FLIO: FAILURE LINKS INTO OPTIMISTIC USING DIFFIE HELLMEN KEY ALGORITHM

J. Antony Daniel Rex[1]

[1]*M. Phil., Research scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), Salem (Tamil Nadu), India*

Abstract

In Mobile ad-hoc network (MANET) a node may transfer the data to the destination with the help of the cooperative node. A change in network topology may degrade the path of current data transfer, and then it causes the link failure. In this kind of routing, security and key organization are important and complex problem. This research work tries to give a solution for link failure by using Distributed Time Sequence Routing protocol (DTSR), the DTSR is used to locate the correct relay node and sink node for data transmission.

Keywords: *DSDV, Key Agreement, Link Failure, MANET, etc…*

---***---

1. INTRODUCTION

In mobile ad-hoc network, there is no need of any infrastructure network, Node can be move anywhere. So that MANET can be defined as an independent mobile node that communicates over wireless links without any infrastructure. Here every node at as a router it can transfer the data to source to distention Router only fixes how to forward packets to node. There are various routing protocols are been used to MANET .if the path node have stable link then the data will reach the distention, at the time of sending data if the node topology has been change, then link failure will accrue in MANET. The communication of each node has to known each other then only the failure will not accrue, for the intend they need key agreement for each node, it also give the vulnerable to the node and secure to the packets.

2. KEY AGREEMENT

In the proposed system Distributed Time Sequence Routing protocol (DTSR) is used to send the data efficiently and quickly on the network. DTSR protocol is used to transfer the data without any modification. Availability parameters are connectivity and functionality in the network organization layer. Loss is the fraction of packets lost in transit from sender to target during a specific time interval, expressed in percentages. The Proposed system aim is to improve the network throughput, Network delivery ratio, and availability and data loss. Consequently, the Diffie-Hellman algorithm is used with a form of authentication which uses the certificates to ensure that symmetric keys are established between nodes. The steering metrics are evaluated in dissimilar literatures to indicate the significance and measuring purpose of frequent routing protocols. A cryptographic key exchange method was developed by Whitfield Diffie and Martin Hellman in 1976. This method is called as “Diffie-Hellman-Merkle” method. Key distribution is an important aspect of conventional algorithm and the entire safety is dependent on the distribution of key using secured channel

Key exchange algorithm is:

Step1: GLOBAL PUBLIC ELEMENTS
Select any prime no.: ’q’ Calculate the Primitive root of q:’a’ such that a<q.

Step2: ASYMMETRIC KEY GENERATION BY USER ‘A’
Select a Random number as private key X_A where $X_A<q$. calculate the public key

Y_A where $Y_A = a^{X_A} \bmod q$.

Step3: KEY GENERATION BY USER ‘B’
Choose an arbitrary number as the private key X_B where $X_B< q$ Calculate the public Key Y_B where $Y_B = a^{X_B} \bmod q$.

Step4: Exchange the values of public key between A and B

Step5: SYMMETRIC KEY (K) GENERATION BY USER 'A’

$$K=Y_B^{X_A} \bmod q.$$

Step 6: SYMMETRIC KEY (K) GENERATION BY USER 'B'

$$K= Y_A^{X_B} \bmod q.$$

3. EXPERIMENTAL RESULT

3.1 Packet Delivery Ratio

Packet Delivery Ratio (PDR) is shown figure 1 and it has been calculated by dividing the number of packets received by the destination through the number of packets originated by the source.

$$\text{PDR} = \frac{\text{Total number of data delivered}}{\text{Total numbers of sending data}}$$

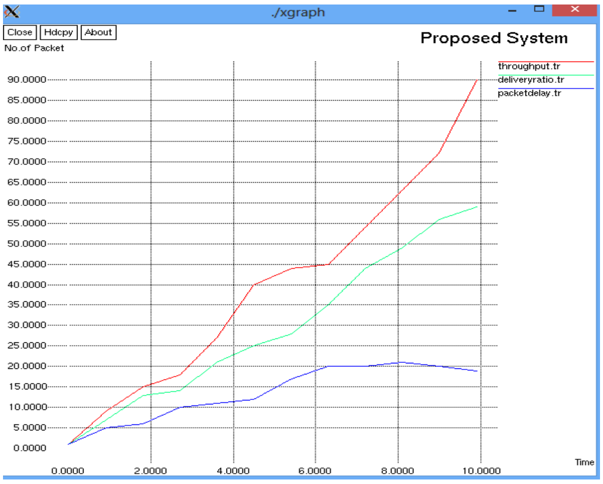

Fig 1: Proposed System

4. CONCLUSIONS

Most of the Link failure will be occurs in MANET by topology change, here this work Present the key distribution scheme, based on intrusion detection method for using a data transmission from source to destination on the network. It based high level security and more energy efficient data transmission on their network. Transfer the data form source to destinations within the node coverage area using Diffe Hellman key algorithm. In this algorithm is used to avoid the link failure and it also provide the secure to the packet transfer.

This work has used efficient Symmetric cryptographic primitives, called key authentication protocol with shared secret keys between communicating nodes on the ad-hoc network. It prevents Denial-of-Service attacks and modification of hop count attacks by malicious node.
In future, work may be conducted to improve the performance metrics of packet delivery ratio and control overhead of Secured DSDV by using efficient multi-hop route cache techniques.

REFERENCES

[1] Key Distributed Cryptography using Key Algorithm in MANET ISSN (Print) : 2319 – 2526, Volume-2, Issue-5, 2013, Rajesh Kumar Dangi, Rachna Singh Thakur

[2] An Algorithm for Improvement of Link Failure in Mobile Ad-Hoc Network Vibhor Kumar Goal* and Rishabh Shrivastava** and Vivek Malik* International Journal for Science and Emerging ISSN No. (Online):2250-3641Technologieswith Latest Trends” 10(1): 15-18 (2013)

[3] LSR Protocol Based On Nodes Potentiality in Trust and Residual Energy for ADHOC NETWORKs, Shaik Sahil Babu #1 , Arnab Raha #2 , M.K. Naskar #3 International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[4] “A survey on power aware routing protocols in mobile adhoc networks” by Dr.D.Vasumathi, N.Sainath, U.Moulali, B.Koteshwara Rao July-august 2012

[5] Identifying Trusted Routing Path in ADHOC NETWORKs through TARF, Journal of Advanced Technology in Engineering, Vol. 1, No. 1, December 2012. pp.37-41.

[6] Design and implementation of a Trust-aware routing protocol for large ADHOC NETWORKs, Theodore Zahariadis11 , Helen Leligou, Panagiotis Karkazis 5 , International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010

[7] Stallings, W., “Cryptography and Network security: Principles and Practices,” Fourth Edition, Pearson Education, 2006.

[8] A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge, published in Proceedings of the IEEE INFOCOM, March 7-11, 2004, Hong Kong. Pages 586-597.

[9] Chung and U. Roedig. “Poster Abstract: DHB-KEY – A Diffie-Hellman Key Distribution Protocol for Wireless SensorNetworks”, Adjunct Proceedings of the 5th IEEE EuropeanWorkshop on Wireless Sensor Networks (EWSN2008), Bologna,Italy, January 2008.

[10] DHB-KEY: An efficient key distribution scheme forwireless sensor networks, Infolab21, Lancaster Univ., Lancaster Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on

BIOGRAPHIE

J. Antony Daniel Rex, M. Phil., Research Scholar, Govt. Arts College, Salem – 636007. I have attended three National level Workshops, One National level Seminar and Published one Paper titled as “Routing Protocols in MANET” in National level Conference.