International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP75-80

Trustworthy and Secure Information Transmission In MANET

Priyanka D.Takalkar[1], Aaradhana A. Deshmukh[1]
(Dept.of Computer Engineering, Smt.Kashibai Navale College of Engineering Pune, India, takalkar.priyanka37@gmail.com)

Abstract:- A "mobile ad hoc network" (MANET) is an independent system of mobile routers and hosts connected by wireless links. The routers are open to move arbitrarily and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and randomly. For data communication, we need a routing protocol that adapts to topology changes. In the collaborative MANET environment, practically any node can maliciously or greedily disrupt and deny communication of other nodes. In MANET Secure data transmission is one of the best issue. We are doing enhancement in the secure data transmission in MANET using trust based multipath routing protocols. Expecting the performance enhancement in Packet delivery ratio,End to end packet delay, Throughput of secure data transmission in comparison with existing similar routing protocols for MANET

Keywords: - Decryption, Encryption, Mobile Adhoc Network, Misbehaving nodes, path Trust, Secure Data Transmission, Security Algorithms.

I. INTRODUCTION

Mobile ad-hoc network (MANET) is of high research value and wide application prospects. Due to its mobility, dynamic topology, equivalence, self-organizing and other unique features, it has great advantages in emergency communications and military mobile communications. Routing is one of the core issues in mobile ad-hoc network. An effective routing mechanism will be helpful to extend the successful deployment of mobile adhoc network. There are various techniques available for secure data communication from source to destination in manet. In single route routing only single route is available in between source and destination by using that route we can send data from source to destination, but if that route is not available or if connection is failed then we cannot send data from one node to another. There are various routing protocols present in single routing. Multiroute routing protocols are proposed based on the principle that higher performance can be achieved by recording more than one feasible route. Multipath routing has been explored in several different contexts. By implementing multipath routing, data forwarding can continue uninterrupted on other available routes without waiting for finding a new route even if the primary route fails data. In MANET, Multipath routing protocols are used to provide reliable communication as well as improve quality of service of ad hoc and mobile Network. Multipath routing allows the establishment of multiple routes between a pair of source and destination node in mobile ad hoc network. It is typically proposed in order to increase the reliability of data communication or to provide load balancing and has received more and more attentions.

II. RELATED WORK

This section analyzes all the existing methods to MANET environment. This method focuses on data security. The SMT (Secure Message Transmission) is well known protocol for data transmission [1]. It is used to maintain the data transmission against random malicious behavior of network nodes. SMT for secured data communication provides end to end secure and strong feedback mechanism. SMT uses an active path set comprising node disjoint paths, determined and deemed operational at the source for communication with a specific destination's disperses each outgoing message, adding limited redundancy to the data and dividing the resultant information into no of pieces, which are transmitted across routes one piece per route.

SMR (Split Multi-path Routing) is open maximally node disjoint paths [5]. In this method routes are discovered on demand. When destination received RREQ (Route Request) packet, destination selects two multiple node disjoint paths and send RREP (Route Reply) packet towards source.

In Multipath DSR Protocol, this protocol uses multipath forwarding approach [11][6]. In this each node sends RREQ to other node if it is received from a different ROUTE, using this method we are able to identify or avoid misbehaving nodes. When node received RREQ packet it first checked whether it is processed previously if yes then it simply fall the packet.

In TDSR, Trust is calculated on the basis of direct trust and indirect trust [7]. In this if trust value of node is fall out of a acceptable threshold range that nodes are added to the blacklist. In this when node X send RREQ packet to neighboring node i.e. then Y checks its blacklist whether node X is in it or not, if not then Y forwards the packet towards other node.

In paper [12] using threshold value detect misbehavior of node using packet forwarding misbehavior algorithm. If node exceeds the threshold value then it is considered as a malicious node and if those below the threshold considered to be correctly behaving.

III. PROPOSED SYSTEM

Communications in mobile ad hoc network has two phases i.e. route finding and secure data communication .These both phases focuses on data security.

3.1 Multiple Secure path Discovery
Multiroute routing consists of finding multiple routes between a source and destination node.

1.1.1 Trust calculation
Trust is an important aspect in mobile adhoc networks (MANET).

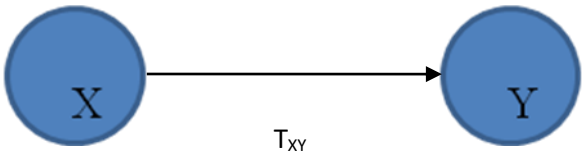

Fig 1. Trust between nodes

T_{XY} is the trust in a node y by node x as Txy and is given by the following equation,

$$Txy= P_A / P_P \quad (1)$$

Where P_A represents the category packet acknowledgements that maintain a count of the number of packets that have been forwarded by a node. P_P represents the category packet precision, which preserves a count of the number of packets received correctly.

1.1.2 Path Discovery at Source Node

By Broadcasting RREQ packet, source initiates route discovery process. RREQ packet contains trust value field.

$$RREQ: \{IPd, IPs, seq\ num\} || p\_trust \quad (2)$$

after broadcasting the RREQ.

3.1.3 RREQ processing at intermediate nodes

Intermediate node forward the RREQ packet if it received from another node and it adds its trust value to RREQ packet for avoid route loop.

$$p\_trust = p\_trust + T_{XY} \quad (3)$$

3.1.4 RREP processing at intermediate nodes

Intermediate node receives the RREP packet if it received from another node and it adds its trust value to RREP packet for avoid route loop. It updates n_trust field as,

$$n\_trust = n\_trust + T_{XY} \quad (4)$$

3.1.5 RREP at destination node

In RREP, it contains two fields p_trust and n_trust.RREP is

$$RREP: \{IPs, IPd, seq\ num\} \| p\_trust \| n\_trust \quad (5)$$

3.1.6 Path decision at source node

After finding multiple routes between source and destination, we have to find best route which is trustworthy. When RREP packet reaches to the source node, it calculates route_trust which is the trust value associated with path

$$path\_trust_{i} = ((p\_trust + n\_trust) / 2) \quad (6)$$

$$(path\_trust)_{s\text{-}d} = \max (path\_trust_{i}) \quad (7)$$

Where i is trust value of i^{th} path.

Consider the following network,

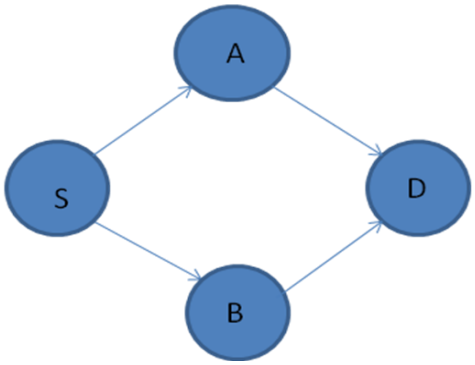

Fig 2. Ad hoc network

Consider S as a source node and D as destination node. Here source does not have the direct route towards destination. So first S initiates route discovery by sending RREQ to its neighbours. Let us consider RREQ packet reach at D by using route S-A-D.Each intermediate node modifies p_trust by adding trust value of the node from which it received the packet. p_trust value is,

$$p\_trust = T_{AS} + T_{DA} \quad (8)$$

Now RREP is sent from D to S from the path D-A-S. Now n_trust will also updated by intermediate nodes. n_trust will be,

$$n\_trust = T_{AD} + T_{SA} \quad (9)$$

$$path\_trust_{i} = ((p\_trust + n\_trust) / 2) \quad (10)$$

$$path\_trust_{S\text{-}D} = ((T_{AS} + T_{DA} + T_{AD} + T_{SA}) / 2) \quad (11)$$

3.2 End to End data security

3.2.1 Encryption Process

Encryption is the process of encoding information in such a way that other cannot read it, but only official parties can. Message is divided, encrypted and forwarded through secure multiple paths. The proposed algorithm is an symmetric algorithm. Based on the length of the cipher key 10, 12, 14, round keys are generated. The input for this algorithm is 128bit.Then key size is 16byte.Steps in encryption and decryption process is as follows,

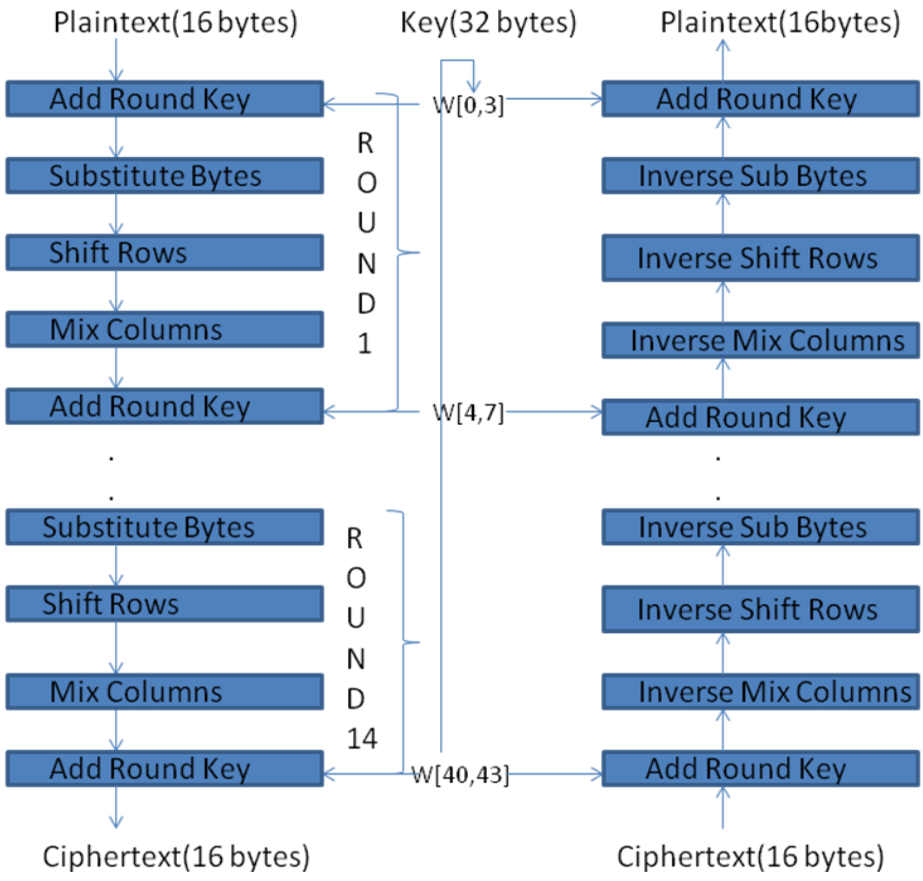

Fig 3. Encryption & Decryption Process

3.2.1.1 Substitute Byte Transformation
AES defines a 16*16 matrix of byte values called S box that contains a permutation of all possible 256 bit values.The leftmost 4 bits of the byte are used as a row value and rightmost 4 bits are used as a column value.These row and column values serve as indexes into the S-box to select a unique 8 bit output value.

3.2.1.2 ShiftRows Transformation
The first row of state is not altered.For the second row,a 1-byte circular left shift is performed.For the third row,a 2 byte circular left shift is performed.For the fourth row,3 byte circular left shift is performed.

3.2.1.3 Mix Columns Transformation
Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 02 & 03 & 01 \\ 03 & 01 & 01 & 01 \end{pmatrix} \begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{pmatrix} = \begin{pmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{pmatrix}$$

Fig 4. Mix Columns Transformation

3.2.1.4 AddRoundKey Transformation
This is the last step in algorithm. In AddRoundKey transformation,128 bits of states are bitwise XORed with the 128 bits of the round key.

3.2.2 Decryption Process
Decryption is the reverse procedure of encryption.

IV. DISCUSSIONS

a. Metrics
To calculate the performance of the proposed method, we can use the following metrics:

End to End Delay: time taken by the data packets to reach their respective destination.

Throughput: It is the rate of successful packet delivery over a communication path.

V. CONCLUSION

In this proposed method, we can perform secure routing with the help of trust value of path, also we can provide security using security algorithm. In future it can be implemented in real time application with the help of end to end delay and throughput.

VI. REFERENCES

Journal Papers:

[1] Panagiotis Papadimitratos and Zygmunt J. Haas" Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security September 19, 2003.

[2] Poonam Gera, Kumkum Garg, Manoj Misra, "Trust Based Multi-path Routing for end to end secure data delivery in MANETS", SIN 10 Proceedings of the 3rd international conference on Security of information and networks, Pages 81-89,ACM, 2010

[3] Jiazi YI, Asmaa ADNANE, Sylvain DAVID, Benoıt PARREIN, "Multipath Optimized Link State Routing for Mobile ad hoc Networks", published in Ad Hoc Networks 9, 1 (2011).

[4] Rohan Rayarikar,Ajinkya Bokil,"An Encryption Algorithm for End-to-End Secure Data Transmission in MANET ",IJCA, Volume 56– No.16, October 2012 .

[5] Lee, S., Gerla, M. Split multipath routing with maximally disjoint paths in ad hoc networks.Proceedings of the IEEE ICC (2001) 3201–32055

[6] Pissinou, N., Ghosh, T. and Makki, K. 2004. Collaborative trust-based secure routing in multihop ad hoc networks. Networking (Athens, Greece 2004). Lecture Notes in Computer Science, vol. 3042, 1446-1451

[7] Wang, C., Yang, X. and Gao, Y. 2005. A Routing Protocol Based on Trust for MANETs. In Proceeding of Sixth Annual International Conference on Grid and Cooperative Computing (Beijing, China). Lecture notes in computer science, vol. 3795, 959-964.

[8] . B. Pranisa,B.Thanikaivel,, "Fast and Secure Data Transmission in MANET", International Conference on Computer Communication and Informatics (ICCCI)Jan. 10 – 12, 2012.

[9] Asad Amir, Pirzada, Amitava Datta, Chris McDonald"Trust-Based Routing For Ad-Hoc Wireless Networks", 12th IEEE international conference on network,pp 326-330,2004.

[10] Poonam Gera, Kumkum Garg, Manoj Misra, "trust-based Multi-Path Routing for Enhancing Data Security in MANETs",International Journal of Network Security, Vol.16, No.2, PP.102-111, Mar. 2014

[11] Johnson, D.B Maltz,Jetcheva, J.G 2003, "The dynamic source routing protocol for mobile adhoc networks,Internet draft IETF,RFC 3561.

[12] Oscar F. Gonzalez, Michae Howarth, GeorgePav ou,"An Algorithm To Detect Packet ForwardingMisbehavior In Mobile Ad-Hoc Networks ",IEEE (2007).