International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Volume 11, Issue 01)
Publishing Month: January 2015
An Indexed and Referred Journal
ISSN: 2347-601X
www.ijemhs.com

Secure Congestion Control Algorithm

Monika[1] and Jitendra Kumar[2]
[1,2]Royal Institute of Management and Technology, Chidana, Haryana (India)

Abstract
Mobile Ad-hoc Network is an Infrastructure less and decentralized network. The wireless nodes in MANET can communicate with each other through a direct wireless link. This paper propose a secure congestion control algorithm that uses Data Encryption Standard (DES) in MANET which sends the encrypted data from source node to destination node by using congestion controlled path and decrypt the data at the destination node. So in this paper we are trying to identify the best routing algorithm which will improve the congestion control mechanism among all the multipath routing protocols.
Keyword: *DES, Congestion, MANET*

1. Introduction

The major issue in MANETs is congestion control with security. In MANETs, any active node can be communicated with any other active node using intermediate node[1]. An important objective of this algorithm is to send secure data from valid source to valid destination without congestion. Maintaining and allocating network resources effectively and fairly among a collection of users is a major issue. The resources shared mostly are the bandwidth of the links and the queues on the routers. Packets are queued in these queues awaiting transmission. When too many packets are contending for the identical link, the queue overflows and packets have to be dropped. When such drops become general events, the network is said to be congested. In ad-hoc networks, since there is no fixed infrastructure there are no separate network elements called routers and hence the mobile nodes themselves act as the routers. The source is informed about the congestion in the network so that either it may slow down the packet transmission rate or find an alternate route which may not necessarily be an optimal route. It must be pointed out that all the congestion control methods are able to inform the source about the congestion problem because they use Transmission Control Protocol (TCP) [2] [4] [5].

2. Congestion control with Security Algorithm

Various Assumption are as follow: Source nodes and destination nodes are selected using random function. The Key is generated at each node using random function. Data at source nodes and destination nodes are encrypted and decrypted by using DES algorithm.

Proposed Algorithm

Step 1: Generate random nodes for simulation
Step 2: Select different source nodes & destination nodes.
Step 3: Generate the KEY at each node.
Step 4: Encrypt the KEY at each node using DES algorithm.
Step 5: Find the shortest paths from each source node to destination node.
Step 6: Repeat step 7 until all paths from source nodes to destination nodes are congestion free.
Step 7: If congestion occurs at any node i due to path pj from source node sk to destination node dk and path pj+1 from source node sl to destination node dl, then choose next alternate path for pj+1 from sl to dl.
Step 8: Repeat step 9 until all the data is transmitted to all destination nodes.
Step 9: Decrypt the KEY using DES algorithm.
Step 10: If Key matches for dj, then destination node found for sj.

3. Results & Analysis

We proposed a technique to solve the secure congestion problem in MANET using DES algorithm

for providing security in congestion control in MANET. Different parameters like Total Packet, Received Packets, Drop Packets Packet Delivery Ratio (PDR), Delay Time are considered with respect to different scenarios for checking the effectiveness of our work. Here, Total Packet means the total number of packets gets transmitted from source node to destination node. Total Packets depends upon congestion. As the congestion increases, Total Packets also increases. Packet Delivery Ratio means the total number of successfully delivered packets by the network. PDR depends upon received packet and drop packet. When the no. of packets transmitted on the network is greater than the handling capacity of network, network becomes congested due to which packet drop occurs. As packet drop increases, PDR decreases and vice versa. Delay time is an important design and performance characteristics of MANETs. The delay of the network specifies how long it takes for a bit of data to travel across the network from source node to destination node. We performed a number of simulation runs for the different number of scenarios.

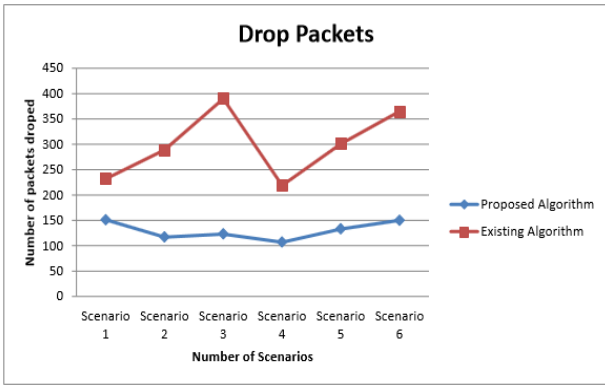

Figure 1: Packet Drop Comparison

Graph in figure 1 shows the comparison of drop packets in our network and previous network. In our network, drop packet is reduces because no. of received packets are increased.

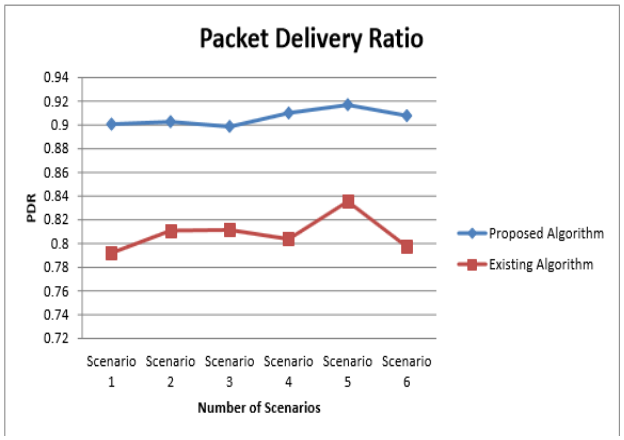

Figure 2: Comparison of PDR

Graph in figure 2 shows the Packet Delivery Ratio is increased in our network because it specifies the ratio of successfully packet delivered from source nodes to destination nodes. In our network, every time Packets gets delivered from congestion free path with secure key, thereby less chance of congestion at intermediate node to occur and packet are transmitted safely without any drop and less chance of loss of packet at destination node. So PDR increased in our network which shows that our work is more effective than previous network.

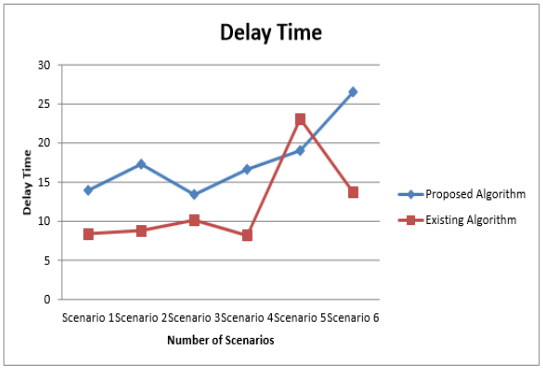

Figure 3: Comparison of Delay

Graph in Figure 3 shows the delay time of proposed algorithm is increased as compared to the existing algorithm when no congestion occurs. Delay time of the proposed algorithm is less or same as compared

to the existing algorithm when congestion occurs at any node in the network. From the above table 6.5 and 6.6 for node 30, total received packets are increases in proposed algorithm as compared to the existing algorithm, total drop packets are decreases in proposed algorithm as compared to the existing algorithm. So packet delivery ratio is also increases in proposed algorithm. Total delay time is increases in proposed algorithm because proposed algorithm adds the security in the existing algorithm.

4. Conclusion and Future Work

In this paper, we define the problem of secure data delivery in mobile ad-hoc networks. We propose a secure congestion control algorithm in MANET which sends the encrypted data from source node to destination node by using congestion controlled path and decrypt the data at the destination node. Destination node decrypts the data into original form, if it has a valid key through which received data is decrypted. To inhibit the data misuse and loss of data, we have implemented the security using symmetric technique. The encryption and decryption are used for the security in congestion control mechanism. In this proposed work, we use the DES encryption system for the encrypting of the data to be sent. Then, choose the path between source and destination with the use of congestion control mechanism and data are sent to the destination nodes via intermediate node. Finally, we use the DES decryption system for the decryption of the received data. After implementing the proposed algorithm, we analyze the delay time and throughput. Average delay time of congestion control with security is decreased as compared to the congestion control without security and Throughput of congestion control with security is increased as compared to congestion control without security. According to the performance analysis, the proposed work is more efficient because it provides security, reduces the delay time and increases the throughput.

References

[1] S.Sudha, V.Madhu Viswanatham et al. "Implementation of Enhanced Data Encryption Standard on MANET with less energy consumption through limited computation" In Proceeding of International Journal of Engineering Research and Development eISSN : 2278-067X, pISSN : 2278-800X, www.ijerd.com Vol. 2, Issue 4, pp. 46-52 July 2012).

[2] Gulshan Kumar et al. "A Hybrid Approach for Providing Security in MANET", In Proceeding of International Journal Of Information Security Science, Vol.1, No. 3, 2011.

[3] Xiaoqin Chen, Haley M. Jones, A.D.S Jayalath, "Congestion Aware Routing Protocol for Mobile Ad-hoc Networks", Department of Information Engineering, National University, Canberra.41

[4] Raju Kumar, Riccardo Crepaldi, Hosam Rowaihy, Albert F. Harris III, Guohong Cao, Michele Zorzi, Thomas F. La Porta, "Mitigating Performance Degradation in Congested Sensor Networks.", IEEE Transactions on Mobile Computing, Vol. 7, No. 6, June 2008.

[5] MATLAB Manuals, "www.mathworks.com".