International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 2 Issue 4 ‖ April. 2013 ‖ PP.23-27

Minimized Delay and Adversary Detection in DTNs

P.Srilega, Nagajothi M.E.

[1]*Student, M.E Computer Science & Engineering Karpagam University Coimbatore, Tamil Nadu.*
[2]*Assistant Proffessor, Computer Science & Engineering Karpagam*
University Coimbatore, Tamil Nadu

ABSTRACT: *Adversary detection in DTNs is very useful for scores of applications such as military, satellite and interplanetary, disaster rescue. The Disruption Tolerant Networks (DTNs) turn out to be vulnerable while the legitimate nodes are compromised and the adversary modifies delivery metrics of the node. The traditional Reputation based Trust Management mechanisms are not an effective way to handle such kind of attacks. In this paper, we have analyzed the nodes based on their behaviors during their past interactions and misbehavior due to adversaries attack. The proposed scheme TRMM (Threshold and Reputation Management Mechanism) can effectively improve the secured communication in DTNs. It takes into consideration of reputation value correlated between clusters of neighborhood nodes. It outperforms the typical reputation based trust management used in MANETs and provides high packet delivery ratio.*

Keywords: *Delay, DTNs, Adversary, malicious nodes, Reputation, Packet Delivery Ratio*

INTRODAUCTION

Delay/Disruption Tolerant Networks are occasionally connected networks and characterized by sporadic contact between nodes. Due the explosion in the evolution of wireless devices, enormous infrastructures have been emerged. Some of the applications include disconnected remote village, e-governance, telemedicine, Battlefield warfare, disaster rescue, DieselNet etc, Like MANETs, the nodes can be easily deployed and they do not need permanent infrastructures. Intermediate nodes always wait for opportunities to forward data towards destination. In which, if a path is interrupted the same path or alternate one is re-established rapidly. DTNs may feature dedicated relay or infrastructure nodes. Nodes in such DTNs often associated with other nodes in routing decisions and forwarding their messages. The tremendous increase of wireless devices ultimately increases the challenges that previously not exist in DTNs. Specifically large delays, intermittent connectivity and the absence of end to end path.

Most of the recent research focus on Byzantine (insider) adversary may pose a serious threat against DTN to compromise the network performance. A Byzantine adversary can do serious damage to the network in terms of data availability, latency, and throughput. The most common problems include dropping, modifying the legitimate packets and injecting fack packets. It may also try to maximize their personal benefits by enjoying the services provided by the DTN network.

In this paper, we propose TRMM, Threshold and Reputation Management Mechanism for DTN, to detect misbehaviors and attain accurate detection cost and performance. TRMM is motivated by the Voting based techniques in clusters of Neighborhood nodes. In which, each node maintains the reputation values calculated based on the packet delivery ratio.

DTNs

DTNs have been identified as a newly emerging network which usually deals with communications in extreme challenging environments such as, Vehicular ad hoc networks, Planetary/Interplanetary, Disaster Response, Underwater sensor networking and Satellite Networks. In these environments, the continuous end – to – end paths between the source and the destination are usually unguaranteed. Some the problematic architecture in DTNs are,

- The end to end path between the source and destination exists only during certain period of time.
- Retransmission based on timely and stable feedback is not available and not reliable.
- Packet loss is relatively high in end to end path.
- Fixed stations and routers are not available and do not support TCP/IP.
- Security mechanisms such as Reputation based management mechanisms are not sufficient for meeting security concerns.

The DTNs envisage security mechanisms that protect the infrastructure from unauthorized use. It is not acceptable for an unauthorized user to flood the network that cause the authorized user suffers with denying services.

DTNs can generally be classified as two broad types – hierarchical and flat topologies. A hierarchical DTN, few network nodes at the top of the hierarchy control a larger number of nodes at the lower layers in a tree structure. Flat topology DTNs, where there is no distinction between the nodes.

Security in disruption tolerant networks can be divided into two categories, namely end-to-end security and intermediate-hop security. End-to-End security in DTNs deal with providing security for sender-receiver. Intermediate hop security deals with security between security-aware nodes. The original solutions for secured communication in DTNs are, 1) Identity based encryption, where the nodes receive information in encrypted form by public key 2) Tamper-evident tables with a gossiping protocol.

CLUSTERING IN DTNS

Clusters are the set of nodes grouped together. Each node in a cluster has similar properties. It is derived depends upon the objective that aims to achieve. Clusters are constructed by electing cluster heads. Non-cluster nodes joined and become members of clusters in which the node with highest priority is selected as cluster head. Distributed clustering algorithm used to form a cluster in delay tolerant mobile network. Most of the clustering algorithms used the distance measure between data points. True contact probability is maintained between the nodes of the clusters. Subsequently, a set of functions including Syn(), Leave(), and Join() are devised to form clusters and select gateway nodes based on nodal contact probabilities. Cluster table consists of Node ID, Cluster ID, Destination ID and Time stamp etc. The problem in clustered network is that they unable to contact the other neighborhood nodes with accurate contact probabilities. As a result the nodes often delayed in delivering the packets of data. If nodes grouped under a same cluster have the maximum chance to contact. If nodes are in the different cluster they had very less choice to contact even in the multi – hop routing scheme. Due to the loosely connected network, packet dropping probability is high. The contact probabilities of all nodes that entered in communication are maintained on the gateway table.

Cell radii can very from tens of meters in buildings, and hundreds of meters in cities, up to tens of kilometers in the countryside. The shapes of the cells are never perfect circles or hexagons as shown in the **Fig.1.**

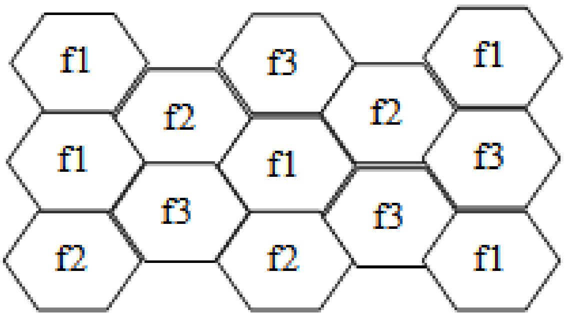
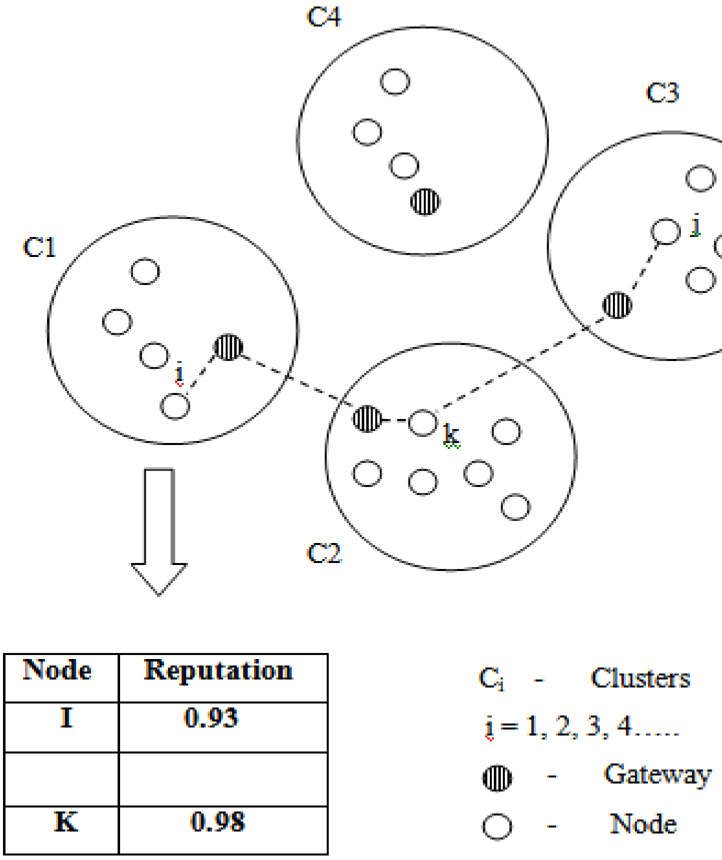


Fig.1. Clustering of cells

But depend on the environment (buildings, mountains, valleys etc.), on weather conditions, and sometimes even on system load. Typical systems using this approach are mobile telecommunication systems, where a mobile station within the cell around a base station communicates with this base station and vice versa. All cells within a cluster use disjointed sets of frequencies (f1, f2,f3). In real transmission, the pattern looks different. The hexagon pattern is the simple way of representation and which shows the repetition of frequencies clearly. The transmission power of a sender has to be limited to avoid interference with the next cell using the same frequencies. To reduce interference sectorized antennas are used.

IV. THRESHOLD AND REPUTATION MANAGEMENT MECHANISM

The proposed scheme TRMM, Threshold and Reputation Management Mechanism which evaluates the nodes based on their behavior during their past interactions within cluster. The scheme detects non-cooperating nodes which reacts for Byzantines attacks. The resultant scheme would effectively provide high data availability and packet delivery ratio. TRMM is motivated by the Voting based techniques in clusters of Neighborhood nodes. If nodes i and j are in the same cluster, they can directly communicate each other. If they are not on the same cluster, lookup table of gateway is referred by node i.



Node	Reputation
I	0.93
K	0.98

Fig2. TRMM in DTNs Clusters

Let consider Fig2. In which node i of cluster C1 send data message to the gateway and finds the intermediate node k of cluster C2. Node k now forwards the data to node j of C3. There is no transaction happened at C_4.In which, each node maintains the reputation(R) value of other nodes calculated based on packet delivery ratio. The packet delivery ratio (PDR) is calculated by number of legitimate packets sent and no of legitimate packets received by a node.

PDR = No of legitimate packet received/
No of legitimate packets sent *100

A. Inspecting the Transmitter node

In this phase, auditing records of the neighbor nodes are examined and reputation can be exchanged along with its routing table. For example, Node i wants to deliver the packets to Node j on the remote cluster. They pick up an intermediate Node k. First of all, the reputation Ri is tested with all the neighbors in the same cluster and updated. Any node has reputation below τ cannot continue its transmission. As the next step node delivers the packet to intermediate nodes through gateway, it goes for waiting stage until receiving the acknowledgement. The ACK consists of {Info, i,, k, j, ts}. Info refers message and ts refers time slice. The Algorithm 1 specifies the entire process done for choosing the appropriate transmitter node.

Algorithm 1: Inspect a Transmitter node i

```
Initialize all the nodes of cluster
Demand all neighborhood nodes to exchange Ri, Di, Fi
Ri = Compute (Rpast, Di, Pi,Fi,α)
update Node i's routing table
if Ri < = τ then
i establish connection with k
else
stop
```

Di,Pi indicates the delivery probabilities and past interactions respectively. Compute function computes and updates the reputation value of node ie.

B. Computing Reputation Value of intermediate node

The reputation value is in the range of [0, 1]. The lower the value of Reputation, Higher the probability that the node is a malicious node.

Initially $R_{i,k}$ = No of legitimate packet received/
No of legitimate packets sent

The recent reputation value of node i that enters with node k in order to transfer a packet to node j can be updated as follows,

$R_{i,k}= (R_{i,k\,(past)} + R_{k,j})*\alpha$

α is the initial constant. We assumed it as 0.5

Algorithm 2 Find Adversary Node

```
1. choose an intermediate node k
2.  if  reputation Rk> $\tau$ then
3.  choose k to store and forward data
4.  Compute and update $R_{i,k}= (R_{i,k\,(past)} + R_{k,j})*\alpha$
5. else
6. anounce k is an adversary node
7 .end if
```

C. Testing with Threshold

As the algorithm 2 suggest Threshold values can be set and compared with reputation of each node that entered on the connection.

$R_{i,k} > \tau$

τ refers threshold value. $R_{i,k}$ cannot continue to transfer the packets if it goes below τ . Threshold value is locally defined by analyzing the previous performance of all the nodes in a cluster.

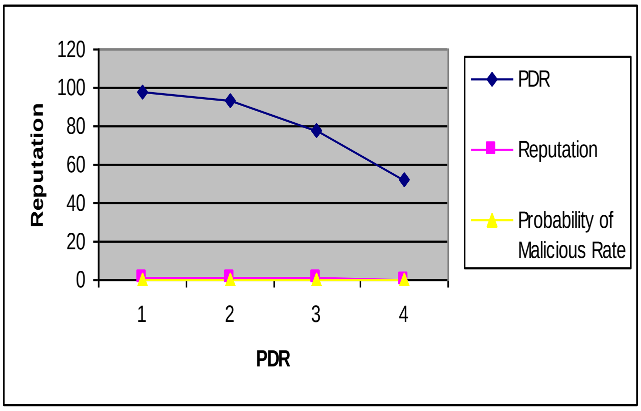
V. SIMULATION

The evaluation of DTNs environment is performed by using Network simulator -2. We assumed a node i source node which has sent 60 data packets and received acknowledgement for 56 data packets from k at the given time then PDR is 56/60 *100= 93.33. Initial value of $R_{i,k} =$ 0.93.In the next step, when 55 out of 56 packets transferred from node k to the destination node j,

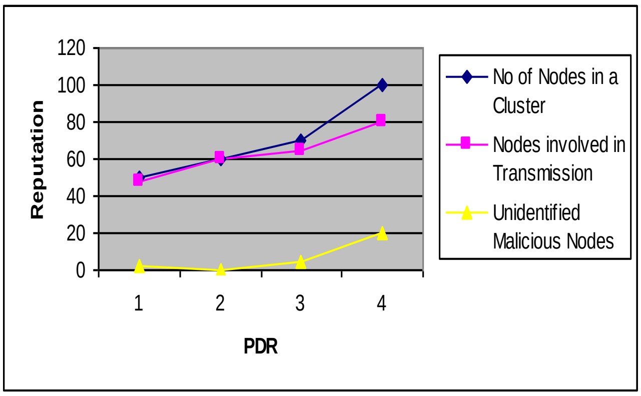
$R_{i,j}$ =(0.93 +0.98)*0.5= 0.95

Now 0.95 is updated as the latest reputation value of i in the node i's routing table. Higher the packet delivery ratio, higher the value of reputation.

We use Packet Delivery Ratio(PDR) to evaluate the misbehavior level of a malicious node. PDR denotes the ratio between dropped packets and received packets. If PDR goes below 50, it is completely a malicious node. In our experiment, we have shown the unidentified malicious nodes. It occurred because of sudden packet dropping of that node. By calculating this false rate we can improve the performance of the network.



(a) Detection of Malicious Nodes



(b) Unidentified Malicious Nodes
Fig. 3. Malicious Node Rate Detection using PDR value

We use malicious node rate to denote the identified malicious nodes. In Fig.3.,We have specified with different packet delivery ratio and reputation values 0.98, 0.93, 0.78, and 0.52 and where malicious node rate is calculated as 2%, 17%, 22%, 48% respectively.

The performance observations primarily depend on the evaluated PDR and their computational metrics. Naturally, the performance depends on the size of the simulation area, the number of nodes, their communication range, the mobility model, and the scanning intervals which together govern the frequency of connection events.

Simulations may be faster than real-time but complex setups in simulation and large memory space cause significantly slowdown their process. The simulator continuously reports the ratio of simulation time per second of real time elapsed, which gives some performance indication. The Simulation speed also depends on the simulation time solution that is the intervals at which the simulation time is advanced. This interval is adjustable and doubling the interval may often make the simulation run almost many times faster.

CONCLUSION

The Reputation based mechanism enables a node on DTN cluster to identify the truthfulness of the intermediate nodes in which it enters on transaction. TRMM used threshold value to detect and isolate the adversaries who damages transactions of other nodes in a network within short period of time. The proposed scheme improves the performance of Neighbor discovery protocol by quickly computing the reputation values in a DTN environment. Moreover, the mechanism provides high data availability in minimized delay for detecting and isolating the malicious nodes.

The future work, will address 1)How each network node accurately compute the reputation values of other network nodes in a short time , 2) How each legitimate node detects and isolates the malicious nodes from the network to minimize their impact to the network performance in a short period of time.

An efficient approach has to be framed for maintaining a reputation rating and a trust rating about everyone who is of interest and that approach have to be fully distributed ad no agreement is necessary to speed up the detection of misbehavior nodes, it is advantages cautiously, make use also of reputation records from others in addition to first – hand observations. These records should consider in the case when they come from a source that has consistently been trustworthy or when they pass the deviation test which evaluates compatibility with one's own reputation ratings.

REFERENCES

[1]. Erman Ayday, Faramarz Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks". 2012
[2]. Gao, Zhaoyu, "PMDS: A probabilistic misbehavior detection scheme in DTN". 2012
[3]. Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen"MUTON: Detecting Malicious Nodes in Disruption-Tolerant Networks". 2010
[4]. Bensi Vijitha.J, Mrs. Sudha.R, "Clustering in Adhoc networks based on Load Balancing for Delay – Tolerant Applications",2012
[5]. Ari Keranen, Mikko Pitkanen,Mikko Vuori, Jorg Ott "Effect on Non – cooperative Nodes in Mobile DTNs". 2011
[6]. K. Fall, "A Delay – Tolerant Network Architecture for Challenged Internets,"Proc. ACM SIGCOMM, pp.27-34,2003.
[7]. Y. Yang, Q.Feng, Y.L.Sun, and Y.Dai, "RepTrap: A Novel Attack on Feedback – Based Reputation Systems", Proc. Fourth Int'l Conf. Security and privacy in Comm. Networks(SecureComm '08), pp. 1-11, 2008.
[8]. A.Kate ,G. Zaverucha, and U.Hengartner, "Anonymity and Security in Delay Tolerant Networks," Proc. Third Int'l Conf. Security and privacy in Comm. Networks(secureComm '07), 2007.
[9]. J. Burgess, G.Bissias, M.Corner, and B.Levine, "Surviving Attacks on Disruption – Tolerant Networks without Authentication," Proc. Eighth ACM Int'l symp. Mobile Ad Hoc Networking and computing, pp. 61-70, 2007.
[10]. B.n.Vellambi, R.Subramanian, F.Fekri, and M.Ammar, "Reliable and Efficient Message Delivery in Delay Tolerant Networks using Rateless Codes," Proc. First Int'l MobSys Work-shop Mobile Opportunistic Networking(MobiOpp'07) pp. 91-98,2007.