IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 - 8791
www.ijreat.org

Advanced Trust Establishment among Nodes in DTN using Probabilistic Misbehavior Detection Scheme and Nectar Protocol

D. Durai kumar[1], M.Valarmathi[2]

[1]Associate Professor, Dept. of Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

[2]M.Tech-Information Technology, Ganadipathy Tulsi's Jain Engineering College, Vellore, Tamilnadu, India.

ABSTRACT—*In Delay Tolerant Networks (DTNs), secure data transmission is affected to a great extent because of malicious and selfish behavior of nodes. Due to the distinct characteristics like lack of contemporaneous path, high variation in network condition, designing a misbehavior detection system is considered as a great confront. In order to address this, in this paper we propose a trust model for secure data transmission. Our trust model introduces the periodically available Trusted Authority (TA) to judge the behavior of nodes based on the collected evidences. To further improve the effectiveness of the proposed model, Nectar protocol is used to choose the appropriate intermediate node that has sufficient contacts, such that the probability of packet transmission rate can be improved. We also associate the detection probability with node's reputation for effective inspection.*

Keywords— Nectar protocol, Trusted Authority, Reputation.

1. INTRODUCTION

Delay Tolerant Network is a communication network designed to withstand long delays and outages. The current networking technology relies on a set of fundamental assumptions that are not true in all environments· The first and most important assumption is that an end-to-end connection exists from the source to the destination. This assumption can be easily violated due to mobility, power saving etc. Examples for such networks are sensor networks with scheduled intermittent connectivity, vehicular DTNs that publish local ads, traffic reports, parking information [1] and deep space networks. Delay-tolerant network (DTN) is an attempt to extend the reach of networks. It promises to enable communication between "challenged" networks.

Delay Tolerant Networks have unique characteristics like lack of contemporaneous path, short range contact high variation in network conditions, difficult to predict mobility patterns and long feedback delay. Because of these unique characteristics the Delay Tolerant Networks (DTNs) move to an approach known as "store-carry-and-forward" strategy where the bundles can be sent over the existing link and buffered at the next hop until next link in the path appears and the routing is determined in an “opportunistic” fashion.

In DTNs a node could misbehave by refusing to forward the packets, dropping the packets even when it has the potential to forward (e.g., sufficient memory and meeting opportunities) or modifying the packets to launch attacks. These types of malicious behaviors are caused by rational or malicious nodes, which try to maximize their own benefits. Such malicious activities pose a serious threat against network performance and routing. Hence a trust model is highly enviable for misbehavior detection and attack mitigation.

Routing misbehavior detection and mitigation has been well crammed in traditional mobile ad hoc networks. These methodologies use neighborhood monitoring or destination acknowledgement (ACK) to detect dropping of packets [2]. In the mobile ad hoc networks (MANET) first complete route is established from source to destination, before transmitting the packet. But in DTN the nodes are intermittently connected, hence there is no possibility for route discover and it has other unique characteristics like dynamic topology, short range contact, long feedback delay which made the neighborhood monitoring unsuitable for DTN. Although many routing algorithms [3, 4, 5, 6, 7] have been proposed for DTNs, most of them do not consider the node’s willingness to forward the packet and implicitly assume that a node is willing to forward packets for all others. They may not work well since some packets are forwarded to nodes unwilling to relay, and will be dropped. There are quite a few proposals for misbehaviour detection which are based on forward history verification (e.g., multi layer formation [8]) and by providing encounter tickets [9], which incur high transmission overhead as well as high verification cost. Different from the exiting works in which the Trusted Authority (TA) performs the auditing based on checking the contact history [10], is critical and time consuming. Our proposed system uses nectar protocol for selecting the appropriate intermediate node such that the inspection or auditing process can be simplified and the packet dropping rate can be considerably reduced. To achieve a tradeoff between detection cost and security, our Trust model relies on inspection game [11] based on game theory. This introduces a periodically available Trusted Authority (TA) to judge the nodes based on collected routing evidences. Our Trust model jointly considers the incentive and malicious node detection scheme in the single framework along with the effective nectar protocol for selecting the appropriate intermediate node.

The contributions of this paper can be summarized as follows.

1. We propose a Trust model which demonstrates the selection of appropriate intermediate node by using Nectar protocol.

2. Malicious node detection is carried out by the Trusted Authority (TA) based on the evidences generated by nodes, which are selected by the application of protocol.

3. Hence packet dropping rate can be considerably reduced and the performance of the network can be improved.

2. PROPOSED TRUST MODEL

2.1 SYSTEM MODEL

Each and every node when enters the network, it has to pay a deposit amount (D), the account details and the reputation of every node is maintained by the Trusted Authority (TA). Key distribution takes place with the knowledge of the Trusted Authority. We assume that each node has finite communication range, hence if a node wants to send the data to the one, which is out of the coverage area it has to be transmitted by series of intermediate nodes. Task evidence, forwarding chronicle and contact log are maintained by every node, which is considered as proof for data forwarding. Selection of the intermediate node is carried out by the nectar protocol.

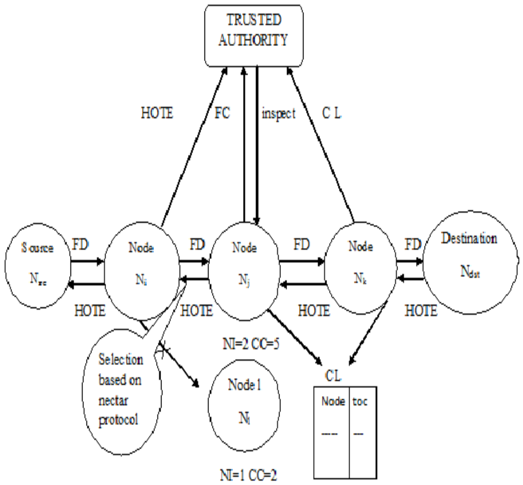

Fig 1: Trust model architecture

HOTE – Hand Over Task Evidence

FD – Forwarding

FC – Forward Chronicle

CL- Contact Log

NI - Neighborhood Index

N_i, $N_{j,}$ $N_{k,}$ $N_{l\,–}$ Intermediate Nodes

CC – Contact Counter

toc- time of contact

3. NECTAR PROTOCOL

Nectar protocol is used for the selection of appropriate intermediate node. The Neighborhood Index calculation is based on recent contact log. The nodes that are frequent neighbours present a high Neighborhood Index. When the nodes N_i and N_j meets for the first time, the Neighborhood Index to each other is assigned to 1. While nodes N_i and N_j are within communication range, the Neighborhood Index and the Contact counter are increased in a linear fashion. Then nodes N_i and N_j update the Neighborhood Index for destinations that are not within communication range. Suppose that node j (N_j) has an improved Neighborhood Index to destination ($N_{dst)}$ [Fig.1] than node l (N_l). In this case, the node l's Neighbourhood Index (NI) to destination (N_{dst}), (N (N_l; N_{dst})) will be computed by the following procedure. We divide Contact (N_j; N_{dst}) counter, which represents the number of time slots that nodes j ($N_{j)}$ and N_{dst} remain in contact by two a distance metric and an aging metric. The distance metric is calculated by adding 1 to Hops (N_j; N_{dst}) counter, which represents the amount of hops between N_j and N_{dst}. The amount of time slots that nodes j ($N_{j)}$ and N_{dst} are out of communication range raised by an aging constant (**σ**) defines the aging metric. The Neighborhood Index formula in Equation(1), favours the delivery of messages to appropriate intermediate node that are near from a destination and have been in contact recently.

$$N\,(N_{l'};\,N_{dst}) = \frac{\text{Contact}\,(N_j;\,N_{dst})}{(\text{Hops}\,(N_j;\,N_{dst}) + 1)\times(TS\text{-}ts\_update + 1)^{\sigma}} \quad \text{----------} \; (1)$$

Where Contact (N_j; N_{dst}) defines the amount of time slots that node i and destination are in contact, Hops (N_j; N_{dst}) express the number of hops required for nodej to reach the destination. TS represents current Time Stamp, ts_update (N_j;N_l) Time Stamp of the last route update from node j to node l.

If node l has already a route to node N_{dst}, and node j has a better Neighborhood Index to node N_{dst}, N (N_i; N_{dst}) will be updated in a weighted fashion. By using this approach, the Neighborhood Index calculation mitigates the impact of new information, and prevents nodes from altering a known Neighborhood Index with data that may have a limited validity. If the Neighbourhood Index is changed, then the associated value is reduced, allowing another neighbor, with a better Neighborhood Index, to be the next hop.

4. ROUTING PROOF GENERATION PHASE

The generated routing proof is used to judge if a node is malicious or not.

4.1 Hand Over Task Evidence Generation $E^{i\to j}_{task}$: Hand Over Task evidences are used to record the number of routing tasks assigned from the upstream nodes to the target node N_j.We assume that source node (N_{src}) has message M, in order to forward to the destination (N_{dst}). For simplicity of presentation ,consider that message is stored at the intermediate node (N_i), when N_j comes within the transmission or radio range of N_i ,then it will determine by means of nectar protocol whether to choose node j(N_j) as the intermediate node or not, in order to forward message M to the destination. If node j (N_j) is the chosen next node then the flag bit will be enabled (or *flag* = 1) and the Task evidence $E^{i\to j}_{task}$ need to be generated, to demonstrate that a new task has been assigned from node i (N_i) to node j (N_j). Where T_{ts} and T_{Exp} refer to the time stamp and the expiration time of the packets. We set $M^{i\to j}_{M}$= {M, Nsrc, flag, N_i, N_j, N_{dst}, T_{ts}, T_{Exp}, and Sig_{src}} where Sig_{src} = Sig_{src} (H (M, N_{src}, N_{dst}, T_{Exp})) refers to the signature generated by the source nodes on message M. Node N_i generates the signature Sig_i=$SIG_i\{M^{i\to j}_{M}\}$ to indicate that this forwarding task has been delegated to node N_j. while node N_j generates the signature Sig_j=$SIG_j\{M^{i\to j}_{M}\}$ to show that N_j has accepted this task. Therefore, we obtain the hand over Task Evidence as follows:

$$E^{i\to j}_{task} = \{M^{i\to j}_{M} , Sig_i, Sig_j\} \quad (1)$$

4.2 Forwarding Chronicle generation $E^{j\to k}_{forward}$:

When N_j meets the next intermediate node N_k, N_j will check if N_k is the suitable next intermediate node in terms of Nectar routing protocol. If yes, N_j will forward the packets to N_k, who will generate a forwarding history evidence to show that N_j has successfully finished the forwarding task. N_k will generate asignature Sig_k = SIGk {H ($M^{j\to k}_{M}$)} to demonstrate the authenticity of forwarding history evidence. Therefore, the complete forwarding history evidence is generated by N_k

$$E^{j\to k}_{forward} = \{M^{j\to k}_{M} , Sig_k\} \quad (2)$$

In the audit phase, the node which is inspected will submit its forwarding history evidence to TA to demonstrate that it has tried its best to accomplish the routing tasks, which are defined by hand over task evidences.

4.3 Contact log generation $E^{j\leftrightarrow k}_{contact}$:

Whenever two nodes meet, a new contact log is generated and the neighbourhood index is updated accordingly. Each node also maintains a contact counter, which keeps track of how often the nodes meet each other. When two nodes N_j and N_k meet, a new contact log $E^{j\leftrightarrow k}_{contact}$ will be generated. Suppose that $M^{j\leftrightarrow k}$ = {N_j ,N_k, T_{ts}}. N_j and N_k will generate their signatures Sig_j = SIG_j {H ($M^{j\leftrightarrow k}$)} and Sig_k = SIG_k{H ($M^{j\leftrightarrow k}$)}. Therefore, the contact history evidence could be obtained as follows

$$E^{j\leftrightarrow k}_{contact} = \{M^{j\leftrightarrow k}, Sig_j, Sig_k\} \ (3)$$

The contact log will be stored at both of meeting nodes. In the audit phase both the nodes will submit their logs to the TA. Maintenance of contact history could prevent the blackhole or greyhole attack.The nodes chosen by the nectar protocol with sufficient contact with other users, but if it fails to forward the data, will be regarded as a malicious or selfish one.

5. AUDITING PHASE

Since the selection of intermediate node is based on the Nectar protocol, the dropping rate of packect is reduced considerably. Inorder to further improve the network performance and to avoid packet dropping, our trust model introduces the Trusted Authority (TA), which periodically launches the ivetigation request.

In the auditing phase, the Trusted Authority (TA) will send the investigation request to node N_j in a global network during a certain period [t1, t2]. Then, given N as the set of nodes in the network, each node in the DTN will submit it's collected {$E^{i\to j}_{task}$, $E^{j\to k}_{forward}$, $E^{j\leftrightarrow k}_{contact}$} to TA. After collecting all of the evidences related to N_j , TA obtains the set of task evidence S_{task}, the set of messages forwarded $S_{forward}$ and the set of contacted nodes $S_{contact}$. To check if a suspected node N_j is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by N_j.

6. ALGORITHM FOR MALICIOUS NODE DETECTION AND ATTACK MITIGATION

The TA judges if node N_j (Suspected node) is malicious or not by triggering the Malicious node detection algorithm. Where node j is the suspected malicious node, S_{task} is the set of hand over task evidence, $S_{forward}$ is the set of forward chronicle, and R is the set of contacted nodes, N_k (m) as the set of next-hop nodes chosen for message forwarding, C represents the punishment (lose of deposit), w denotes the compensation (virtual currency or credit) paid by TA.

Algorithm 1 The malicious node detection algorithm

```
procedure BASICDETECTION ((j, $S_{task}$, $S_{forward}$, [t1, t2], R))
    for each m $\in S_{task}$ do
        if m $\notin S_{forward}$ then
            return 1
        then
            give a punishment C to node j
        else
            pay node j the compensation w
        else if m $\in S_{forward}$ and $N_k$ (m) $\not\subset$ R then
            return 1
        then
            give a punishment C to node j
        else
            pay node j the compensation w
        end if
    end for
    return 0
end procedure
```

7. PROBABILITY FIXING INSPIRED BY GAME THEORY.

There are two strategies available for the trusted authority and the nodes. The Trusted Authority can choose inspecting (I) or not inspecting (N). Each node also has two strategies, forwarding (F) and offending (O).

Theorem : If TA inspects at the probability of $P_b = g+\varepsilon/w+C$ in Trust Model, a rational node must choose forwarding strategy, and the TA will get a higher profit than it checks all the nodes in the same round.

Proof: This is a static game of complete information, though no dominating strategy exists in this game, there is a mixed Nash Equilibrium point.

If the node chooses offending strategy, its payoff is

$$\pi_w(S) = -C \cdot (g + \varepsilon/w + C) + w \cdot (g + \varepsilon/w + C)$$
$$= w - g - \varepsilon \qquad (4)$$

If the node chooses forwarding strategy, its payoff is

$$\pi_w\,(W) = P_b \cdot (w - g) + (1 - P_b) \cdot (w - g) = w - g \quad (5)$$

The latter one is obviously larger than the previous one. Therefore, if TA chooses the checking probability $g+\varepsilon/w+C$, a rational node must choose the forwarding strategy.

Furthermore, if TA announces it will inspect at the probability P_b = $g+\varepsilon/w+C$ to every node, then its profit will be higher than it checks all the nodes, for

$$v - w - (g + \varepsilon/w + C) \cdot h > v - w - h \quad (6)$$

the latter part in the inequality is the profit of TA when it checks all the nodes.Note that the probability that a malicious node cannot be detected after k rounds is $(1- g+\varepsilon/w+C\ )^k \rightarrow 0$, if $k\rightarrow\infty$. Thus it is almost impossible that a malicious node cannot be detected after a certain number of rounds. By using the Nectar protocol itself we avoid the packet lose probability**.** Hence effective detection can be carried out by our trust model.

8. REPUTATION SCHEME

We also correlate the probability of inspection with node's reputation. Reputation is maintained by the TA. The node with good reputation will be checked with lower probability and the node with bad reputation will be checked with higher probability.

9. CONCLUSION

In this paper we propose a Trust Model which could effectively detect the malicious node and ensures secure transmission of data. The selection of neighbour node is based on Nectar protocol, by which the packet dropping rate is considerably reduced and it also simplifies the work of Trusted Authority (TA). We also reduce the detection overhead by introducing the Trusted Authority (TA) designed on the basis of inspection theory, in a periodic fashion.

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] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehaviour in mobile ad hoc networks, in Proc. *ACM MobiCom'06*, 2000.

[3] A. Lindgren, A. Doria, O. Schelen, Probabilistic routing in intermittently connected networks, ACM SIGMOBILE CCR 7 (3) (2003) 19–20.

[4] J. Burgess, B. Gallagher, D. Jensen, B. Levine, Maxprop: Routing for vehicle-based disruption-tolerant networks, Proc. INFOCOM, 2006.

[5] E. Daly, M. Haahr, Social network analysis for routing in disconnected delay-tolerant MANETs, Proc. MobiHoc, 2007, 32–40.

[6] A. Balasubramanian, B. N. Levine, A. Venkataramani, Dtn routing as a resource allocation problem, Proc. ACMSIGCOMM, 2007.

[7] P. Hui, J. Crowcroft, E. Yoneki, Bubble rap: social-based forwarding in delay tolerant networks, Proc. MobiHoc, 2008.

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

[9] F. Li, A. Srinivasan and J. Wu, "Thwarting Black hole Attacks in Disruption-Tolerant Networks using Encounter Tickets," in Proc. of *IEEE INFOCOM'09*, 2009.

[10] Haojin Zhu, *Member, IEEE,* Suguo Du, Zhaoyu Gao, *Student Member, IEEE*, Mianxiong Dong, *Member, IEEE*, and Zhenfu Cao, *Senior Member, IEEE* "A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks"

[11] Fudenburg, "Game Theory", p17-18, example1.7: inspection game.