Secure Inter Hop Verification with Onion Protocol Implementation for Reliable Routing In Wireless Networks

Nagarajan Ravi [#1], Jeyanthi. P [*2]
[#] Department of Information Technology, Sathyabama University,
Chennai, Tamil Nadu, India
[1] nagarajanravim@gmail.com

***Abstract*— Mobile Adhoc Network provides a new challenges and difficulty when nodes are used in large network with maximum number of nodes and the reason of limited bandwidth and dynamic topology establish a good routes from nodes and maintaining that routes is a very hard. To achieve the security in Mobile Adhoc Network (MANET) is very difficult because of changing topology, wireless links vulnerability, and more management point. In this proposed system we proposed onion protocol with Advanced Encryption Standard (AES) algorithm and multi-hop route forwarding algorithm. In the proposed we propose an onion routing networks using a new protocol. We describe a new secure and reliable packet sending scheme using the onion routing with Advanced Encryption Standard (AES) algorithm. When node comes to registering in network, it will get the primary key, secondary key, node id. Once source identified shortest path to destination node, it will get primary key of all nodes in the shortest path. This onion protocol with Advanced Encryption Standard technique is used to secure the data from other nodes in the network and provide the reliable packet delivery to destination. In this proposed system we use multi-hop Route forwarding algorithm technique to provide efficient shortest path from source node to destination node. It achieves shortest path identification by test of request and response process. In the proposed system all intermediate nodes not only doing packet forwarding and it is responsible for decrypting the packet using that secondary key. Secure and reliable packet delivery is achieved in this system by onion routing with Advanced Encryption Standard algorithm and multi-hop route forwarding algorithm**

Keyword- MANET, Route discovery, Onion protocol, Data forwarding

I. INTRODUCTION

Basically MANET is mobile nodes collection, which communicates with other nodes by broadcasting. In Mobile adhoc networks, they do not have any central administration and existing infrastructure [1]. Therefore, the Mobile Adhoc Network (MANET) is using a temporary network communication. Mobile Adhoc Network (MANET) is working without infrastructure, so nodes in wireless network dynamically form their own network and connection on the flying movement. In wireless communication all nodes can listen to the communication if it is in sending range [2]. These wireless network nodes use some default routing protocols to identify the sender and receiver for every message. In wireless mobile adhoc network security is a major issue, particularly in military application. Now days this problem is going serious over the node mobility. Already various approaches have proposed to handle this security problem [3]. But now there is no routing algorithm is suitable for the environments. Over some years, more number of networks has been proposed with onion routing technique and some networks have been implemented. Onion routing [4], is a technique where message are covered in multiple encryption layers, forming an encryption like onion. In this scheme delivering message to destination by a no of intermediate onion nodes or routers, each intermediate router and node is responsible to decrypt one layer, and forward the packet or message to next router or node. A common process of an onion routing scheme is classify a collection of nodes that relay users of the system traffic. Users of this scheme then randomly select a path over the onion routers network and form a circuit, a sequence of nodes which will route traffic. After formed the circuit, each nodes in the circuit shares symmetric to user, that key will be used to encrypt future onion layers. In this proposed system we present onion routing protocol and Advanced Encryption technique. In that First network is constructed with n no of nodes [6]. After that nodes in the network can request data packet to other nodes. We can simulate nodes in the networks are moving because of the nodes mobility property. All nodes are maintained to forward data packet to other nodes. In this proposed scheme, discovering the shortest path is first process, and sends the packets to other node. When nodes come for registering into to the network, they get id and other information [7]. In this multi hop route forwarding is used to identify shortest path detection and Advanced Encryption Standard algorithm is used to achieve encryption process. Data is encrypted using Advanced Encryption Standard (AES) technique with primary key of all intermediate nodes. The wholesome is forwarded to first node, where the first decryption will be done by that node decryption key. In this proposed system, source node transmits the encrypted data packet to intermediate

node depending on the selected route. Then intermediate nodes decrypt and transmit packet to destination node. Finally destination nodes get data securely by its last decryption process [8]. Using this system we achieve the data forwarding securely and shortest way. This system mainly overcomes the problems of Existing Electronic Suspense Tracking and Routing (ESTAR) system, which ensure route stability, malicious, selfish attacks, and node failure. This proposed system use new protocol with encryption for packet delivery speed and most secure data forwarding

II. RELATED WORKS

Normally nodes in the multi-hop wireless networks would like to communicate with other nodes in networks; so it can transmit the packet by the help of other nodes in the network. This type of multi hop packet transmission is able to extend the network coverage area by spectral efficiency of area and limited power [9]. This multi hop networks can be used in rural and developing areas at low cost in is more readily available. When consider the multi hop wireless civilian networks, nodes in network contains the long connection with network. In heterogeneous multi hop wireless networks, nodes hardware resources and level of nodes mobility may greatly vary. Heterogeneous multi hop wireless networks can be used in many applications like multimedia data transmission and data sharing. For ex, users in one particular area (college, university campus, etc) having various wireless enabled devices (laptops, cell phones, tablets, etc.) can create a network to distribute files, information sharing, and communication. In military and some disaster-recovery applications, behaviour of the node predictable because such type network is maintain by one authority and that network is closed [10]. For various reasons Sometimes behaviours of node is unpredictable in the application of civilians. The nodes may be self-interested and autonomous and it belongs to different authority. The nodes have different energy capabilities and hardware and may have various goals. Malfunctioned and selfish node is the addition problem in mobile network. Because of malfunctioned nodes drop the packets frequently and break the routes due to the software and hardware problems and this type nodes disrupts the transmission of data. Since mobile nodes are running in battery driven, some nodes are not interest to transmit the packets to save their energy [11]. When many nodes are in cooperative mode to relay the packets, the routers will be short, and network connectivity, network partition possibility is lower. Moreover nodes in the network have equipped with different hardware quality, such as buffer size and CPU speed, the nodes whose having more hardware resources can easily perform packet transmission more successfully when compared to other nodes. For example, Professional Development Awards (PDA) could not be transmitting the packet effectively because of the resources scarcity. In HMWNs, nodes are not able to transmit the packet to other effectively due to nodes moving from transmission range to neighbor transmission range [12]. Due to this nodes uncertainty behaviour, dynamic routes will degrade stability of routes. It is also one of the reasons to endanger the data transmission reliability and degrade the performance of network. In wireless network one node could be a reason to break route, and some selfish or malicious nodes can break the routes repeatedly. If any route is broken when transmitting the packet to other nodes, the node has to retransmit the packet and identify the new route. These types of route discoveries may bring network wide flooding of routing request that takes a more amount of network resources [13]. Route breaking increases the delivery latency of packet and may reason communication fail in multi-hop. In order to create stable route to transmit packet and maintain the traffic flow, considering the nodes ability and reliability takes places to create informed routing decisions. In existing system Electronic Suspense Tracking and Routing System (E-STAR) protocol is used to establish a reliable and stable routes in Heterogeneous multi hop wireless networks. Electronic Suspense Tracking and Routing System (E-STAR) combines payment and trust systems with an energy-aware and trust-based routing protocol. In this payment system it uses the credits to charge nodes that transmit packets and give reward to those nodes relaying packets. An offline trusted party (TP) takes responsible to manage the credits accounts of nodes because sometimes the trusted not involved in communication sessions. The nodes which are participating in packet relaying compose proofs, its called receipts, and submit that request to Trusted Party. The payment systems used to identify the selfish nodes and it helps other nodes to identify selfish node and earn credits [14]. It can give fairness by nodes rewarding system that helps other nodes to relay packets in the network. However, this payment system will not sufficiently ensure the stability of route. In the proposed system it use stimulate method for nodes to avoid the route break to earn credits, but due to some other reasons routes could be broken. Example of some reasons includes node failure, low resources, and selfish attacks. To overcome these issues we use onion routing protocol with Advanced Encryption Standard and multi hop routing algorithm. This proposed system provides reliable and secure packet forwarding mechanism

III. PROPOSED WORK

A. *Secure and reliable data forwarding using onion protocol*

This paper proposes onion routing protocol with Advanced Encryption Standard and multi hop route forward algorithm to overcome the existing problems. This system provides a very securable and fast packet transmission in multi hop wireless adhoc network. It provides the reliable and secured packet delivery. In this proposed system based on request response scheme, source selects the path from source to destination node. When ever node registering into the network, it will get node id, primary key, and secondary key. These primary keys and secondary keys are used for encrypting and decrypting the data packets. Once Source discovers the destination, it starts to find shortest path to forward packets. This system uses the multi hop route forwarding algorithm to find the shortest path. After finding shortest path Source collect the primary keys of all intermediate nodes and encrypt the data using that primary keys. This wholesome is forwarded to first node, where first decryption is started using that secondary key. Like that all the intermediate nodes are decrypted. Finally source will get secured and reliable data.

B. *Node Construction with Communication*

In this proposed system, first we need to construct the network with n number of nodes. After that nodes can forward data from one to other node in that network. Nodes in the network are moving, because it's having the mobility property.

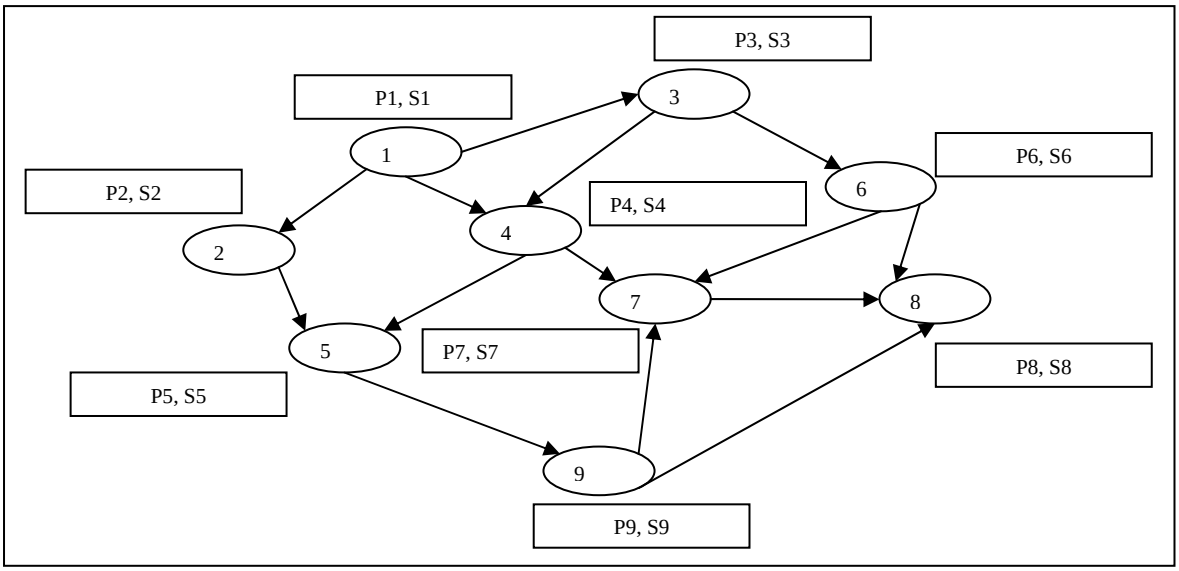

Fig1 Network Construction

The Above Figure 1 shows, each node in the networks gets node id, primary and secondary key once nodes enter into the network. Nodes primary and secondary keys are used to encryption and decryption operation.

C. *Route Discovery*

MANET is a collection of mobile devices with wireless connectivity. It has no fixed infrastructure, restricted resources and broadcast range. Communication between the nodes is achieved by the dynamically discovered routes, using that routes nodes can transmit the packets with help of some other nodes. But identifying the routes between nodes is major task. The security and efficiency is an important concern while forwarding the packet. This proposed system uses the multi hop route forwarding algorithm to discover the shortest path from source to destination. After finding routes between source and destination, Source sends packet to destination.

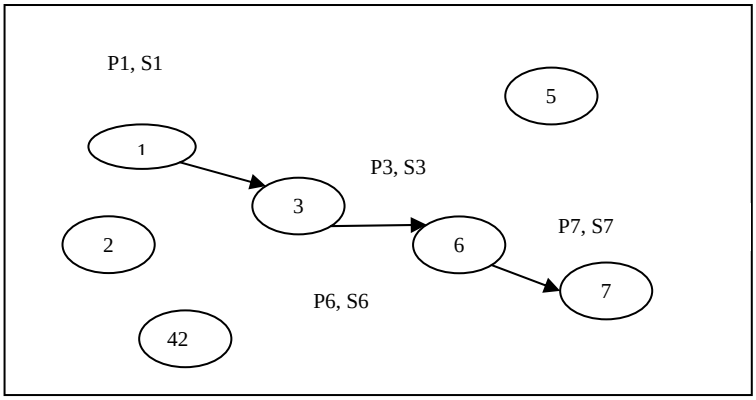

Fig 2 Shortest Route Discoveries from Source to Destination

D. *Onion Protocol Technique with Trusted Authority*

This protocol is used to provide security on data by some layer of encryption, and it overcomes the packet delay latency. Once the shortest path is discovered successfully from source to destination, Source node collects primary key of all intermediate nodes. Then source node start the first encryption process by the destination node primary key. Respectively, the encryption process is done by all intermediate nodes primary keys. Source node forwards the encrypted packet to neighbor or intermediate node based on selected route. Neighbor node provides secondary key for decryption process and decrypt the data. After that the neighbor node forwards the data packet to next intermediate node. Like that all the neighbor nodes in the selected route are decrypted by its secondary key. Finally destination nodes receive the secured and reliable data packet by its decryption process.

E. *Overall Architecture*

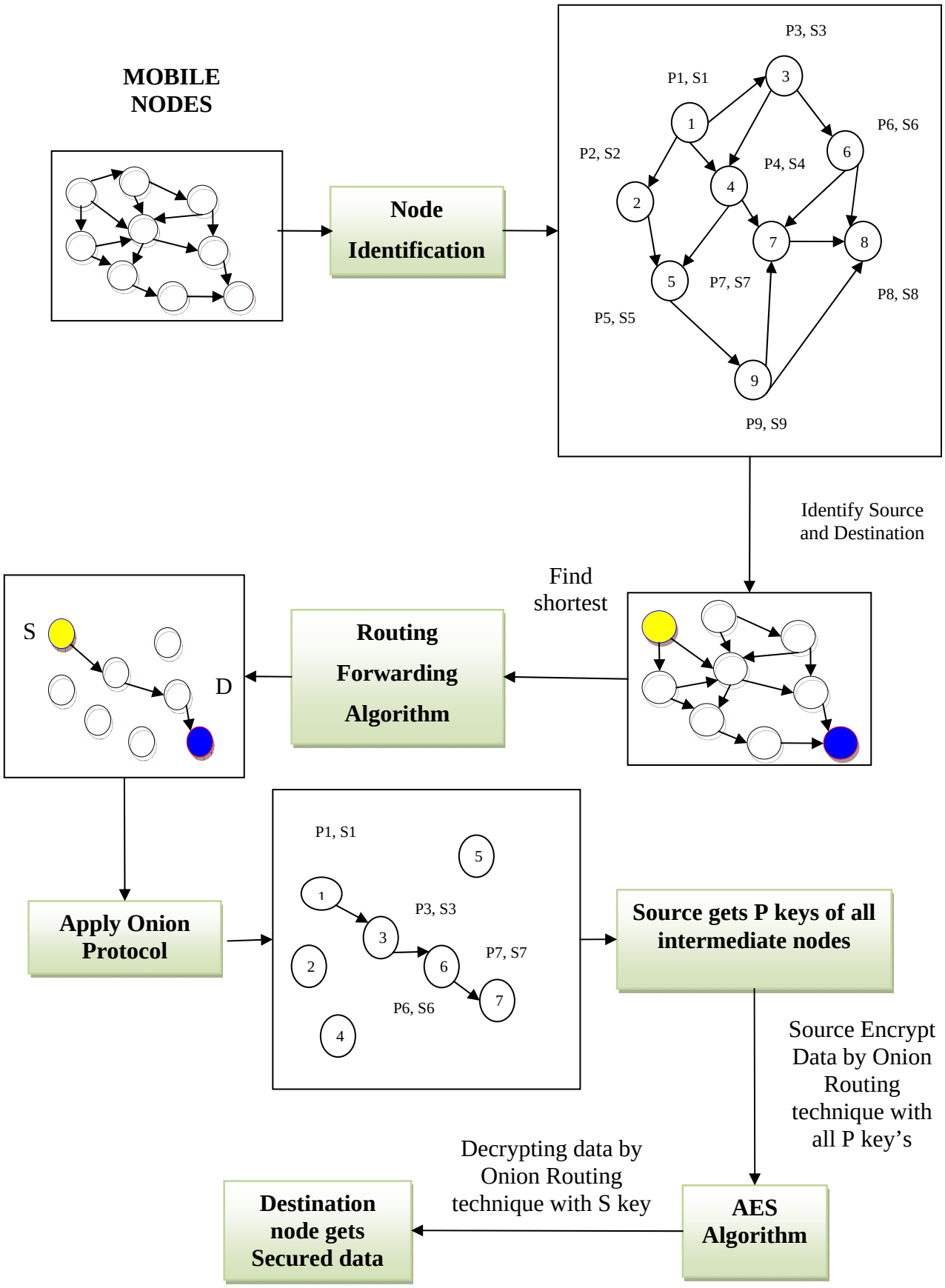

Fig 3 Reliable Packet Sending Using Onion Protocol

IV. RESULT AND DISCUSSION

This paper proposes Advanced Encryption Standard with onion protocol to overcome the issues of Electronic Suspense Tracking and Routing (E-STAR) protocol, and we use multi hop route forward algorithm to select the shortest path from source to destination.

A. *Network Constructions with N Nodes*

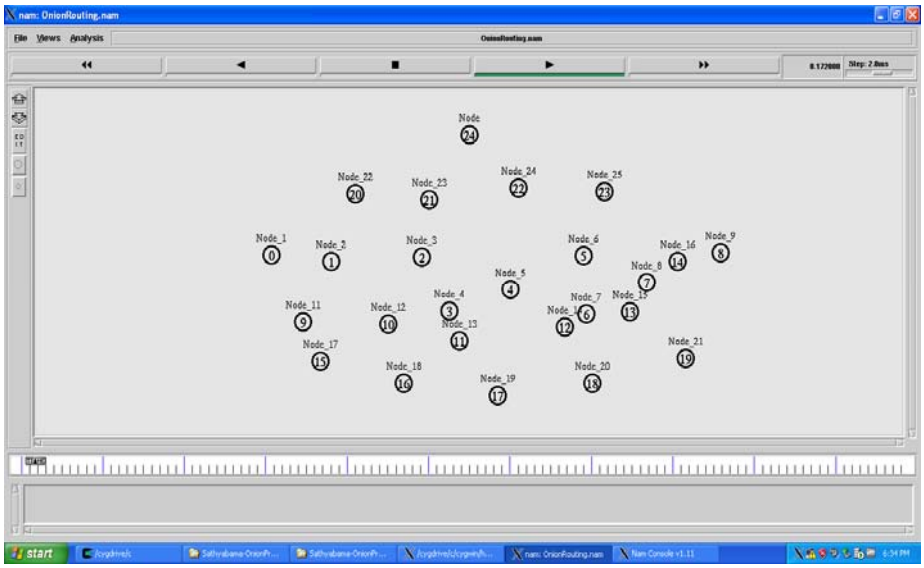

Fig 4 Network Constructions with N Nodes

The First process of this paper is constructing the network with n number of nodes. The above Figure 4 shows the network construction with n number of nodes. Constructing the network is used to relay the data packet from one node to other node in the network.

B. *Providing Id, Primary and secondary key to nodes*

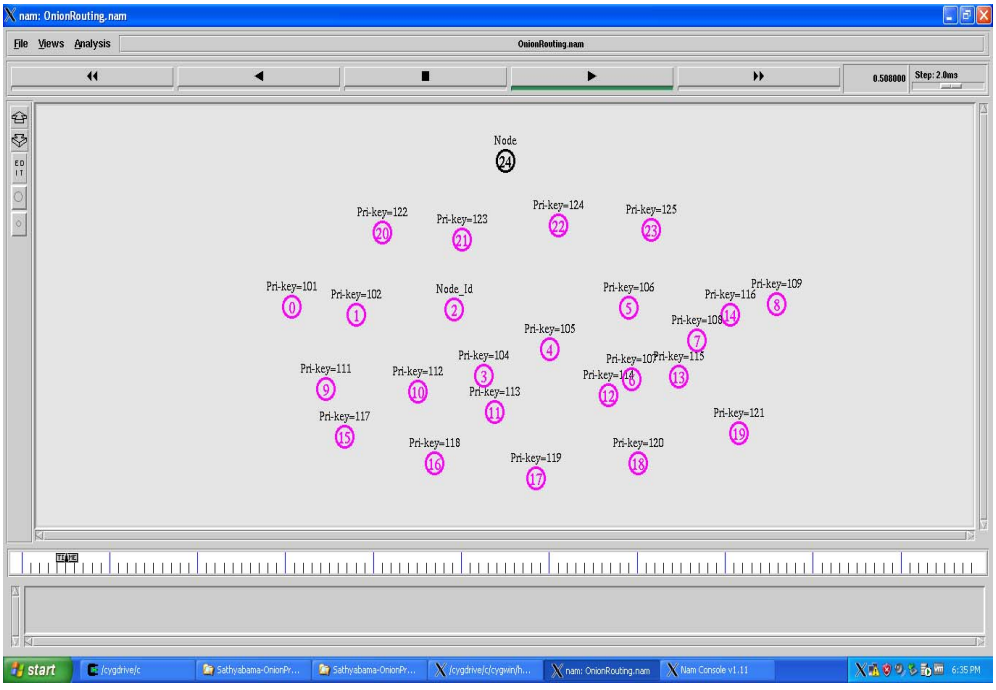

Fig 5 Providing Id, Primary and secondary key to nodes

The above Figure 5 shows the process of nodes getting its node id, primary and secondary key. These two key are used to perform the encryption and decryption operation on data packet. In the proposed system multi hop route forwarding algorithm is used to find the shortest path from source to destination. Finding the route is important to forward the packet from one node to another. In existing system Electronic Suspense Tracking and Routing (E-STAR) protocol is used to transmit the packet with secure and reliable way. It used the reward and

payment system for reliable packet transmission. But in our proposed system it use the layer of encryption using the onion routing protocol to transmit the packet secure and reliably.

C. *Request Sending To Destination Node*

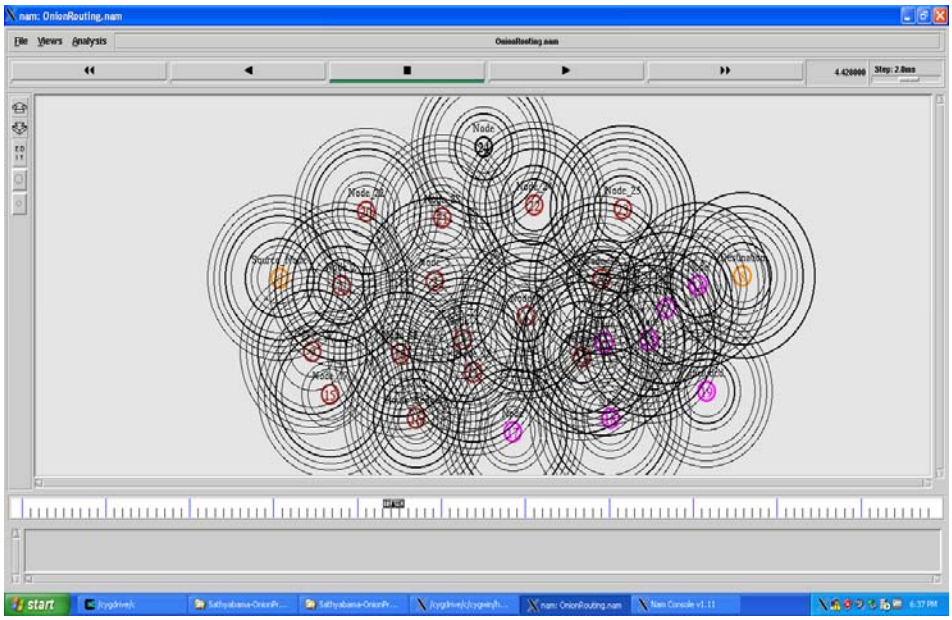

Fig 6 Requests Sending To Destination Node

The Figure 6 shows the process of request sending from source to destination node to find the shortest path. Once source node decides the destination node, source wants to find the shortest path to forward the packet. Here we use the multi hop route forwarding algorithm to find the shortest path in the network.

D. *Packet reaching time from source to destination*

Table 1 Packet reaching time from source to destination

No. Of Nodes	E-STAR	Onion Protocol
10	30.984	10.967
20	40.125	20.963
30	60.324	40.734
40	110.871	90.576

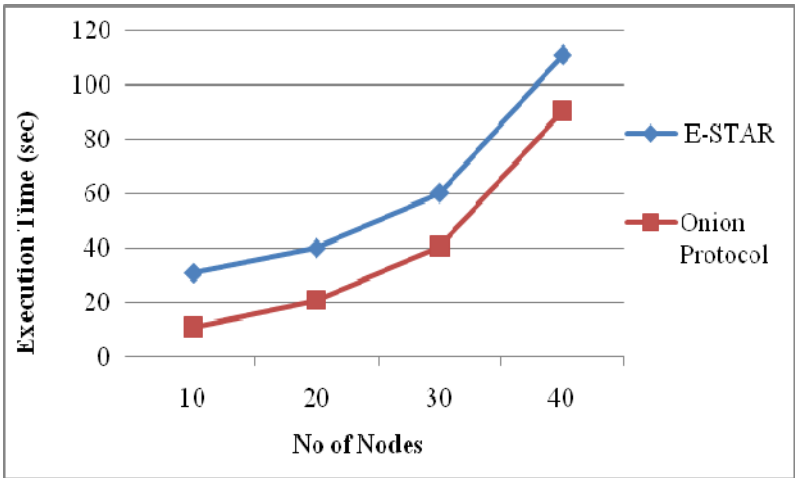

Fig7 Packet reaching time from source to destination

The above figure shows the node execution time from source node to destination node. When compared to existing system our proposed system minimize time for nodes to reach the destination. This system also support, if no of nodes increases in intermediate path in network, it will reach the destination more quickly than existing system.

V. CONCLUSION

In existing system Electronic Suspense Tracking and Routing (E-STAR) is used for establishing the reliable and stable routes for mobile adhoc network. It uses the trust/payment system with trust based and energy aware routing protocol for stable routes. It penalizes the nodes that report the false information by decreasing the chance of that node to be selected by routing protocol in future. In proposed system we use onion routing protocol for secure and reliable packet transmission. Onion protocol provides the layer of encryption and decryption process to secure the packet while transmitting to destination node and this system uses the multi hop route forwarding algorithm to find the shortest path from source to destination. Onion protocol with Advanced Encryption Standard algorithm is a two key encryption process. In this source the encrypted data with primary keys and each neighbor node is responsible for decrypting the packet with its secondary key, so any neighbor node in the selected route can not access the data while transmitting the packet to other neighbor node. When compared to the existing system our proposed system provides more security on data and minimizes the overhead of network.

REFERENCES

[1] David A. Maltz, Josh Broch, Yih-Chun Hu, Jorjeta Jetcheva and David B. Johnson, (1998), "A performance comparison of multihop wireless ad hoc network routing protocols. Proceedings of the 4th Annual IEEE / ACM International Conference on Mobile Computing and Networking (MobiCom'98), pages 85.97

[2] Ismail, D, Jaafar, M, (2007), "Mobile ad hoc network overview", Applied Electromagnetics, Asia-Pacific Conference, IEEE , Page 1 - 8 DOI 10.1109/APACE.2007.4603864

[3] Potdar,V. Sharif, A. ; Chang, E. (2009), "Wireless Sensor Networks: A Survey", Advanced Information Networking and Applications Workshops. International Conference IEEE, Page(s):636 – 641, DOI:10.1109/WAINA.2009.192

[4] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, (2009), "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical Journal, vol. 13, no. 4, pp. 175-193.

[5] C. Chou, D. Wei, C. Kuo, and K. Naik, (2007), "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE Journal On Selected Areas In Communications, VOL. 25, NO 1.

[6] Volker Fusenig, Dagmara Spiewak; Engel, T. (2007), "Acimn protocol: A protocol for Anonymous Communication In Multi hop wireless Networks" Wireless Telecommunications Symposium, Pomona, CA, IEEE , DOI: 10.1109/WTS.2007.4563320.

[7] Vasantha, V. , Manimegalai, D., (2007), "Mitigating Routing Misbehaviors Using Subjective Trust Model in Mobile Ad Hoc Networks" Conference on Computational Intelligence and Multimedia Applications International Conference IEEE (Volume:4) Pp. 417 - 422

[8] X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, (2012), "Autoregressive Trust Management in Wireless Ad Hoc Networks," Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3, pp. 229-242

[9] Charles E. Perkins, (2001) "Ad Hoc Networking". Addison-Wesley, ISBN 0-201-30976-9.

[10] Mesut Güne¸s, Otto Spaniol, "Routing Algorithms for Mobile Multi-Hop Ad-Hoc Networks" International Workshop NGNT.

[11] Ritu Aggarwal, (2013) "Security on Dynamic Source Routing Protocol Using Onion Routing Encryption", International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Volume-2, Issue-6

[12] G. Indirania and K. Selvakumara, (2014), "A Swarm-Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)," Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103..

[13] H. Li and M. Singhal, (2007), "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53.

[14] Aniket Kate Greg M. Zaverucha Ian Goldberg David R. Cheriton, (2010)"Pairing-Based Onion Routing with Improved Forward Secrecy" ACM Transactions on Information and System Security (TISSEC) Volume 13 Issue 4.

AUTHOR PROFILE

Nagarajan Ravi received the B.Tech degree in Information Technology from Paavai College of Engineering from Namakkal in 2012. He is currently doing M.Tech in the department of Information Technology in Sathyabama University, Chennai, Tamil Nadu, India.

Jeyanthi. P received the Ph.d degree in Department of computer science from Sathyabama University, Chennai, Tamil Nadu, India, in 2015. She received her ME degree in Department of computer science from Sathyabama University, Chennai, Tamil Nadu, India, in 2001. She received her BE degree in Department of computer science from periyar Maniammai College from Thanjavur, in 1996