ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Anonymous Routing in Trust Valued MANETs Prior to the Deployment of Onion Routing

Vamsi Krishna .Y[1], Vignesh .S[2]

Associate Professor, Department of Information Science and Engineering, Sri Krishna Institute of Technology ,Chikkabanavara Bangalore, India[1]

UG Student, Department of Information Science and Engineering, Sri Krishna Institute of Technology ,Chikkabanavara Bangalore, India[2]

ABSTRACT: Invisible property is very important for communication of the confidential data which is usually applied in mobile adhoc networks (MANETS) and it is a tedious task to have unidentifiability and unlinkability in structureless network. In existing system several anonymous routing protocol have been proposed but still there are no satisfactory results that have high packet transmission based on trustworthiness. Therefore this paper proposes an effective trustworthy algorithm which is explained in brief as part of onion routing process which gives effective increment of the packet security exploitation from the middling nodes which is to be forwarded to final destination, which gives efficient anonymicity of the packet carrying the confidential data. It also explains the tor- onion routers, its traffic, hidden services, abuses and attacks in tor network.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are structure less network which are easily prone to security threats and attacks. Since it's a dynamic topology, It is tough task to provide trust full and secure communications with authentication and anonymicity. So it is important to have a trusted network management, implicitly when the nodes do not have any prior knowledge of each other to give assurance that the information is given only to the trusted node in which there are four particular behavioural entity[1] and there are four major features of trust full network which are Context dependence, Function of un certainity , Quantitative value, Asymmetric relationship [2] this traditional method is used to calculate trust value for every node and specific decision is taken whether to eliminate or retain node in the routing path. The trust value is calculated for every node based on the success and failure rate [2]. The basic requirement of the MANET is to have the trust capacity for invisible and anonymous communication so that node should be un findable for mobile nodes. This paper proposes an algorithm which uses a trust value which in turn explains the deployment property of effective key based encryption onion routing protocol to provide anonymous routing and the authenticity is given by group signature which is briefly explained in tor network. There are many routing protocols that have anonymous and include authentication, such as AODV [3], DSR [4], AASR[5] but none of this explain the effective procedure to provide packet exploitation. For this reason, the paper proposes a trust value calculation using trust algorithm in wireless network. This paper includes background and related work in section II ,network assumptions in section III, objective, overview and Routing design in section IV, Trust algorithm in section V, onion routing protocol process and its hidden services, abuse , attacks in section VI, performance and simulation results in section VII conclusion and future enhancement are described in section VIII.

This paper adopts a special key encrypted onion to record a identified route and design an encrypted secret message to check the RREQ-RREP connectivity .Group signature is used to authenticate the RREQ packet per hop, and to protect the intersecting nodes from changing the routing packets.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

II. BACKGROUND AND RELATED WORK

This process of background and its associated works give us some implementation methods that are effectively and widely used in anonymous secure routing.

A. Trapdoor: Is a mechanism that is based on cryptographic function and is one of the basic concept that is used in single lane function between[6] the pair of sets by which it will accumulate the data elements by the middling nodes such as node IDs in the trap door. Only certain authorized nodes such as sender and receiver can access the data elements because, before deploying the trapdoor mechanism, the node should initially share the secret key to have end to end key agreement mechanism.

B. Group Signature or cluster signature : The cluster signature will [7] provide effective confidentiality and integrity without altering the anonymicity of the network such that every node in the network will have its own public or private key which is issued by the group authorizer, so that nodes can also produce its own private key and this signature is being found identical by the other member clusters in the network hence cluster signature establishes the effective authentication without changing the anonymicity in the network The keys can only be traced and checked by the trusted group authority.

C. Onion Routing: Onion routing is a special technique for anonymous communication in which data messages are encrypted which are analogous to onion as show in fig.1 below and this mechanism will deploy a private communications in a public network [8]. The sender node forms up the inner core of an onion which is a identical route message. In this situation, in a route request phase, each forwarding node adds an encryption layer to the route request message. The sender and receiver nodes need not know the ID of the node to which the message as to be forward or received from. The receiver node receives the onion and puts it along the routing track back to the sender node. The intersecting middling node can check and validate its implementation by decrypting and eradicating the outer layer of the onion, thus eventually an anonymous route can be
established with the help of onion routing protocol.

D. Multipath routing: As the name suggest, the path is not constrainted or made static for finite nodes [9], but it is enhanced to have multi node connections with the multiple paths intermediately thus in turn reduces the traffic load and can have effective and smooth resilient data transmission.

Fig .1. onion routing topology

III.NETWORK ASSUMPTIONS

In this phase lets assume that MANET is denoted by I and believe the following assumptions.

A. Public Key Infrastructure (PKI): Every node I initially has a pair of public or private keys produced by the public key infrastructure (PKI) or this keys can be also generated by other certificate authority (CA). For node X ($X \in I$), its public/private keys are denoted by $KX+$ and $KX-$ respectively as we pre assume that there is a dynamic key management scheme in I which is based trust management[1], which supports the network to execute without online PKI or other CA services.

B. Group Signature: A s i n f o r m e d earlier the entire network I has a group formation and each node have a pair of group public or private keys given by group manager. The group public key is indicated by $GI+$, is identical for all the nodes in I, and so the group private key, denoted by $GX-$ (for $X \in I$), is differentiable for each and every node. Node X will sign a message with its private key $GX-$, and this data message will be decrypted through the public key $GI+$ by the other cor r esponding or nodes in I, which keeps the anonymity of X. This also pre considers that there exists a dynamic key management scheme working parallely with admission control function of the network for satisfactory

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

trust and anonymity of the network I, which intiates the group signature technique is working correctly. Such considerations are also taken in the existing work of military ad hoc networks [7].

C. Neighborhood Symmetric Key: As name tells that the nodes which are next to each other can have a agreement and can create its secret key by public or private key. And this combination will have a triggered either by a time changing dynamic HELLO messages for initial deployment or by the routing discovery RREQ messages. For two nodes X and Y ($X, Y \in I$), the exchanged symmetric key is notified by K_{XY} and this method is adopted for the data message transmissions between the nodes. There are some methods supporting the connectivity of single-hop shared key, such as MASK, RAODR, and USOR. In this work, we assume one of the technique is preferable in I The notations are indexed as follows in table 1

Notations	Descriptions
K_{X+}	Public key of node X
K_{X-}	Private key of node X
G_{T+}	Group public key of network I
G_{X-}	Group private key of node X
K_{XY}	Symmetric key shared by nodes X and Y
$\{d\}K_{X+}$	Data d is encrypted by key K_{X+}
$[d]K_{X-}$	Data d is signed by node X
$\langle d \rangle K_{XY}$	Data d is encrypted by shared key K_{XY}
$(d)K_X$	Data d is encrypted by one symm. key of X
$O_K(m)$	Encrypted onion for message m with key K
N_A	One-time Nym. generated by X to indicate itself
dest	A special bit-string tag denoting the destination

IV. OBJECTIVE AND OVERVIEW OF THE PROTOCOL

A.Objective

This paper proposes an effective trusted secure protocol which intend helps to provide authent ication and confidentiality of the packet transmission in MANETS which will have below mentioned features .

1) Trust based: Only the selected nodes will be deployed in data transmission as a result it forms a high security.

2)Privacy: The data is maintained confidential by involving only private nodes , Thus it involves an effective anonymous communication.

3)Network Security: I t provides a resisting capacity to attacks such as active and passive attacks by identifying initially only in the network.

4)Performance: effective privatization and efficient network security which will increase the performance of MANETs.

B .Overview of Protocol :

This paper put forth the packet node forwarding theme in MANETs in which they are centralized by using a protocol . Packet forwarding are done by using the approved node based on group signature[7] and onion routing[5] which effectively increases the packet security exploitation hash worth and forwarding property based on the specific correct destination node. The destination is verified by the trapdoor technique by

it provides an end to end secret key encrypt ion, now this protocol gives us an trust algorithm which gives the special middling node to have a effective shorter routing based on the trustworthy packet which in turn facilitates the effective top to finish packet transmission delay and consumption of the energy which is being used.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

C. Routing Design

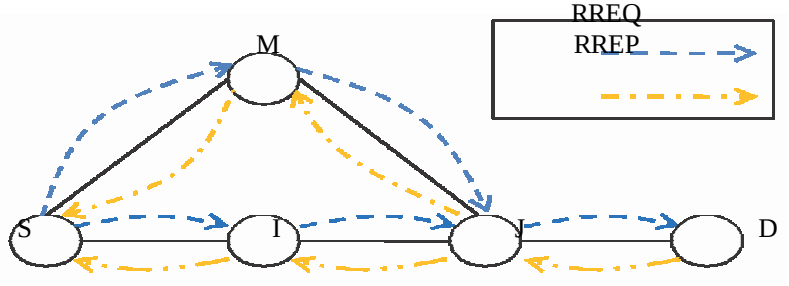

Fig2. Network topology

The design of the Authenticated anonymous secure routing protocol based on the t rust is shown below[2] [7] .The trust routing within the network is provided to the packet during its transmission. The routing methods which will move from the sender S and the receiver D as shown by above fig .2. Here to design the specific routing design we consider the design as one is on demand routing protocol [9] and AASR[7] which explains onion routing process so we adopt this two concepts to have better and clear understanding. Routing design is explained in following steps :

Step 1: Every node I at the initial provided by the PKI as said earlier it gives the private/public key for nod e *X* ($X \in I$), in which the public/private keys square measurement which is denoted by KX+ and KX+.

Step 2: As considered as entire network as I every cluster group node adds group public/private key generated by the group authorized manager. The group public key is denoted by GI+ in which this is same for entire network I where as the personal group is different for

different nodes which is denoted by Gx- (for $X \in I$).

Step 3: Node x will sign a message with its personal key GX which is given by the group manager and this message is decoded through the general public key GI+ by the backside node in network I which keeps the invincible property from neighborhood symmetric key.

Step 4:By using public key and private key the two corresponding nodes establishes a security association.

Step 5:By activating the periodical message or the route request message for 2 nodes *X* and *Y* ($X, Y \in I$), used for the communicating among them and it is denoted by Kx y .

Step 6:An additional trust worth node is assigned " TT r u s t " to calculate which is in turn done by the be low explained trust algorithm.

Step 7:To the corresponding neighbouring node it exchanges a information as show(Neighbor_Nym,Session_Key) .

Step 8: the routing table is updated when every it has a new entry and it stores the request anonym the secret verif ication message at the time of route discovery(Req_Nym,Dest_Nym,Ver_Msg,Next hop_Nym,Status) .

Step 9: The forwarding table records and stores the dynamic data of the longtime route(Rt_Nym,Prev_hop_Nym,Next_hop_Nym)

Step 10: While forwarding it will check for the trust value , this trust value is compared with the other neighbouring trust node if the trust is not satisfied then it will choose other routing path.

Step 11: The source node will start it transmission in a specified route to the destination if there is any middling node the data packets

will forward by using the route pseudonym.

V. TRUST ALGORITHM

The specified rule for the trust values will be applied for individual nodes firstly all the nodes in the structureless adhoc network have one hundred trust value the rule will have two steps one is initialization and other is the updating the initialized trust values.fig3 shows the routing process based on the trust value.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

[A]Initialization:
1.As said earlier the involving nodes for communication will be
initialized by 100.
2.Assuming that 1 trust value= 10 packets dropped (to reduce packet exploitation)

[B]Updating the trust value:
Here we can divide themes of updating the trust values in three waysone is based on correct transmission other is in which packets are delayed or dropped ,last is the criminal node.
1. If the packets are transmitted correctly from node to node , if it lies between 1 to 10 then trust value is incremented by one that is- Updated trust value =old trust value +1 ,or else if the packet transmission is more effective and its above 10 the it will update trust incrementally as -Updated trust value=old trust value+(correctly transmitted packets/10)
2. If the packets are dropped or delayed that is if delay lies between 1 to 10 packets then it is decremented by 1 as shown Update trust value=old trust value-1. Else if the packets are more delayed that if it is more in number the we decrement node trust value by- update trust value=old trust value-(packet dropped or delayed /10).
3. If the trust value of particular node is negative or criminalized
then it will automatically dropped.
When the

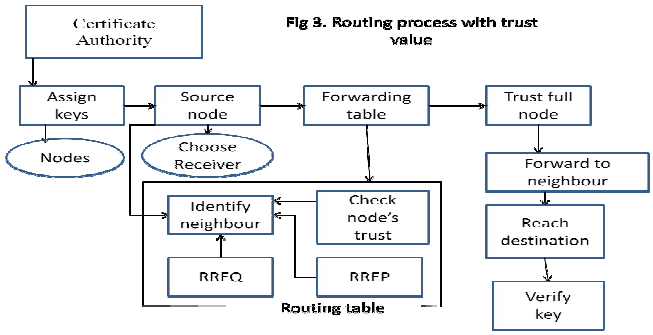

Fig 3. Routing process with trust value

VI. ONION ROUTING

As discussed earlier in the back ground and related work we saw what is onion routing , now here we discuss the process of onion routing protocol , we adopt the concept of AASR[5] in which it explains the anonymous secure authenticated routing in chaotic nature.

A . Procedure of onion routing
Below are the following steps taken onion routing protocol.
Step 1: during the route discovery process a source node exposes aRREQ in network.
Step 2:if an middling nodes gets the RREQ packet it will check the RREQ by considering its own group or cluster public key and this will add up one layer of encryption on core data and this process untilRREQ reaches destination node.
Step 3: once if the RREQ reaches the destination node, then the RREP packets will exposed back to the source node.
Step 4:on the reverse path back process if the middling nodes gets the RREP packets then it will update the routing and forwarding tables, then
later one by one the encrypted layer is removed (decrypted) this process is carried until RREP reaches the source node.
Step 5:As soon when the RREP received from the sender node it will update its routing table and forwarding table the this route discovery phase is completed.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Step 6:Then the source node transmit the data and the middling node forwards the data packets by using node pseudonym.
This is the over view of the onion routing process based on the network assumption and routing design which are specifically made for anonymous and secure routing. And the trust value calculation based on trust algorithm says that only specific trusted nodes to involve in the packet transmission because to reduce the packet exploitation. The most common argument against tools for anonymous communication is to have effective authenticated anonymous in packet transmission but criminals can use it to plan future crimes, exchange illegal content etc. without exposing it to the recepients who are involved in the communication , [10].Now a days criminal acts that they are intending to have effective anonymous routing based on the network traffic loads so the people will not have suspection over criminals so to get rid of this we use Tor to get away with their actions.

B . Tor- onion routers
Tor is a distributed, exposed anonymous MANETs . it is not worked by any organization but a set of organization so to have a specific individual generatingnthere own bandwidth and processing capacity the tor software is an open source so any body can use it to check the defects and flaws the tor project is maintained by the free haven project and make it unphisable and it is deployed in the stack and TCP application of mobile networks with the help of SOCKS interface so the tor will have an anonymous communication over large specified tor network with specified tor packets based on trust value in turn the tor network is authorized for only specified registered client and server because they the communicators should have some specification to data base accessing for the back up and boot strap process. This is also done to lower the load on the main directory. A list of some directory servers is distributed with Tor to facilitate joining the network strapping process.

As our paper main is to implement the authenticated anonymous routing protocol (onion routing) only in trusted nodes in a network to reduce packet exploitation

C. Hidden Services
It is the main feature in the tor onion network for which it is having the effective use anonymous communication ,so there are other internet
hidden servies top track or follow the specified user, such as message board or other web pages. The host will not have any knowledge of the communication happening, but the main disadvantage is that it will not always support the dns via socks in fact Hidden Services can be accessed by all users of the Tor network, and are developed to defend the assessing authority, DDoS and physical attacks respectively tor uses a " rendezvous points" in which hidden servies are provide the location of the network cannot be specified so this creates a high anonymicity for communication.

D. Abuse and Attacks
1)Abuse
Executing the exit nodes on the tor networks is the main reason for abuse such that the misuse of the tor for spam ,threats ,hacking,abusive IM and file sharing illegally infact being having more strict policies and procedures the traffic has been reduced . the exit policies defends
and rejects private IP address ,subnet address, email(SMTP) and also windows file sharing methods etc.how ever the exit nodes are prone to
the abuse and threats which will also issue with ISP agreements denying the traffic delays .but the update ISP have developed a copy right infrignment to reduce the exit node abuse.by limiting it certaining preferred bandwidth and its range.
2) Attacks on Tor
The tor network does not high proof anonymity and confidentiality ,in fact it provides a satisfaction the have anonymous communication
traffic by the exit nodes to last destination is initially sent with plain text to check whether it has any attacks by interception by any localized hacking network including to the exit nodes , so it confirms that there is not threat for anonymity, but the problem is to provide the confidentiality. So the answer to this is that to use encryption on the application level between the source and destination if the both

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

sender and receiver uses a tor network. Then the exit node is chosen as the destination nodes and there traffic is encrypted during the process.
The plain text snooping is a main attack on the system, but many are unaware of this process of hacking. There are some more attacks which will expose the tor user to some extent but one being in the time analysis except the DNS problem, in which it will vision the packet travelling which are too tough to find for a specific user or organization so this explains the possible attacks in tor network.

VII .PERFORMANCE SIMULATION AND RESULTS

As earlier said that we use the concept of AASR[5] and AODV[3] for the effective module and extending it scientifically to have the good and decent performance , so here we tend distinguish the result performance with AASR and trust algorithm as explained above. To compare the performance we consider the matrices that are effectively listed out below based on its features and characteristics it exposes the performance analysis of the proposed system , As a result we award the performance given by AASR and AODV for each configuration and records,So there five square matrices are considered as shown and explained below:

1.Through put :As is name says that through put is the packets delivering capacity with full energy and with less modulation .Efficient through put gives the efficient packet communication with less traffic congestion.the target is set so that if high packet turned over in network then the capacity of packet through put is more effective . And it is estimated that 40% to 45% of the packet transmission is achieved in proposed system. And through put graph is shown in fig.4.
2.Packets Birth and its delivery rate : As in proposed system we said based on selected packets we will deploy onion routing process to anomycity so that packet birth and its delivery rate also is increased in network with high capacity nodes based on the trust algorithm and make less prone to traffic congestion in the proposed system it is the packet reduced approximately by 13% to 15% and the delivery rate is given by the CBR resources which say based on the receiver receiving packets the magnitude of the packets delivered rate is calculated And the packet loss ratio graph is shown in fig 5.
3.End to End delay : the end to end delay says the time period of packet travelled from one node to another node i.e from sender node to receiver node.In which it includes the retransmission, buffering, propagation factors which are effectively consider to measure the end to end delay .one more main factor is selecting the optimal path which reduces the end to end delay by increasing the range of each hop jump and intermediate hops(jumps) in the network so the path is more stabilized and made more effective to lessen the end to end delay.the graph of end to end delay is shown in fig 6.

Fig 4: Per flow through put

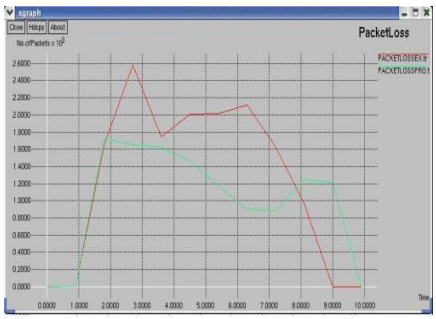

fig 5:Packet loss

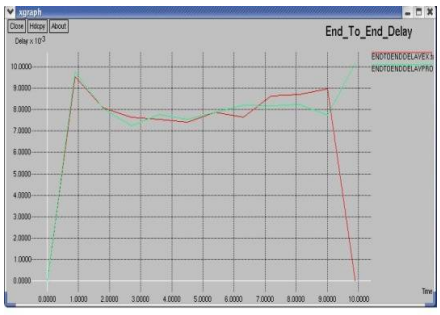

fig 6:End to end delay

VIII. CONCLUSION AND FUTURE ENCHANCEMENT

This paper, designs an effective trust algorithm to reduce the packet exploitation based on the trust value of certain specified nodes that can be considered for the authenticat ion of anonymous routing protocol[5] for MANETs in chaotic

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

condition. This explains the procedural process of onion routing to have a anonymous routing with incept concept of group or cluster signature which is used for the authentication and it also explains the tor onion routers. Its hidden services, lastly abuse and attacks in tor network. The future work, is to integrate the onion routing with garlic routing. **Garlic routing** is an enhancement of onion routing that encrypts multiple messages together to make it more difficult for attackers to perform traffic analysis and making it more secure which have highly structured anonymous routing. It is one of the best protocol that differentiates I2P (invisible internet project) from other privacy or encryption networks. Thus, trust model provide high anonymicity to routing protocols.

REFERENCES

[1] Sridhar subramanium and Bhaskar rama Chandra ,"trust Based Scheme for Qos Assurance in Mobile Ad-hoc Network". International Journal of Network Security & Its Applications (IJNSA), Vol.4,issue.1, January 2012
[2] "Trust computation and Trust dynamics in Mobile Adhoc Network:survey.". IEEE Communications Surveys & Tutorials Vol.14 , Issue: 2 ,2012
[3] C. Perkins, E. Belding-Royer and S. Das, " Ad hoc On- Demand Distance Vector (AODV) Routing," Internet RFCs pp 15-24, July2003.
[4] D. Johnson, Y. Hu, and D. Maltz, "- The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Internet RFCs,pp 9-12, Feb 2007.
[5] wei liu and mingy u ,"AASR:Authenticated Anonymous secure Routing For MANETs in Adversial environments". IJAICT Volume 1, Issue 6, October 2014
[6] S.william and W. stallings ,"Cryptography and network security" 4th Edition pearson Education India vol 1 ,pp 10 -25 ,2006.
[7].D Boneh,X.Boyen ,and H.Shancham," Short group signatures", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 4,issue.6, Dec 2014
[8]M.G.Reed,P.F.Syverson, and D.M. Goldschlag,"Anonymous connections and Onion Routing".IEEE Journal on selected Area in comm.,vol 16. IEEE journal on selected areas in communications, vol. 16,issue. 4, may 1998
[9]Jiejun Kong, Jun Liu, Xiaoyan Hong, Dapeng Wu, Mario Gerla, "On Performance Cost of On-demand Anonymous Routing Protocols in Mobile Ad Hoc Networks", in Mobile and Wireless Network Security vol 1 issue 4 ,July 2007.
[10] Henrik Erkkonen, Jonas Larsson and Datateknik, Chalmers, "Onion Routing with TOR". Computer communication and distributed systems vol 1, issue 1, jan 2015