International Research Journal of Computer Science (IRJCS)
Issue 04, Volume 3 (April 2016)
ISSN: 2393-9842
www.irjcs.com

Effective Routing of Data Packets in Networks and implementing security

N. Swathi meena*
Department of CSE,
Kingston Engineering College
Vellore, Tamil Nadu

THEJASWINI. G
Department of CSE,
Kingston Engineering College.
Vellore, Tamil Nadu

Suganya.K
Department of CSE,
Kingston Engineering College
Vellore, Tamil Nadu

Abstract— Data routing in networks is the process of effectively routing a packets of data from a source node to a destination node. There are various problems which occur in the process of routing a data from a source node to a destination node. The data packet may be lost in the transition or it may not be transferred to the intended destination due to failure in the intermediate nodes. There is also another problem of the time duration involved in the process of transition. Generally the routing path should be chosen in such a way that the time taken to transfer the packets of data is less. This research works makes use of a protocol to effectively route the packets of data by identifying the shortest route to transport the packets of data. This shortest path is identified by the delay it takes to transport the data. Here also the data is securely transferred to the destination because of the use of Advanced Encryption standard. Thus there is a reduction in time for sending the data and confidentiality of the data is ensured by encryption and decryption.

Key words- Data routing, delay, Advanced Encryption Standard, encryption, decryption, Confidentiality.

I. INTRODUCTION

Data routing is a important method of routing a data from source to destination and it has got many application in networks. There are different protocols to route packets from source to destination like OSPF, RIP. There are protocols like TCP and Udp for transfer of packets TCP is a connection oriented protocol whereas UDP is connectionless. In this work the following is performed Every node while registering, server will provided with Id, primary key, secondary key and decryption key. Source will find out the optimum path and it will collect primary key of all intermediate node. Data's first encrypted using AES algorithm and then with corresponding primary key of all the hops. This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Then collecting its id and secondary key which is transmitted to both source and destination node. Same way all the id's and secondary key are collected and concatenated, so as to verify both source and destination. TPA implementation is also achieved for successful validation of concatenated keys their by reward is provided to the intermediate hops. The overall organization of the paper is as follows section II describes related work, section III outlines the work, section IV describes the experimental setup, section V presents the experimental evaluation, section VI concludes the work.

II. RELATED WORK

G . Shen et al. in their work, "hop relay for next generation wireless access network" reviews the key technical advances with multi-hop relay in cellular network novel technical solutions and algorithms for multi-hop relay are introduced and analyzed, including the separation of control and data, effective signal-to-interference-plus-noise ratio (SINR)-based routing algorithms, and cooperative relay schemes.

J.S. Baras et al. in their work, "On trust models and trust evaluation metric for adhoc network" interpret the concept of trust as a relation among entities that participate in various protocols. Trust relations are based on evidence created by the previous interactions of entities within a protocol. In this work, they were focusing on the evaluation of trust evidence in ad hoc networks.

Robert H.Peng et al. in their work, "Anonymous Secure Communication In Wireless Adhoc Network" define more strict requirements on the anonymity and security properties of the routing protocol, and notice that previous research works only provide Weak Location Privacy and Route Anonymity, and are vulnerable to specific attacks. Therefore, they propose the Anonymous Secure Routing (ASR) protocol that can provide additional properties on anonymity

III. SYSTEM DESIGN

A. Architecture Diagram description
This module consists of functionalities like accepting constructing network, route request, route selection, packet forwarding, decryption and TPA verification.

Steps:

- *Network Construction*
- *Route Request Based On Routing Table Checking*
- *Route Selection And Source Side Encryption Process*
- *Packet Forwarding*
- *Decryption Process*
- *TPA Verification And Payment Process*

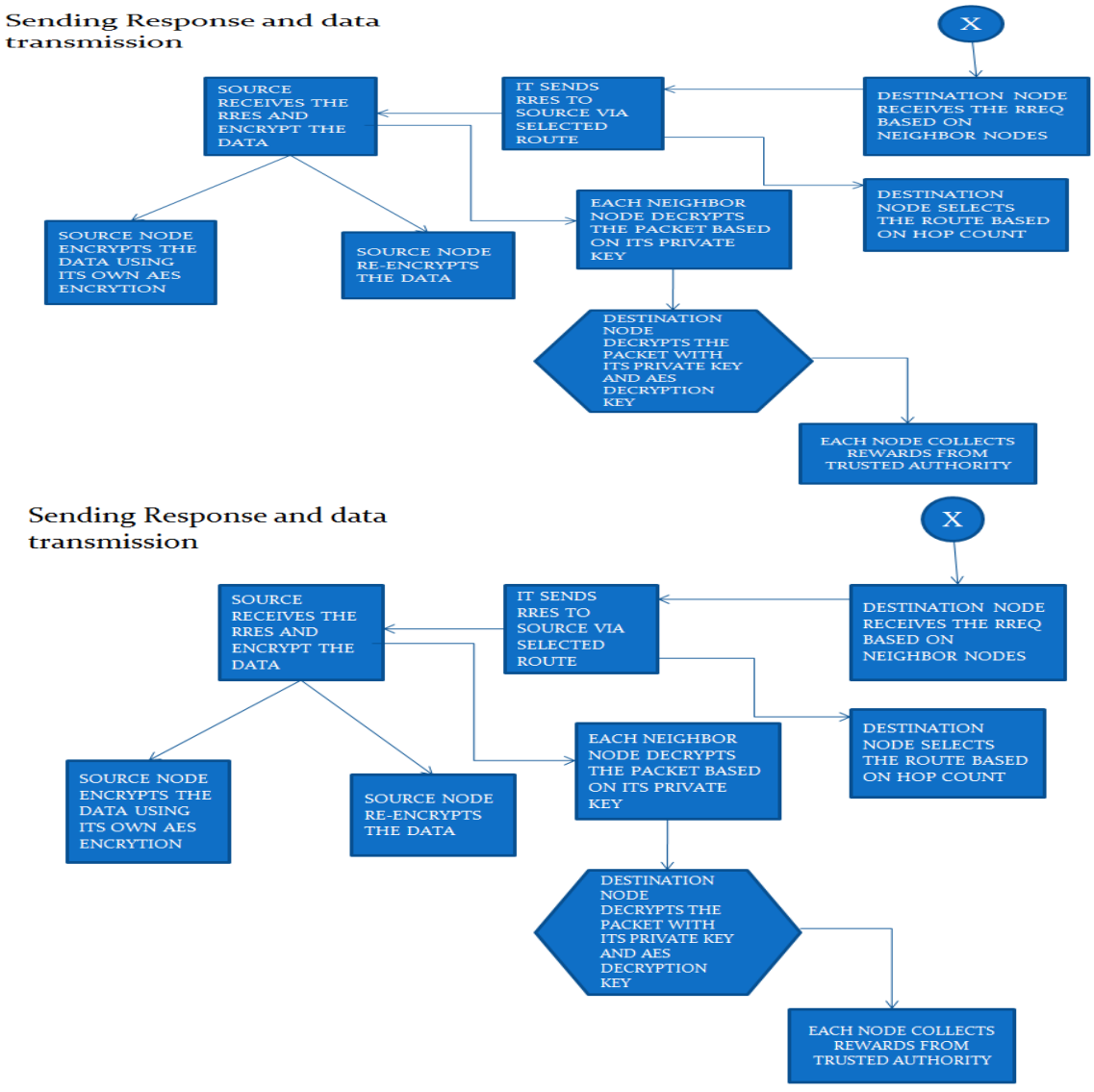

Fig. 1 Overall architecture.

1. NETWORK CONSTRUCTION

In this Project concept, first we have to construct a network which consists of 'n' number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, we can assume that the nodes are moving across the network. Network is used to store all the Nodes information like Node Id and other information. Each node is having primary key, secondary key and private key. Also network will monitor all the Nodes Communication for security purpose.

2. ROUTE REQUEST BASED ON ROUTING TABLE CHECKING

In this module, source node sends hello interval request to all intermediate nodes for identifying minimum hop count, capacity of intermediate nodes, based on node connectivity. It can use the routing table in the RREQ packet to estimate how many its neighbors have not been covered by the RREQ packet from previous intermediate node. Each intermediate node validates the RREQ packet and updates its routing tables. Finally RREQ reaches to destination node.

3. ROUTE SELECTION AND SOURCE SIDE ENCRYPTION PROCESS

In this module, the RREQ is received and verified by the destination node. The destination node selects the route based on hop count and throughput. Then the destination node assembles an RREP packet and broadcasts it back to the source node. Each intermediate node validates the RRES packet and updates its routing tables. After route selection, source encrypts the data based on AES encryption and it collects the selected neighbor nodes public key from routing table. Although source conducts the encryption process based on selected route public keys using AASR protocol based on onion routing.

4. PACKET FORWARDING

In this module, source node forwards the encrypted packet to neighbor node based on selected route. Neighbor node gives it own private key for one part of decryption process. After that it will send to next neighbor node. Similarly each neighbor nodes in selected route decrypts the packet based on its private key using AASR protocol. Some time attacker node also receives the packets. In that time, it gives its private key but packet is not decrypted. So it didn't analyzes how many number of encryptions placed on. Thus we improve the data security.

5. DECRYPTION PROCESS

In this module, neighbor node decrypts the packet and finally sends to destination node. Then the destination node decrypts the packet with its private key and AES decryption key. Finally destination node views the original data. Since the paths capacity will vary dynamically, so that the paths will be changed dynamically as per data transfer along the network. So it increases the packet delivery ratio and decreases the average end-to-end delay.

6. TPA VERIFICATION AND PAYMENT PROCESS

In this module, after data transmission each intermediate node in selected path sends its id and secondary key to trusted party auditor. Destination node also sends the id and secondary keys of selected nodes to TPA after data retrieval from source node. Then TPA audits the both id and secondary keys are match or not based on ESTAR protocol. If match means TPA rewards to that trusted node. Suppose it mismatch it easily identify the attacker node.

IV. EXPERIMENTAL SETUP

Here the nodes are constructed as the first step, then a network model is constructed and then when a packet of data is to be forwarded the destination node is identified and the data is encrypted by a encryption key before it is sent. This encryption process will be done by the AES algorithm. Then delay for each route is computed and the route which has a minimum delay is found and packets will be routed to that path. The destination node will be notified when a data is received. Then that destination node needs to provide the decryption key inorder to decrypt the file. The node creation and the routing are done in java. The maintenance of the nodes and the routing tables is done by a SQL server.

V. EXPERIMENTAL EVALUATION

The following experiments were carried out and the results obtained shows that this method provides a best routing mechanism and there is usage of weights in-terms of cost for a node for transferring the packets it receives rewards.

TABLE I
NODE ROUTING DETAILS

START NODE	DESTINATION ROUTE	ROUTES	COST
N 0	N3	N0-> N1->N3	10
N0	N3	N0->N2->N3	5
N1	N4	N1->N2->N4	6
N1	N4	N1->N3->N4	8
N5	N9	N5->N7->N9	10
N5	N9``	N5->N8->N9	12

TABLE II
ENCRYPTION KEYS AND HASH VALUES FOR NODES

NODE ID	HASH VALUE	ENCRYPTION KEY
N0	4	45
N1	6	56
N2	7	67
N3	4	53
N4	5	16
N5	2	72

TABLE III
BEST ROUTE FOR TRANSFER

START NODE	DESTINATION NODE	BEST ROUTE
N 0	N3	N0-> N1->N3
N1	N4	N1->N2->N4
N5	N9	N5->N7->N9

VI. CONCLUSION AND FUTURE WORK

Thus a secured and effective routing is performed by the usage of these mechanisms namely, Network Construction, Route Request Based On Routing Table Checking, Route Selection And Source Side Encryption Process, Packet Forwarding, Decryption Process, TPA Verification And Payment Process. Further enhancement can be done in a varied usage of this encryption and decryption algorithm and the performance may be computed.

REFERENCES

[1]. Mohamed M.E.A. Mahmoud, Xiaodong Lin, "Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015.
[2]. C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.
[3]. K. Liu, J. Deng, and K. Balakrishnan, "An AcknowledgementBased Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536- 550, May 2007.
[4]. M. Mahmoud and X. Shen, "PIS: A Practical Incentive System For Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010
[5]. M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.
[6]. P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model," IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172- 185, Sept. 2010.
[7]. D. Johnson, D. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," Ad Hoc Networking, C. Perkins, ed., chapter 5, pp. 139-172, AddisonWesley, 2001.
[8]. A. Withby, A. Jøsang, and J. Indulska, "Filtering Out Unfair Ratings in Bayesian Reputation Systems," The Icfain J. Management Research, vol. 4, no. 2, pp. 48-64, 2005.
[9]. A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.
[10]. P. Resnick and R. Zeckhauser, "Trust among Strangers in Internet Transactions: Empirical Analysis of Ebay's Reputation System," Proc. NBER Workshop Empirical Studies of Electronic Commerce, 2000
[11]. A. Withby, A. Jøsang, and J. Indulska, "Filtering Out Unfair Ratings in Bayesian Reputation Systems," The Icfain J. Management Research, vol. 4, no. 2, pp. 48-64, 2005.