Distributed Misbehavior Detection Scheme for Delay Tolerant Networks

Lalit Kulkarni, Jagdish Bakal, Urmila Shrawankar

Abstract: ***Opportunistic forwarding mechanism in Delay Tolerant Networks (DTN), are prone to get disconnected from the nodes in the network. These types of networks deal with intermittent connectivity, large delays.Existing routing protocols of DTNs fights with these issues, but fail to integrate the security available for delay tolerant networks,it is necessary to design a secure routing protocol to overcome these issues. There are centralized Trust Authority (TA) based security systems but the disconnection or failure of TA, affects the security model and network performance. It becomes crucial to have the distributed approach for security system and have multiple TAs working on security model. This reduces the possibility of poor network performance. The paper presents a distributed misbehavior detection system, and implements multiple TAs for implementing the security model for DTN.***

Keywords: Delay Tolerant Networks, DTN, Trust based scheme

I. INTRODUCTION

Delay Tolerant Network (DTN) communication is used whenever traditional networks fail to deliver the data. DTNs are helpful and the best solution to the intermittently connected devices. DTN uses store-carry-forward mechanism to deliver the data to the destinations. In this process the source node has to rely on multiple intermediate nodes and trust their forwarding and cooperating abilities [1-4]. This poses a significant problem of security in DTN. Performance of DTN increases with the cooperation intermediate nodes. To motivate the cooperation among the DTN nodes, some incentives should be offered to forwarding DTN nodes. On the other hand the forwarding DTN node should also trust the next node so as to maximize the delivery probability. This can be achieved only if there is trust management system working along with the incentive schemes [5].

DTNs can be used in various applications like battlefield networks, disastrous networks, vehicular ad-hoc networks, under water networks, etc. The routing in DTN becomes the center of attraction for the researchers due to wide areas discussed above [6]. But the routing behavior has been neglected by the research community [7-8]. DTN nodes can drop packets to save energy or with some intention to affect the original data. This kind of behavior is dangerous for DTN.

In this paper the distributed approach of malicious detection scheme is used to provide the security. The scheme is named as Distributed Misbehavior Detection System (DMDS). The scheme evolves around the trust based strategy, which contributes to the increased security of DTN and shows better performance over other similar security scheme.

II. RELATED WORK

DTNs are prone to get disconnected from the nodes in the network. These types of networks deal with intermittent connectivity, large delays [2]. This is explained in Figure 1. Securing such types of network is one of the critical issues apart from routing issues. There are many security algorithm and secure routing protocols for the normal wireless networks. But these protocols do not work for DTNs.

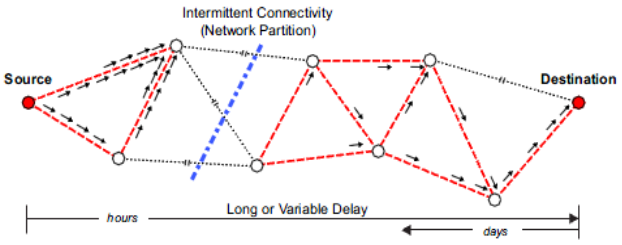

Figure 1. Delay Tolerant Networks

Malicious and selfish behaviors represent a serious threat against routing in delay/disruption tolerant networks (DTNs). The author proposesiTrust [2], a probabilistic misbehavior detection scheme (PMDS), for secure DTN routing toward efficient trust establishment.iTrust introduces a centrally available Trusted Authority (TA) to judge the node’s behavior based on thecollected routing evidences and probabilistically checking. TA could ensure the security of DTN routing at a reduced cost.PMDS improves the efficiency of the scheme,but the only problem with centralized approach is that if TA is disconnected the security scheme fails.

Revised Manuscript Received on July 25, 2019.

Lalit Kulkarni, JagdishBakal, Urmila Shrawankar
G. H. Raisoni College of Engineering, Nagpur, MS, India

Retrieval Number: I32830789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3283.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Trust has been widely used as a security scheme in the World Wide Web in different ways, trust between devices must be ensured by methods utilizing trust as a tool for DTN security [9]. MobiGameis another security protocol against selfish nodes, which is also credit based and game theory-based approach, user-centric and social-aware reputation incentive scheme that works on fairness. ConSub works to overcome selfish behavior of the node by use of TFT (Tit-For-Tat) mechanism. Selfish nodes are forced to behave properly as ConSub system reacts in the same way [10].

Pham et.al. proposed a piggyback method to identify multiple attacks related to the black hole, gray hole and flooding attack in DTNs [11]. Multiple attacks were detected by utilizing the encounter record technique with rate limit. Limitation of the algorithm is its detection time and cost [12-13].

III. SECURE ROUTING SCHEME

As shown in the Figure 2, there is a pool of trust authorities (TA) working in a group. The nodes participating in the communication on message forwarding have to create the credit history of the message forwarding work they are doing. As explained in Table 1, the DTN nodes i *and j* maintain the contact history$H_C{}^{i-j}$. These records are maintained by each node along with their destinations.

$$H_C{}^{i-j} = \{N_i,\ N_j,\ N_{src},\ N_{dst},\ T_j\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [1]$$

This will help DTN nodes to choose next nodes for data forwarding. When each nodes learns about the neighbor nodes, nearest TA provides the list of available trusted nodes N_a. Source node N_{src} then creates n copies of messages to forward. After receiving the contact history the node B forwards the message m to node C. The forward history $H_F{}^{i-j}$ is shared with the neighbor node A.

$$H_F{}^{i-j} = \{M,\ N_{src},\ N_{dst},\ N_i,\ N_j,\ t_i,\ Sig_{src}\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [2]$$

In this communication node A acts as a witness. Once the node C receives the forwarded message from B, it shares $H_{FV}{}^{i-j}$with node A and subsequently node A confirms forward history $H_{FC}{}^{i-j-k}$. The same record is forwarded by the node A to the nearest TA as a witness history. This process continues till the actual messages gets delivered to the destination node N_{dst}. Once the destination node confirms the message delivery to the nearest TA, it checks the integrity of all the witness histories and issues the trust value as per the algorithm 1. The contents of all the histories are as explained in the following equations. Each DTN node adds its signature to the history record so as to maintain the integrity of the witness history received at the TA.

$$H_{FV}{}^{i-j} = \{m,\ N_i,\ N_k,\ Sig_j\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [3]$$

$$H_{FC}{}^{i-j-k} = \{H_{FV},\ Sig_k\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots [4]$$

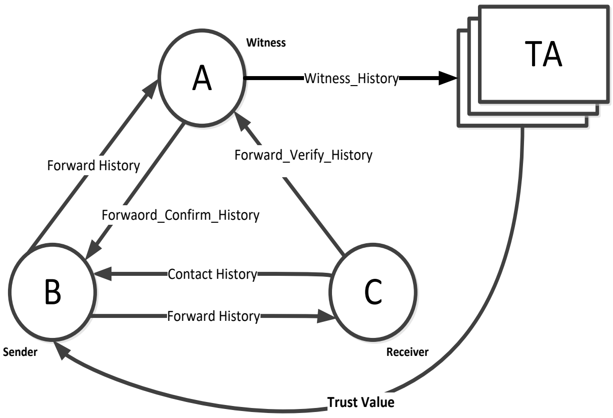

Figure 2. Distributed misbehavior detection system

The algorithm explains the steps involved in detection of malicious nodes. The algorithm maintains the Trust Property *(X)* which is the function of three variables Unselfishness (u), Connectivity(c) and Energy (e).

Trust Property

$$X = \{u, c, e\} = \begin{cases} 0, & No\ Trust \\ x, & Fractional\ Trust \\ 1, & Complete\ Trust \end{cases} \text{-----------------} \text{------} [5]$$

From the value of X, Trust T_t is calculated as bellow.

Trust T_t = Weighted Average of X at time t

$$T_t = \textstyle\sum_{i=0}^{t} X_i/t \text{------------------------------} [6]$$

There are three cases of the node being malicious. These cases are discussed here.

Case I: As explained in algorithm, the number of available trusted nodes and the no of forwarded messages should be equal in normal message forwarding. If any node from $N_a$does not keep this message in its buffer then it has to be detected as a malicious node. This can be detected in the step 4. As soon as the node is detected as malicious node, the trust value of this node has to be reduced. It is reduced by Trust Update∇t. It is calculated as follows.

$$\nabla t = w.T_t \text{ ----------------------------} [7]$$

Where $w =\ 0.05, 0.1, 0.15, 0.2$

The weight w is the factor with which the trust update value increases or decreases. It takes the initial value of 0.05 and for further rounds of the activities in takes other values as 0.1, 0.15, 2.

Table I: Terminology

Notation	Description
n	$\lvert N_a \rvert$ No. of copies sender node have created
N_a	Set of available trusted nodes for forwarding message
M_{id}	Message id
N_{src}	Source Node
N_{dst}	Destination Node
Sig_i	Signature of Node i
m	Message $\{M_{id}, N_{src}, N_{dst}\}$
R	Set of nodes needed for routing
S_f	Set of forwarded messages
T_i	Trust of a node i
∇t	Trust Update
t_i	Contact time of node i
${H_C}^{i-j}$	Contact History of node $i$and j
${H_F}^{i-j}$	Forward History of message from node $i$to j
${H_{FV}}^{i-j}$	Forward Verify History of message from node $i$to j
${H_{FC}}^{i-j-k}$	Forward Confirm History by k^{th}nodeof message from node $i$to j
u	Unselfishness of a node
c	Connectivity a node
e	Energy a node
X	Trust Property $\{u, c, e\}$

Case II: Further if message is not available in the forward verify history, then also the node is malicious and can be detected as per the step 7 of the algorithm. This situation can happen when a node does not want to verify the message delivery of the other nodes.

Case III: If the routing protocol requires to create R copies of the messages to forward, but if the number of messages created (n) are less than the no. of copies that are created then the node can be treated as malicious node.

If a node does not belong to any of the above category then that node will be treated as a normal which helped in message forwarding and should be given a credit with an increased trust value as per the step no 14 of the algorithm.

Algorithm I

```
1.  procedure DMDS
2.  { ${H_F}^{i-j}$, ${H_C}^{i-j}$, $[t_1, t_2]$, $N_a$, $S_f$}
3.  forEach$m \in S_f$ do
4.  if$|S_f| < |N_a|$then
5.  $T_i = T_i - \nabla t$
6.  return 1
7.  else if $m \nexists H_{FV}$ then
8.  $T_i = T_i - \nabla t$
9.  return 1
10. elseif$|R| = |S_f|$ and $n < |R|$then
11. $T_i = T_i - \nabla t$
12. return 1
13. else
14. $T_i = T_i + \nabla t$
15. return 0
16. end for
17.    end procedure
18. end procedure
```

IV. SIMULATION SETUP AND RESULTS

Opportunistic Network Environment (ONE) is used as a network simulator to implement the algorithms. There are different scenarios in which the network environment is tested. The parameters of the network are as shown in Table 2. The DMDS algorithm is compared with the security scheme discussed in earlier section PMDS.

Table 2: Network Parameters

Parameter	Value
No. of DTN Nodes	50, 100, 150
No. of TA Nodes	8, 16. 24
Mobility Model	Random Map Based Route
Area	2 Km x 2 Km
Message TTL	480 min (8 hours)
Message sizes	1MB to 5 MB
Node Buffer	100 MB

As shown in Figure 3 the delivery ratio is higher than PMDS until the malicious nodes % reaches 50%. If the % malicious nodes is higher than 50% bothalgorithmsbehave similar. Figure 4 shows the comparison of both algorithms on the basis of malicious nodes detection. The graph clearly shows that DMDS detection rate is higher than PMDS. But DMDS fails to detect the nodes if malicious nodes increase and are more than 50% of the total number of nodes in DTN.

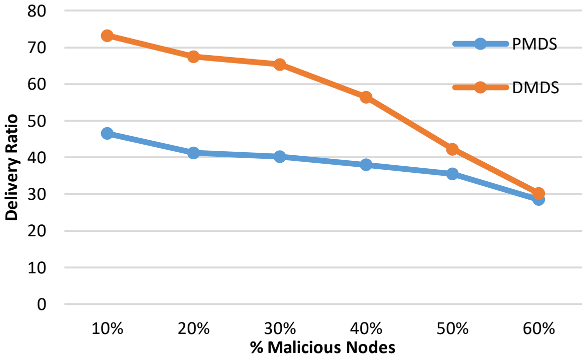

Figure 3. Delivery ratio

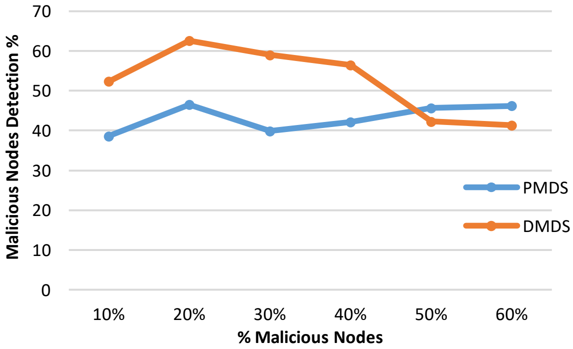

Figure 4. Malicious nodes detection

Figure 5 and 6 shows the comparison of two algorithms on the basis of Delay and delivery latency. Delay for DMDS is almost 30% lesser than PMDS. And average delivery latency is also 10% less than PMDS. But it is not consistent. The average delivery latency behaves abnormally when the number of messages are abruptly increased. As shown in Figure 6, when 20% malicious nodes are in the network the message creation event generated high number of messages. This is to check the effect of high message overhead on the algorithm.

V. CONCLUSION

The security provision to DTN is a critical issue and the DMDS algorithm provides the necessary security to DTNs. The security scheme uses the distributed approach over a centralized approach of the trust authority. Instead of one trusted authority, multiple trust authority works in a distributed approach, and can improve the performance of the security scheme. The algorithm performs better than PMDS for delivery ratio, malicious detection rate, delay and average latency. Although the DMDS algorithm fails to perform better than PMDS with larger malicious nodes, as over 50%. Which is a very rare case in DTNs. This can be improved if the security algorithm is integrated with the existing routing protocol. The integration of the routing protocol and a security scheme will also be improved on delivery ratio and detection of malicious activities in all situations.

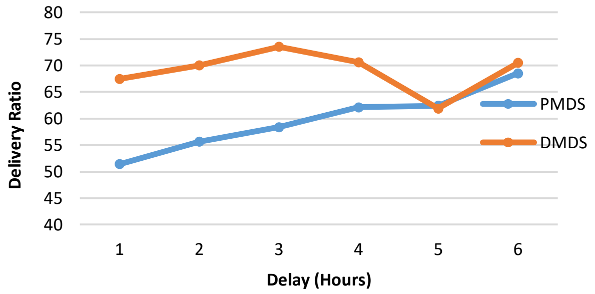

Figure 5. Delivery Ratio and Delay

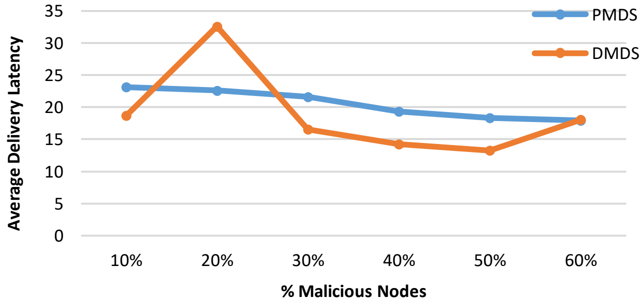

Figure 6. Average delivery latency

REFERENCES

[1] P. Asuquo, H. Cruickshank, C. P. A. Ogah, A. Lei and Z. Sun, "A Distributed Trust Management Scheme for Data Forwarding in Satellite DTN Emergency Communications," in IEEE Journal on Selected Areas in Communications, vol. 36, no. 2, pp. 246-256, Feb. 2018.

[2] H. Zhu, S. Du, Z. Gao, M. Dong and Z. Cao, A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks, IEEE Transactions on Parallel and Distributed Systems, pp 22-32, vol. 25, no. 1, January 2014

[3] L. Kulkarni, D. Mukhopadhyay and J. Bakal, "Analyzing Security Schemes in Delay Tolerant Networks." In Proceedings of the International Conference on Data Engineering and Communication Technology (pp. 613-620). Springer Singapore, March 2016

[4] L. Zhang, J. Song and J. Pan, "A Privacy-Preserving and Secure Framework for Opportunistic Routing in DTNs," in IEEE Transactions on Vehicular Technology, vol. 65, no. 9, pp. 7684-7697, Sept. 2016.

[5] H. Chen, W. Lou, Z. Wang and Q. Wang, "A Secure Credit-Based Incentive Mechanism for Message Forwarding in Noncooperative DTNs," in IEEE Transactions on Vehicular Technology, vol. 65, no. 8, pp. 6377-6388, Aug. 2016.

[6] M. N. M. Bhutta, H. Cruickshank and Z. Sun, "Public-key infrastructure validation and revocation mechanism suitable for delay/disruption tolerant networks," in IET Information Security, vol. 11, no. 1, pp. 16-22, Jan 2017.

[7] T. N. D. Pham and C. K. Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks," in IEEE Transactions on Mobile Computing, vol. 15, no. 5, pp. 1116-1129, May 2016.

[8] Y. Cai, Y. Fan and D. Wen, "An Incentive-Compatible

Routing Protocol for Two-Hop Delay-Tolerant Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 1, pp. 266-277, Jan. 2016.

[9] Z. Li, Y. Liu, H. Zhu and L. Sun, "Coff: Contact-Duration-Aware Cellular Traffic Offloading Over Delay Tolerant Networks," in IEEE Transactions on Vehicular Technology, vol. 64, no. 11, pp. 5257-5268, Nov. 2015.

[10] L. Kulkarni, N. Ukey, J. Bakal and N. Chavan, “A Survey on Energy-Efficient Techniques to Reduce Energy Consumption in Delay Tolerant Networks”. In Computing and Network Sustainability (pp. 83-91). Springer, Singapore, July 2017

[11] X. Lv, Y. Mu and H. Li, "Loss-Tolerant Bundle Fragment Authentication for Space-Based DTNs," in IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6, pp. 615-625, Nov.-Dec. 2015.

[12] S. Eshghi, M. H. R. Khouzani, S. Sarkar, N. B. Shroff and S. S. Venkatesh, "Optimal Energy-Aware Epidemic Routing in DTNs," in IEEE Transactions on Automatic Control, vol. 60, no. 6, pp. 1554-1569, June 2015.

[13] J. Zhou, X. Dong, Z. Cao and A. V. Vasilakos, "Secure and Privacy Preserving Protocol for Cloud-Based Vehicular DTNs," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1299-1314, June 2015.

Retrieval Number: I32830789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3283.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication