Methodology of Improving Efficiency in Delay Tolerant Networks

Sapna. H. D[1],
[1]M.Tech. Student
Dept. of Computer Science Engineering,
[1]BTL Institute of Technology & Management
Bangalore-562125, Karnataka, India

Vidhyalakshmi . R[2]
[2]Assistant Professor,
Dept. of Computer Science Engineering,
[2]BTL Institute of Technology & Management
Bangalore-562125, Karnataka, India

***Abstract*- Delay Tolerant Networks (DTNs) are a class of networks characterized by lack of guaranteed connectivity. It does not mean a delay service instead DTNs provides a service where network enforces disruption. Routing in Disruption Tolerant Networks (DTNs) is threatened by the malicious node behavior. Hence designing a misbehaviour detection scheme in DTN is considered a great challenge. This paper presents iTrust, efficient misbehaviour detection scheme inorder to obtain the secure DTN routing. The basic principle of iTrust is acquainting a periodically available Trusted Authority (TA) to judge the node's behavior through the collected routing evidences and probabilistically checking. We framework iTrust as the inspection game and use game theoretical analysis to establish that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost.**

Key Words – Delay tolerant Networks(DTN's),Trust Management.

I. INTRODUCTION

Delay Tolerant Networks (DTNs) are those networks that seeks to address technical issues in heterogeneous networks.. Different from the traditional networks, the coming forth DTNs are characterized by the lack of guaranteed connectivityand long propagation delays within the network.

In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears and the bundles are. opportunistically routed toward the destinations by sporadic connections. This process is called "store-carry-and-forward" strategy. DTNs are persuadable to having their effective operation compromised by a variety of security attacks because of the features like unreliability of wireless links between nodes, constantly changing topology, restricted battery power, lack of centralized control and others. Security attacks can be through selfish nodes or malicious nodes. Selfish nodes are those who are not willing to forward bundles for others without sufficient reward. Malicious nodes arbitrarily drop others' bundles (blackhole or greyhole attack), which often take place beyond others' observation in a sparse DTN,.It leads to serious performance degradation. Hence misbehavior detection is highly required to assure the secure DTN routing and to improve the efficiency of flow among DTN nodes in DTN's.

II RELATED WORK

Q.Li.S.Zhu and G.Cao explains the process of routing in Socially Selfish Delay Tolerant Networks [3]. Existing routing algorithms for Delay Tolerant Net-works (DTNs) assume that nodes are uncoerced to forward packets for others. In the real world, however, most people are socially selfish; i.e., they are willing to forward packets for nodes with whom they have social ties but not others, and such willingness varies with the strength of the social tie. A Social Selfishness Aware Routing (SSAR) algorithm is proposed to allow user selfishness and provide better routing performance in an efficient way.. The design of SSAR will not take into account malicious behaviors and if attacker launches a black hole attack SSAR can tolerate it with least modification that a node never forwards packets to those .

Work by R. Lu, X. Lin, H. Zhu, and X. Shen, gives the idea of how practical incentive (Pi) protocol is used to accelerate selfish nodes to forward bundle packets in DTNs. By following the proper incentive policy, the proposed Pi protocol can improve the whole DTN network's performance in terms of high delivery ratio and low average delay and also gain the fairness among DTN nodes. Elaborated security analyses have shown that the proposed Pi protocol can resist most attacks launched by selfish DTN nodes. Detail security analysis have shown that proposed Pi protocol can withstand most attacks launched by selfish DTN nodes. Disadvantage is the framework of fair incentive protocol for multi copy algorithms have not yet been defined

H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen says that delay-tolerant networks (DTNs) render a promising solution to support wide-ranging applications in the regions. In DTNs, the intermediate nodes on a communication path are required to store, carry and forward the in-transit messages in an time-serving way, which is named opportunistic data forwarding. Such a forwarding process depends on the theory that each individual node is ready to forward packets for others. This assumption, however, might easily be offended due to the existence of selfish or malicious nodes, which may be unwilling to waste their precious wireless resources to serve as bundle relays. To overcome this problem, multilayer credit-based incentive scheme is proposed to stimulate bundle forwarding cooperation among DTN nodes.

S. Marti, T.J. Giuli, K. Lai, and M. Baker explains Self Adaptive Approach for Defending Flood Attacks in Disruption Tolerant Networks .Here rate limitation is applied to mitigate flood attacks in DTNs, and proposed a scheme which exploits claim carry- and-forward to probabilistically find out the violation of rate limit in DTN environments. In Rate Limit Controller, each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval. Every node also has a bound over the number of replicas that it can generate for each packet. The nodes which have received packets from the attacker carry the claims included in those packets when they move around. When two of them contact, they assure that if there is any inconsistency between their collected claims. This is how the attacker is detected when an inconsistency is found

II. EXISTING SYSTEM

This section describes some of the various methods that are applied to detect the misbehaviour of nodes in mobile adhoc networks. Extenuating routing misbehaviour has been employed in traditional mobile ad hoc networks. These works use destination acknowledgement to detect packet dropping [7], and use credit-based and reputation-based incentive schemes accelerate rational nodes. Even though the existing misbehaviour detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficulty to predict mobility patterns, and long feedback delay have made the neighbourhood monitoring based misbehaviour detection scheme undesirable for DTNs.

Disadvantages

➢ Proposals for misbehaviour based on forward history verification or encounter ticket are costly in terms of transmission overhead and verification cost.

➢ The transmission overhead incurred by forwarding history checking is critical for a DTN because expensive security operations will be translated into more energy consumptions, which represents a fundamental challenge in resource-constrained DTN.

➢ From the trusted authority point of view , misbehaviour detection in DTNs incurs a high inspection overhead.

III PROPOSED SYSTEM

This section presents a novel basic itrust scheme inorder to detect the misbehaviour of nodes in DTN's. In DTN, information is sent from node to node and this information is transmitted in the form of packets. When the connection is established, packets are sent from node to node. But if connection is lost, data packets are collected and then the connection is re-established and data packets are sent again. Thus to nullify packet loss in the network and to improve efficiency, the method is proposed which is known as a iTrust , probabilistimisbehaviour detection scheme.

As shown in Fig 3.1, the itrust has two phases .They are routing evidence generation phase and auditing phase. In the routing evidence generation phase, nodes will meet neighbouring nodes and pass the forwarding history to different nodes. In the auditing phase, trusted authority will differentiate normal node from the malicious node. It will be helpful for the nodes to take the correct path and reach the destination in a efficient way without any time delay.

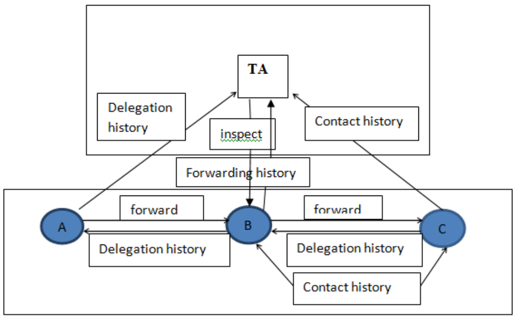


Fig 3.1 . Overview of Routing Evidence Generation Phase and auditing phase.

3.1 Routing evidence generation phase

Suppose node A has packets which has to be reached to node C.If node A meets another node B that could assist to deliver packets to C, then node A will forward those packets to B. Thus, B could forward the packets to node C when C is at the transmission range of B. The path between the sender and the receiver is shown in the Fig 3.1.1. Nodes will select the desired path to reach the destination with the administration of TA.

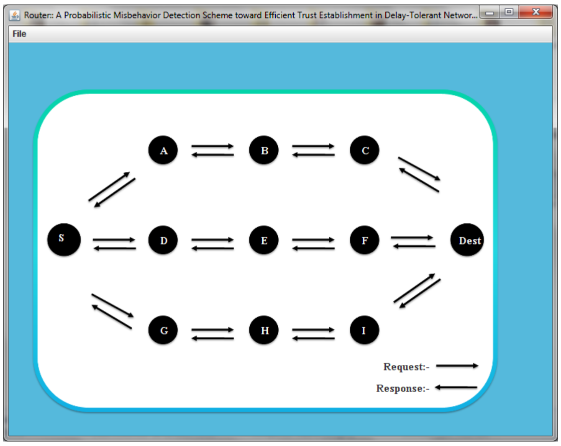
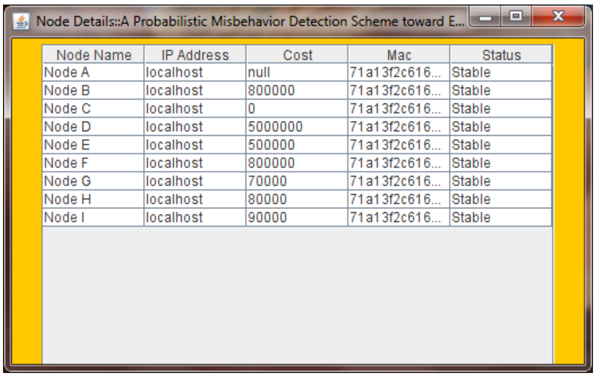

Router:: A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networ...
File
A
B
C
S
D
E
F
Dest
G
H
I
Request:-
Response:-

Fig 3.1.1 Path between sender and receiver

In the routing evidence phase, A sends packet to B, then it gets the delegation history back. B holds this packet, then takes on C and C gets the contact history about B. In the auditing phase, trusted authority will disseminate a message to ask all the other nodes to submit the evidences about B, when TA decides to check B. Then A submits the delegation history about B and C submits the contact history about B. All the evidences about the nodes will be maintained at the router. It is shown in the below Fig 3.1.2.It consists of node name, ipaddress, cost(capacity to forward packets),Mac address and status of node about its stability.



Node Details::A Probabilistic Misbehavior Detection Scheme toward E...

Node Name	IP Address	Cost	Mac	Status
Node A	localhost	null	71a13f2c616...	Stable
Node B	localhost	800000	71a13f2c616...	Stable
Node C	localhost	0	71a13f2c616...	Stable
Node D	localhost	5000000	71a13f2c616...	Stable
Node E	localhost	500000	71a13f2c616...	Stable
Node F	localhost	800000	71a13f2c616...	Stable
Node G	localhost	70000	71a13f2c616...	Stable
Node H	localhost	80000	71a13f2c616...	Stable
Node I	localhost	90000	71a13f2c616...	Stable

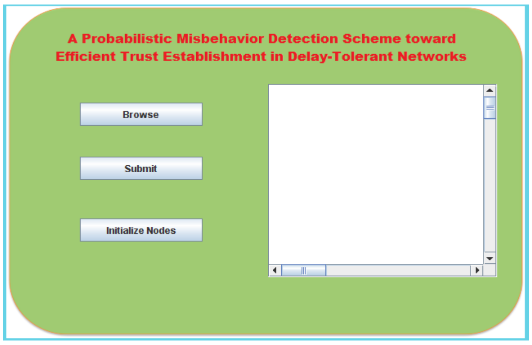
Fig 3.1.2 Node details maintained at the router

There are two steps in the routing evidence generation phase that could be used to judge if a node is a malicious one or not.
a) Delegation task evidence
b) Forwarding history evidence

In the Delegation Task evidence, the message is delegated from node i to node j if node j ..If Nj is the opted next hop delegation task evidence IE^i->j task has to be generated to demonstrate that a new task has been delegated from Ni to Nj. The delegation task evidence is as follows:

IE^i->jtask={IM^i->j M,Sigi,Sigj}

Signatures are generated for the individual nodes to confirm that the destination node has accepted the task. It is done by initializing nodes by the sender .The layout of the sender to browse file to send ,initialize nodes and send it to destination is as shown in the below Fig 3.1.3



A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks

Fig 3.1.3 Layout of sender

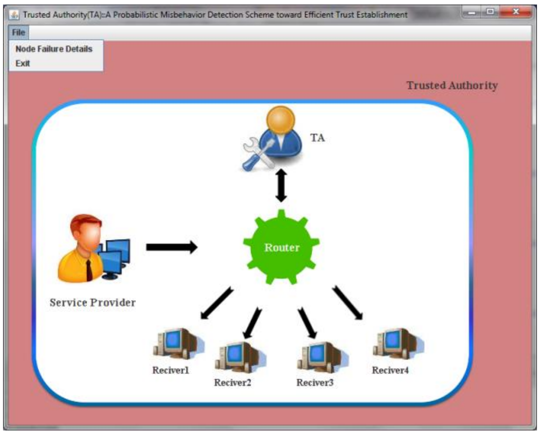
In this phase, TA will establish an investigation request toward node Nj in the global network during a certain period t. Then, given N as the set of total nodes in the network, each node in the network will submit its evidence details to TA. By accumulating all of the evidences related to Nj, TA obtains the set of messages forwarding requests Stask, the set of messages forwarded Sforward, all of which could be verified by checking the corresponding evidences.

Forwarding history evidence IE^$_{\text{j->k forward}}$

Sender will browse file, initialize mac address and finally send file to destination. When node Nj meets the next intermediate node Nk, Nj will suspect if Nk is he desirable next intermediate node in terms of a specific routing protocol. If it is true, then Nj will forward the packets to Nk, who will generate a forwarding history evidence to present that Nj has successfully finished the forwarding task
Algorithm : The Probabilistic Misbehavior Detection algorithm.
Probabilistic misbehavior detection scheme allows the TA to launch the misbehavior detection at a certain probability. The

3.2 Auditing phase

In the auditing phase ,TA will differentiate normal nodes from misbehaving nodes. To verify if a suspected node Nj is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by Nj. The overview of TA task is given in the below figure 4.2 where TA will direct router as which path(receiver) to select .



Trusted Authority(TA)::A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment
File
Node Failure Details
Exit
Trusted Authority
TA
Router
Service Provider
Reciver1
Reciver2
Reciver3
Reciver4

Fig 3.2.1: Layout of TA

To differentiate malicious nodes from normal nodes TA uses the game theory and misbehavior detection method

3.3 iTrust scheme

This section describes the all phases which figures out the operation of TA in detecting the misbehavior of nodes. The Sender will upload file, routing details maintained at the router is used by TA. Node failure details are send to TA. TA will check all the evidence ,gets the information from the routing table and verifies if any attacker is there. Game theory and Probabilistic Misbehaviour detection algorithm is used to detect attackers and alternative path is found. Packets are sent to the destination without any time delay in a efficient way.

advanced iTrust is motivated by the inspection game, a game theoretical model.Here an authority chooses to inspect or not, and an individual chooses to comply or not, For a particular node i, TA will launch an investigation at certain probability If node i could pass the investigation by providing the corresponding evidences, TA will pay node I a compensation w; otherwise, i will receive a punishment C(lose its deposit)

Algorithm1:The Probabilistic Misbehavior Detection algorithm
Step 1:Intialize the number of nodes as node i
Step 2: At a certain probability, TA will ask all the nodes (including node i) to provide

```
        evidence about node i
Step 3:If I could pass investigation by providing evidences
        then
Step 4: TA pays node i the compensation w
Step 5: else
Step 6: TA pays  node i the punishment C
```

Advantages:
Delay tolerance of the network is improved.
Transmission overhead will reduce.
Detection performance increase.

CONCLUSION

A probabilistic misbehavior detection scheme (iTrust) is proposed, which could help to detect the malicious nodes effectively. By an appropriate probability setting TA could assure the security of the DTNs at a reduced detection overhead.

REFERENCES

[1] T. Hossmann, T. Spyropoulos, and F. Legendre, “Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing,” Proc. IEEE INFOCOM ’10, 2010.

[2] Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay-Tolerant Networks,” Proc. IEEE INFOCOM ’10, 2010.

[3] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, “SMART: A SecureMulti-layer Credit-Based Incentive Scheme for Delay-TolerantNetworks,” IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.

[4] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, “SLAB: SecureLocalized Authentication and Billing Scheme for Wireless MeshNetworks,” IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858-3868, Oct. 2008 .

[5] Q. Li and G. Cao, “Mitigating Routing Misbehavior in Disruption Tolerant Networks,” IEEE Trans. Information Forensics and Security,vol. 7, no. 2, pp. 664-675, Apr. 2012.

[6] S. Marti, T.J. Giuli, K. Lai, and M. Baker, “Mitigating RoutingMisbehavior in Mobile Ad Hoc Networks,” Proc. ACMMobiCom ’00, 2000.

[7] R. Lu, X. Lin, H. Zhu, and X. Shen, “Pi: A Practical IncentiveProtocol for Delay Tolerant Networks,” IEEE Trans. WirelessComm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

[8] F. Li, A. Srinivasan, and J. Wu, “Thwarting Blackhole Attacks inDisruption-Tolerant Networks Using Encounter Tickets,” Proc.IEEE INFOCOM ’09, 2009.

[9] E. Ayday, H. Lee, and F. Fekri, “Trust Management and Adversary Detection for Delay-Tolerant Networks,” Proc. MilitaryComm. Conf. (Milcom ’10), 2010.

[10] D. Fudenberg and J. Tirole, Game Theory. MIT Press, 1991.