-available aggregation queries in large-scale sensor networks via set sampling," in Proc. Int. Conf. Information Processing in Sensor Networks, 2009.