

Counterfeit Avoidance using Mark-Time Protocol in Mobile Networks

P.P. Joby
Professor, Department of CSE
PPG Institute of Technology
Tamil Nadu, India

M. Lavanya
PG Scholar
PPG Institute of Technology
Tamil Nadu, India

C. Lincy Magdaline
PG Scholar
PPG Institute of Technology
Tamil Nadu, India

ABSTRACT

Keeping a track of the nodes through which the packets are sent, the retransmission of packets within the network can be avoided. A new protocol called the MARK-TIME protocol is introduced to track the information and store it in common at the base station of the network. The distance of the node in the network is calculated along with the path, is used to transmit the message packets within the network. The detail of the packets and the path along which the data is transmitted is stored in the proxy server at the base station. In the case of delay or loss in communication, due to mobility of nodes in the network, it leads to loss of the receiving packets in the receiver (sink node). It sends a message to the proxy server, which tracks the node and provides efficient transmission without duplication of packets within the mobile network.

General Terms

Proxy Server, Base Station, Source, Sink, Protocol.

Keywords

MTP-Mark- Time Protocol, SnW-Spray and Wait, BSN-Binary Spray and Wait, PROPHET-Probabilistic Routing Protocol using History Encounter and Transitivity.

1. INTRODUCTION

The network has its importance and complexity in communication between the nodes. The main problem is the missing and delay of packets, due to many reasons in mobile networks. The nodes misinterpret the situation and resend the packets to all other nodes, which is a waste of bandwidth and as a result is an overhead. Previous works only concentrated on the calculation of distance of the nodes and modeled it in a way such that the replication is done as soon as the nodes receive packets.

Consider a network that has multiple nodes and a transmission from node 1 (source node) to node 5 (sink node). In this situation, when one intermediate node identifies loss of transmission path, which causes many issues in delivery of message packets within the network, the node does not check other nodes in transmission path to determine the cause of loss or delay in communication, but just replicates the packets. This causes the wastage of bandwidth and time, thereby causing an overhead in the network.

A new protocol called MARK-TIME protocol (MTP) is introduced to overcome the backlogs in the previously mentioned protocol. In this protocol, a proxy in the base station tracks the performance of the all nodes in the particular network continuously.

Consider the above mentioned situation, after one node identifies a failure of communication path which causes inability to transmit message packets, it sends the failure message to the proxy in the base station of the network, rather than replicating the message to all other nodes directly. The

proxy sends messages to all the nodes in the network, to identify if there are stagnant nodes in the transmission path from source to sink. Thus the node that has communication with the stagnant node sends the information to the proxy.

In case that the proxy does not receive any information about stagnant node from other nodes, it sends the missing message to the intermediate node in the transmission path, which in turn replicates the packet to the other nodes in the network by determining new path for communication establishment.

By using this concept, there is a reduction of the number of retransmission of packets due to misinterpretation in the network; thereby creating a reliable network to control the unwanted replication of packets, which reduces the bandwidth and time consumption for data transfer within the network.

Section 2, describes the previous related works in this field. Section 3, describes briefly about the new MARK-TIME protocol. Section 4, contains data about simulated results and graphs. Section 5 concludes the paper, followed by references in section 6.

2. COMPREHENDED WORKS

In the network, the communication between nodes has been a major problem for long periods from when the network usage emerged. Thus, if a message is to be transmitted from one node say source in the network to another node say sink in the network, the transmission path to establish communication and transfer of message packets from source to sink node is determined. The message packets are transmitted in the path, but the main issue in mobile network is the nodes that move randomly, which may lead to communication failure in the network.

If the intermediate node finds a path failure and it is unable to detect next node in the communication path, the message packets get stagnant in the intermediate node, which causes buffer overflow in that node. Thus, to avoid this problem there are many solutions provided earlier.

The traditional routing scheme used is Epidemic Routing (ER)^[7] in which each and every node replicates all packets to all other nodes within the network. This technique may avoid path failure, but it has some disadvantages like decrease in reliability and increase in message drops.

Another technique called Probabilistic Routing Protocol using History Encounter and Transitivity (PROPHET)^[8] is also most widely used, which finds the next hop node to transmit the packets when there is a path failure in the network. It also has some issues such as the probability of the next node to be replaced in case of path failure is tracked continuously and it is time consuming.

The Spray and Wait (SnW)^[6] routing technique involves each node with maximum number of replicas (say m) in the network. Then that node can replicate only m times in the

network and the neighbor node replicates message packets till it reaches the destination node.

The Binary Spray and Wait (BSN)^[6] routing also has maximum number of replicas in the network. If a node has m number of replicas, then the node uses only m/2 replicas in the network to transmit the message.

In Advanced Spray and Wait routing method, the algorithm determines the maximum number of replicas in a node by considering the distance between the node and the base station. The number of replicas decreases when the node is near the base station and the number of replicas increases when the node is far away from the base station.

3. MARK-TIME PROTOCOL

The Mark-Time Protocol is explained with the help of an algorithm and a table.

3.1 Algorithm

The Algorithm describes the MTP protocol for establishing the communication between nodes and transmitting message packets with minimum number of replicas, by avoiding misunderstanding of small delay in communicating nodes as node failure and retransmitting packets to other nodes in network.

MTP Algorithm

i/p- Network nodes (0-n), Source & Sink node

o/p- Message transaction b/w source & sink with minimum number of replicas.

Source node → Nx;

Sink node → Ny;

// Determining transaction path

```
path = Nx;
if( path != Ny)
{
for(i=0;i<=n; )
{
if(Ni is nearest to Nx)
{
path = path + Ni;
}
else
i++;
}}
```

// Message packet transaction between nodes

```
for(j=path;j!=Ny; )
{
if(Nj is visible)
msg→Nj;
else
```

```
{
Nj sends path failure msg to proxy;
if(Nj is visible to other nodes in network)
{
sends delay message
}

// Determining alternative path and replicating else
{
for(i=0;i<=n; )
{
if(Ni is nearest to Nx)
{
path = path + Ni;
msg → Ni;
}
else
i++;
}}}
```

Thus, in MTP if there is any problem in packet transmission path due to missing of node or some delay in processing within the network, a message is sent to the proxy in base station, rather than finding alternative path without knowing whether the problem can be recovered or not. The early specified solutions provide techniques to overcome this problem by continuously tracing an alternative path and retransmission of packets as soon as identifying the problem in path, without verifying the cause or chance of resuming the transmission path.

Thus, the proxy checks weather the missing node is in communication with other nodes of the network and if some node responds to proxy it sends a delay message and the node waits for a period of time to recover the path. If there is no reply to proxy from other nodes about missing node in the network, it considers it as node failure and finds an alternative path and retransmits the packets by replicating it in new path.

In the above algorithm the input of all nodes in the network is given and the source and sink nodes are given as input. Where Nx and Ny are source and sink nodes respectively.

Then source node (Nx) is assigned to path, if Nx is not equal to Ny, the other nearest nodes which leads to path establishment from source to sink are found using 'if (Ni is nearest to Nx)' and the value of Ni is appended to path. If the node is not nearest node to establish path, the value of 'i' is incremented and it checks for other nodes in the network. This process is done till the path reaches the sink node (Ny).

Then the predetermined path is assigned to Nj and if node Nj is visible in network, the message packets are transmitted. If Nj is not visible it sends failure message to proxy.

The proxy checks for the visibility of node in the network and to some other nodes in the network. Then delay message is sent and the intermediate node waits till the visibility of node Nj, and resumes the packet transmission process, else the node Nj is considered as a failed node and new path for packet transmission is found and assigned a path and again the same

process is continued till the message packets reach sink node (N_y) in the network.

Thus, the proposed MTP algorithm helps in avoiding continuous tracking of new paths until problem arise in the network and avoids unwanted replication.

3.2 Proxy Table

In MTP, the communication path establishment and the entire packet delivery process is done with the help of proxy tables present in base station. These tables help to track the nodes and their progress within the network.

In Table 1, the proxy table maintained during MTP protocol execution is displayed. The data on the table are filled according to the progress of nodes under MTP protocol algorithm, which helps in reducing the number of retransmission required during packet transmission in the network.

Table 1. Proxy Table for MTP

Communicating Nodes	Path	Failure Nodes	Response	Resend
1-5	1-4-2-5	4	1	No
2-3	2-4-3	3	-	Yes
3-5	3-4-2-5	2	4	No
4-5	4-2-5	2	-	Yes
5-1	5-2-4-1	1	4	No

4. SIMULATED RESULTS

The proposed MTP protocol is implemented using simulation tool and the output result efficiency are compared with previously proposed solution for the problem in the network. The following graphs are the results obtained by simulating the MTP protocol. Whereas the colours in the graph indicates,

■ SnW ■ MTP

Where,

SnW- Spray and Wait routing technique

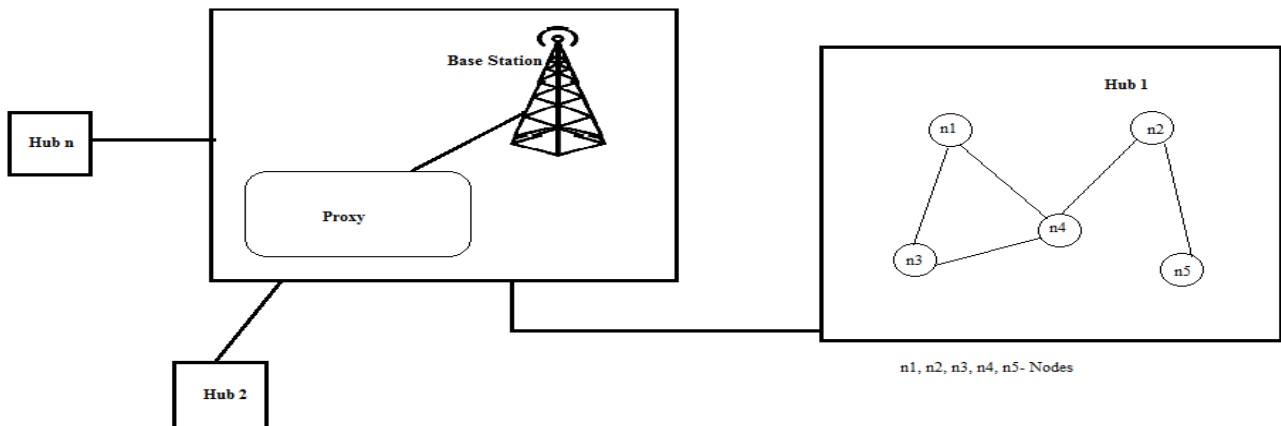


Fig 3: Overview of MARK-Time Protocol

MTP- Mark-Time Protocol

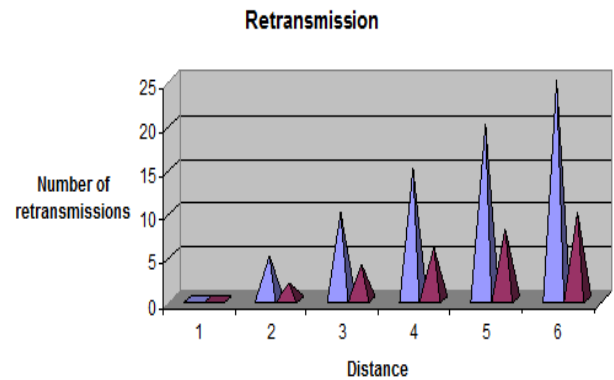


Fig 1: Number of retransmissions of packet

The above graph indicates the results obtained by simulating the previously proposed SnW technique and the proposed MTP protocol with respect to number of retransmission required within the network for delivering message packets from source to sink node. Thus, the number of retransmission required is comparatively reduced by implementing MTP protocol in the network.

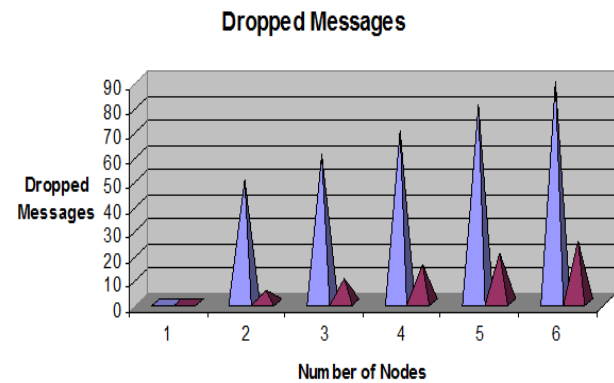


Fig 2: Number of dropped message packets

The above graph represents the number of message drop within the network. The implementation of MTP protocol reduces the message drop by reducing the number of stagnant packets within the network. Thus, the above graphs indicate the result of MTP simulation and its improved performance in network communication.

5. CONCLUSION

The major problem in communication establishment and packet transmission in network is misunderstanding of node failure and finding alternative path. Thus, the MTP protocol is used to overcome the problem with higher efficiency in controlling replication compared to previously proposed solutions.

The future enhancement of this paper can be done related to minimizing the bandwidth and memory consumption of proxy in base station.

6. ACKNOWLEDGMENTS

We extend my heart-felt gratitude to the management of PPG Institute of Technology, for providing us the best platform that satisfies our quest for knowledge which paved the way to progress the project paper.

7. REFERENCES

- [1] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, "Delay tolerant networking architecture," Network Working Group RFC 4838, Apr. 2007.
- [2] K. Fall, "A delay-tolerant network architecture for challenged internets," in Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ser. SIGCOMM '03, Aug. 2003, pp. 27–34.
- [3] Q. Fu, L. Zhang, W. Feng, and Y. Zheng, "Dawn: A density adaptive routing algorithm for vehicular delay tolerant sensor networks," in Annual Allerton Conference on Communication, Control, and Computing (Allerton), Sept. 2011, pp. 1250–1257.
- [4] K. Scott, T. Refaei, N. Trivedi, J. Trinh, and J. Macker, "Robust communications for disconnected, intermittent, lowbandwidth (dil) environments," in Military Communications Conference (MILCOM), Nov. 2011, pp. 1009–1014.
- [5] Y. Zhuang, J. Pan, Y. Luo, and L. Cai, "Time and location critical emergency message dissemination for vehicular ad-hoc networks," IEEE Journal on Selected Areas in Communications, vol. 29, no. 1, pp. 187–196, Jan. 2011.
- [6] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," in Proceedings of the ACM SIGCOMM workshop on Delay-tolerant networking (WDTN), Aug. 2005, pp. 252–259.
- [7] Z. Feng and K.-W. Chin, "A unified study of epidemic routing protocols and their enhancements," in IEEE International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), May 2012, pp. 1484–1493.
- [8] A. Lindgren, A. Doria, E. Davies, and S. Grasic, "Probabilistic routing protocol for intermittently connected networks," Internet Research Task Force (IRTF) RFC 6693, pp. 1–112, Aug. 2012.
- [9] A. Balasubramanian, B. N. Levine, and A. Venkataramani, "Replication routing in dtms: A resource allocation approach," IEEE/ACM Transactions on Networking, vol. 18, no. 2, pp. 596–609, April 2010.
- [10] X. Ma, "Coupling degree seeking based routing strategy for delay tolerant networks," in International Conference on Signal Processing Systems (ICSPS), vol. 1.
- [11] P.P. Joby, Sengottuvelan, "A Localised clustering scheme to detect attacks in wireless sensor Networks" International journal of electronic security and digital forensics, vol 7, No.3,2015.
- [12] X. Wang, Y. Shu, Z. Jin, and H. Chen, "Directional forward routing for disruption tolerant networks," in Asia-Pacific Conference on Communications (APCC), Oct. 2009, pp. 355–358.
- [13] A. Bujari, C. Palazzi, D. Maggiorini, C. Quadri, and G. Rossi, "A solution for mobile dtn in a real urban scenario," in IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Apr. 2012, pp. 344–349.
- [14] D. Hua, X. Du, Y. Qian, and S. Yan, "A dtn routing protocol based on hierarchy forwarding and cluster control," in International Conference on Computational Intelligence and Security (CIS), vol. 2.
- [15] P.P. Joby, Sengottuvelan, "A survey on threats and security schemes in wireless sensor Networks", International journal of engineering research and applications vol 5, issue 1, pp 89-94 2015.
- [16] H. Mei, P. Jiang, and J. Bigham, "Augmenting coverage in a cellular network with dtn routing," in IEEE Wireless Communications and Networking Conference (WCNC), Mar. 2011, pp. 516–521.
- [17] M. Haibo, J. Peng, and J. Bigham, "Augment delay tolerant networking routing to extend wireless network coverage," in International Conference on Wireless Communications and Signal Processing (WCSP), Nov. 2011, pp. 1–5.
- [18] S.-H. Kim and S. Jae Han, "Contour routing for peer-to-peer dtn delivery in cellular networks," in International Conference on Communication Systems and Networks (COMSNETS), Jan. 2012, pp. 1–9.
- [19] W. Jianjian and W. Ronghui, "A routing algorithm based on energy constraint," in International Conference on Computer Research and Development (ICCRD), vol. 2, Mar. 2011, pp. 330–332.
- [20] Q. He, Y. Li, and X. Fan, "A study on buffer efficiency and surround routing strategy in delay tolerant network," in IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dec. 2009, pp. 566–570.