MISCONDUCT DISCLOSURE OF THE INTERMEDIATES USING THE TRUSTED AUTHORITY

N.Vijay[1], S.Aarthi[2], M.Pandiyanathan[3]

[1]*N.Vijay PG Scholar, Computer Science and Engineering, M.A.M College Of Engineering, Tamilnadu, India*
[2]*S.Aarthi PG Scholar, Computer Science and Engineering, M.A.M College Of Engineering, Tamilnadu, India*
[3]*M.Pandiyanathan Professor, Computer Science and Engineering, M.A.M College of Engineering, Tamilnadu, India*

Abstract

In delay tolerant network which has an certain problem for while transmitting data from source to proper destination due to traffic or missing data. To solve this problem, motivating the concept of advanced i-trust scheme. The proposed model which provides solution for that delay tolerant network problem. The game theory approach which has to send an duplicate message from sender to intermediate node, if anyone node act as malicious node,we can easily predict that node and trusted party who verify the signature of intermediate node. To provide security while transmitting the data by introducing the concept of Triple des algorithm.This will provide more security rather than an RSA algorithm.

Keywords—*advanced iTrust, reliable authority, Triple DES, RSA algorithm.*

----------***----------

1. INTRODUCTION

Delay tolerant networks (DTNs) deals with an hetrogeneous network that may lack in continous network connection. Routing is the major concern part of the network because which has to establish the path among all the nodes from the source node to proper destination node. When an user has to forward or send the data from one node to next node, we have to concentrate on two things like route discovery and maintanence phase. If anyone node doesn't have path from source node to any other node, create path to all other nodes from source node by using an discovery mechanism.

2. RELATED WORK

The routing mechanism which has to create path from one node to another node but it does not send a failure data or packet from the corresponding node. We need to send an missing data to the destination node after recovery. By finding an alternate path if any one node get fails while forwarding data. If any user wants to send an data or packet to final node, it requires an intermediate node to reach an destination or final node.

The intermediate node who has to verify by any other reliable party to determine whether the corresponding node is good or not. Because sender and receiver node may not act as thief node but the intermediate node act as an duplicate node. The author described in survey paper such as three main important concepts like packet missing, congestion, dropping of packets while forwarding the data.

Consider the three nodes which are going to communicate one by one. Nodes are A,B,C and then if node A wants to send an data to node C by using an intermediate node B.when an node A starts sending an data to node B,then the node B who receives the data or information. Then node B who has to send the data to node C before that node B has take an original data. These are all the problems facing while sending or forwarding data from one node to another node.

Forwarding history to be maintaining each and every node while sending or forwarding data. The author has to be introduced several techniques to tolerate this problem but it is not suitable for solving the network problem. Suppose if any node act as thief node, the thief node can identify by using an watch dog technique and path has to calculate by using rater method.

The misbehaving node history to be find but not properly eliminating and maintaining duplicate node history or duplicate node from the network by used an existing method.

To overcome this problem introducing the advanced i-trust model and triple des algorithm.

And also it has to be find an duplicate node as well as reliable node to send an original data by using an game theory. This mechanism which has to send an duplicate message or data to intermediated node, which node gives an immediate response to source node that should be considered as reliable node.

3. PROPOSED SYSTEM

The proposed model which deals with an different strategy and algorithm to resolve an overall problem identified in survey. The advanced i-trust model to be identify an unwanted node present inside the network. The user has to create the sender and receiver node at initially and then sender has to select the intermediate nodes to forward the data by using an proposed model.

The sender who has to collect the participating nodes in the intermediate side. After collecting the routing nodes details

that information to be passed to reliable person. Then only sender starts sending an original data to intermediate nodes and intermediate node who has to create the signature among all nodes. Because the reliable person to cross verify the signature of intermediate and reliable node.If it matches with an original signature then only it will forward the original data to next node and receiver has to send an receiving signature to reliable person. Then the reliable person has to once again verifies the signature then it will forward the data to receiver side.

3.1 Advantages

- Each node should maintain the contact details of all nodes.
- Advanced i-trust introducing an misbehavior detection scheme in DTNs.

3.2 Architecture

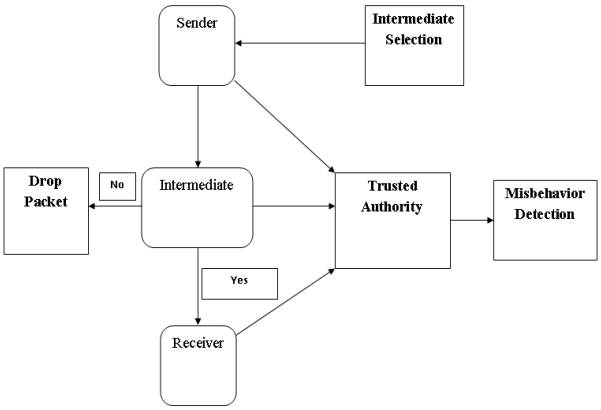

Fig 1. System Architecture

3.3 Proposed Algorithm

create number of nodes to participate n
count from i=1 to n
number starts from 0 to 10n-1
if mi /10n < pb then
all nodes should submit an history
if Detect (i, S,f, [r1, r2], R, D)
Then
Punish the theif nodes
else
payment will not refund back p
end if
else
payment will not refund back p
end if condition
end for condition

3.4 Proposed Modules

There are four modules present in the proposed system. They are Network Formation, Routing Module, Evidence Generation phase, Auditing phase

3.4.1 Network Formation

- Create number of nodes on the network for the data transmission process.
- The ids are generated for each of the individual nodes in the network.
- There are three algorithms are used, from that choose any one of the algorithm and use it to generate keys to all nodes.
- The user has to pay for new account creation.

3.4.2 Routing Module

- To pick the sender and receiver for the data transmission.
- Routing is the next process for select the intermediate node.
- This intermediate node is used to transfer the data from the sender to the destination.
- The distance of each node is calculated. And then the path cost is calculated.
- Based on this the intermediate is selected.

3.4.3 Evidence Generation Phase

- In this the forwarding history evidence is the first process, this is processed in the sender.
- Delegation task evidence is the second process. In this the signature of the source and the signature of the intermediate is processed.
- Contact history evidence is the third step in the evidence generation phase.

3.4.4 Auditing Phase

- Trust authority plays the vital role in the auditing phase.
- Trust authority sends the investigation request to the sender, intermediate, and receiver.
- The routing history to be sends to reliable person. Intermediate send the forwarding history to the trust authority. Receiver sends the contact history to trust authority.
- Based on this the trust authority find the misbehavior of the intermediate node.

3.5 The Advanced itrust Model

The advanced i-trust model which deals with an reliable person to verify the signature of the node history. A node sends an original data to corresponding intermediate nodes after checking an originality of intermediate nodes.

Based on the node mobility and data size to be fixed on the intermediate nodes before starting a process. The game theory method is mainly used for finding an originality of each node and identify the node speed or immediate response to source node. After finding an good node we have to proceed with an new process. And then three different phases to be maintained and game theory concepts which clearly identify the original node in the network.

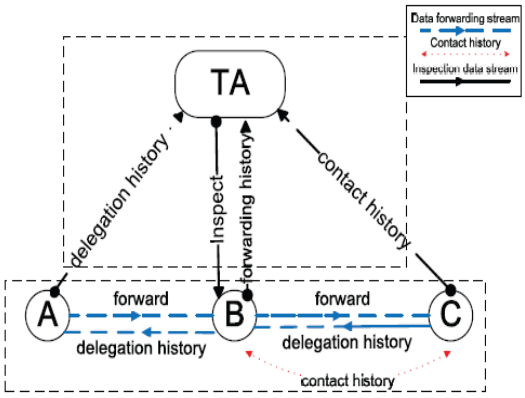

Fig 2. Advanced itrust model

3.5.1 Game Theory Analysis

The game theory is mainly used to identify the duplicate nodes and reliable nodes in the network. And it also number nodes to be calculated at source and destination levels by means of reliable node. The unwanted node doesn't get an initial payment after finding out.

- N = {N0, N1... Nn}
- si = {si0 , si1 , si2 , ..., sin } is the strategy set of the player
- πi is the payoff of the ith player Ni , and it is measured by credit earnings.
- i has an mixed strategy for player p

3.6 Triple DES Algorithm

The triple des algorithm is mainly used for enforcing security rather than rsa algorithm..

And then each time which has three rounds and each round has 56bit.

Two Steps
The plain text which has to converted into ciper text.
And then ciper text process can be again converting to plaintext after decrypting.

4. CONCLUSIONS AND FUTURE WORK

Here we are providing security , integrity as well as data transmission without network traffic. We implemented advanced i- trust model to find the unwanted node. The advanced i-trust model which will provide an greater efficiency for all kinds of network in future.

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots", in Proc. of IEEE INFOCOM'09, Rio de Janeiro, Brazil, April 19-25, 2009.

[2] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know The Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing", in Proc. of IEEE INFOCOM'10, 2010.

[3] Q. Li, S. Zhu, G. Cao, "Routing in Selfish Delay Tolerant Networks" in Proc. of IEEE Infocom'10, 2010.

[4] H. Zhu, X. Lin, R. Lu, Y. Fan and X. Shen,"SMART: Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," in IEEE Transactions on Vehicular Technology,vol.58,no.8,pp.828-836,2009.

[5] E. Aydayi, H. Lee and F. Fekri,"Trust Management and Adversary Detection for Delay Tolerant Networks," in Milcom'10, 2010.

BIOGRAPHIES

Vijay has successfully received his B.E computer science degree(2011) from v.s.b engineering college affiliated to Anna university, Chennai. He is currently doing PG scholar at M.A.M college of engineering, trichy.

Aarthi has successfully received her B.Tech information Technology degree(2012) from Kings college of engineering affiliated to Anna university, Chennai. She is currently doing PG Scholar at M.A.M College of engineering, trichy.

Pandiyanathan has received M.Tech from NIT trichy.He is doing Ph.d affiliated to anna university, Chennai. He is working as professor in M.A.M college of engineering, trichy.