Communication Between Mobile Devices using Opportunistic MSNs with the Help of Community Aware Oppurtunistic Routing Algorithm

[1]D. Sangeetha, [2]N. Karthika
[1]PG Student, [2]Assistant Professor
[1&2]Department of Computer Science and Engineering,
[1&2]Jayaram College of Engineering and Technology, Tiruchirappalli, Tamilnadu, India.

***Abstract* - Mobile Social Networks (MSN) are increasing nowadays as the mobile users would like to share the knowledge with their community. Even though some of the social networks are available, users are unable to communicate only to their individual communities. The difficulty exists to communicate with the separate set of people. To improve the situation, community aware opportunistic routing algorithm has been proposed along with reverse dijkstra's algorithm to efficiently reduce the delivery delay of nodes in the network. The communications among the mobile users are made to traverse in a secured manner. Since communications among the users happen in the network of community homes, computational and maintenance cost of contact information are greatly reduced. This work also proves that energy levels of mobile nodes are also increased.**

Keywords – Mobile Social Networks, opportunistic routing, Community Aware Opportunistic Routing

1. INTRODUCTION

In the modern world, the use of portable devices has increased the use of wireless communication and networking technologies. The conventional methodology such as mobile adhoc networks, intermittent and uncertain connectivity has led to the disruptive and a challenging data forwarding task. To improve the situation, new routing and data dissemination solutions in an opportunistic manner between mobile users have been proposed. The growing environment has created a great attention towards the information centric networks (ICN) in both academia and industries. ICN, an alternative approach for IP-based computer networking used for content data search and retrieval. The user is focused mainly on data and does not care about the origin and about, how it is retrieved. The data are retrieved with the help of the unique identifier.

Public-key cryptography, a technique in the cryptographic system comprise of two separate keys. Of which, one is public and the other is private. By terms, although the keys are both different, they are linked mathematically.

Security is not an essential consideration for public key whereas for private key, authentication of the person required to view the message is must.

The Public-Key infrastructure (PKI) system is used to verify the binding relationship between the public-key and the user identity in public-key cryptography scheme. However, the current PKI scheme has been considered inefficient, unusable and difficult to deploy, especially for the mobile application scenario. For example, in the application scenario of vehicular network without any infrastructure, the PKI service is unusable. Mobile ICN needs a more flexible and usable mechanism to verify the binding relationship of the user identity and public-key.

MSN's is a combination of concepts from two disciplines viz., social network and mobile communication network. Social network defines the structure of the user and the communication between their peers. Broadly, MSNs can be categorized into two types: infrastructure-based MSNs and infrastructure-less or opportunistic MSNs [2].

Figure 1: View of Social Network

Social networks use Infrastructure-based MSN's to acquire information from web. In all these cases, the mobile users are required to connect to the internet to communicate with their peers whereas in opportunistic MSNs, mobile devices need not connect to a centralized server for communication purposes.

This paper mainly focuses on single-copy routing problem in MSNs. The people belonging to a community would like to communicate and share similar stuff with the people of similar communities. By considering this basic fact, a home aware community model has been proposed.

Following this, Community Aware Opportunistic Routing (CAOR) algorithm has also been proposed and used for this purpose.

2. ASSUMPTIONS IN NETWORK

Table 1: Depiction Of Auxiliary Variable

v, l, d, S	*v* is a node, *l* is a location or home, *d* is a destination, and *S* is a set of nodes or homes.
v, l, S, l	The exponential distribution parameter of that node *v* and (any node in) node set *S* visit home *l*.
~Ri	the optimal relay set for the opportunistic routing from a message sender (*i*) to destination *d*.
~ Si,j	the optimal between's set for the message delivery from home *i* to *j*. When the context is clear, the subscripts are removed.
Di,d(*S*)	the minimum expected delivery delay from *i* to *d* via relay set *S*, where *i* may be a node, or a home. Specifically, *Di;d=Di;d*(*~Ri*) when *S= ~Ri*.
Bl,l′ (*S*)	the betweenness of *S*, i.e., the expected delivery delay from home *l* to *l′* only via node set *S*.

In this case MSN composed of $|V|$ nodes $V = \{v \mid v \in V\}$ moving among $|L|$ locations $L=\{l \mid l \in L\}$ ($|L| \ll |V|$) are considered. Each mobile node visits a few locations frequently, while visiting the others rarely.

This work also assumes that each home has a "throwbox" [5], which has the ability to store and transmit messages. Users of different places in the wi-fi enabled area communicate through access points. These access points can also be seen as a type of real throwboxes. This is because that each user can upload or download data from network storages through APs.

Figure 2: Communication among peers

3. OVERVIEW OF OPPORTUNISTIC MSNS

The optimal opportunistic routing scheme means that each message sender delivers messages via its optimal relay set (i.e., delivers messages via the first encountered relay in this set). The key problem is to determine whether a relay belongs to the optimal relay set for each message sender.

Groups can be created in two ways of physical social network and virtual social network. Users communicate with the peers within the short distance through Bluetooth. People would like to share similar stuffs belonging to their community. SOCIALNETS [3] and Haggle [4] are two well-known projects which attempt to exploit the underlying social network structure to develop effective protocols.

The exploitation of user habits and social interactions are carried out by SOCIALNETS whereas Haggle identifies the social networks and it let users to communicate when it come close to the range. The communications occur in a secured manner, if the user thinks of it as an unwanted message, need not accept the request from the other end.

Initially, the topologies of MSNs and Opportunistic Networks are unstable and users appear in and disappear from the network dynamically. Secondly, content producers and consumers might be completely unaware of each other, and may never be connected at the same time to the same part of the network. Thirdly, the involved protocols heavily rely on human mobility and contact opportunity, and hence, the prediction of future contact becomes a critical issue in both MSNs and Opportunistic Networks.

A new metric named social pressure metric has been derived which motivates the friend's community to share more and more information. This enables users of friend's community to track the past contact details, so that without any interruption communication can be made possible.

Algorithm 1 Determine optimal betweenness set

Require:
{⟨v1,l; v1,l′⟩; · · · ; ⟨vn,l; vn,l′⟩} (v1,l′ ≥· · ≥vn,l′)
Ensure: *~ Sl,l′ , ⟨ l,l′ ;D′ l,l′ ⟩*
1: Initialize:
S={v1} and *Dl;l′* (*S*)= 1 *v1,l*+ 1 *v1,l′* ;
2: **for** *i*=2, · · ·, *n* **do**
3: *S=S+{vi}*;
4: Incrementally compute *Dl,l′* (*S*)
5: **if** *Dl,l′* (*S*) increases **then**
6: Break;
7: **return** ~*Sl,l′=S−{vi}* and corresponding *⟨l,l′,D′l,l′ ⟩*;

Algorithm 2 CAOR initialization
Ensure:
G=⟨L,W⟩, where *W ={⟨l,l′,D′L,l′ ⟩|l, l′∈L}*
For each community home *l∈L* **do**
1: Collect *v,l, v,l′* for each *v∈Cl* and *l′∈L−{l}*;
2: Use Algorithm 1 to produce ~ *Sl,l′* and *⟨_l,l′ ;D′l,l′ ⟩*;
3: Create the virtual link
Lambda →ll′:⟨l,l′ ;D′l,l′ ⟩ for each *l′∈L−{l}* and send the link weights to other homes;
4: Receive the link weights from other homes;
5: Construct the contact graph *G=⟨L;W⟩*;

4. NODE STABILITY AND NODE INFLUENCE

Active nodes in the network can be found easily using the two metrics, Node stability and Node Influence. Stability of the node calculates about the node in the network communicate to a certain node over the particular period of time. This stableness in the network allows to identify how frequently, the communication between the two nodes occur over a period of time.

Node influence has been calculated based on how much a node influences other nodes to join the community in the home network. High influence score is obtained based on the node joins the community which influences other nodes to be a follower of that node.

5. DETECTION OF A COMMUNITY IN MSNS

A community is defined as the stronger ties between the members inside the group than the members who reside outside the group. The members of whatever community would like to share materials like images, study items etc to the other members within the community. This has enabled the thirst of detecting the community.

For example, the members belong to a study level would love only to join in the same community of people rather likely to join with the oldies. Modularity methods are used to detect the community in an easier way.

6. CONCLUSION

This paper explains about the routing of nodes in MSNs into some overlapping home aware communities. The work simplifies the routing problem through CAOR algorithm thereby enhances the security in the communicating nodes. Energy level of the nodes has also been conserved through communication within the same network and the communities. Community detection in the MSNs has been presented through the algorithms. The future work of this paper includes implementation of community detection in a more efficient manner thereby creating routing and dissemination solutions.

REFERENCES

[1] Mingjun Xiao, Jie Wu, Liusheng Huang “Community-Aware Opportunistic Routing in Mobile Social Networks”, IEEE Transactions On Computers VOL:PP NO:99, 2013.

[2] N. Vastardis and K. Yang, “Mobile Social Networks: Architectures, Social Properties and Key Research Challenges,” *IEEE Commun. Surveys and Tutorials*, vol. 15, no. 3, pp. 1355-1371, 2013.

[3] European Commission’s FET/Pervasive Adaptation Initiative ‘Socialnets’ project. [Online]. Available: http://www.social-nets.eu

[4] European Commission’s FET Haggle project. [Online]. Available: http://www.haggleproject.org

[5] J. Wu, M. Xiao, and L. Huang, “Homing spread:Community home-based multi-copy routing inmobile social networks,” in IEEE INFOCOM,2013.

[6] J. K. Laurila, D. Gatica-Perez, I. Aad, J. Blom, O. Bornet, T.-M.-T. Do, O. Dousse, J. Eberle, and M. Miettinen, “The Mobile Data Challenge: Big Data for Mobile Computing Research,” in *Proc. of Mobile Data Challenge by Nokia Workshop, Colocated with Pervasive’12*, 2012.

[7] N. Aschenbruck, A. Munjal, and T. Camp, “Trace-based mobility modeling for multi-hop wireless networks,” *Computer Communications*, vol. 34, no. 6, pp. 704-714, 2011.

[8] P. Hui, J. Crowcroft, and E. Yoneki, “Bubble rap: social-based forwarding in delay tolerant networks,” in ACM MobiHoc, 2008.

[9] E. Daly and M. Haahr, “Social network analysis for routing in disconnected delay-tolerant manets,” in ACM MobiHoc, 2007.

[10] J. Wu and Y. Wang, “Social feature-based multipath routing in delay tolerant networks,” in IEEE INFOCOM, 2012.

[11] W. Gao, Q. Li, B. Zhao, and G. Cao, “Multicasting in delay tolerant networks: A social network perspective,” in ACM MobiHoc, 2009.

[12] Q. Li, S. Zhu, and G. Cao, “Routing in socially selfish delay tolerant networks,” in IEEE INFOCOM, 2010.

[13] R. Lu, X. Lin, and X. S. Shen, “Spring: A socialbased privacy-preserving packet forwarding protocol for vehicular delay tolerant networks,” in IEEE INFOCOM, 2010

[14] Vahdate and D. Becker, “Epidemic routing for partially-connected ad hoc networks,” Duke University, Tech. Rep. CS-2000-06, June 2000.

[15] T. Spyropoulos, K. Psounis, and C. Raghavendra, “Spray and wait: An efficient routing scheme for intermittently connected mobile networks,” in ACM SIGCOMM Workshop on Delay-Tolerant Networking (WDTN), 2005.

[16] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: routing for vehicle-based disruption-tolerant networks,” in IEEE INFOCOM,2006.

[17] C. Liu and J. Wu, “Routing in a cyclic mobispace,” in ACM MobiHoc, 2008.

[18] V. Conan, J. Leguay, and T. Friedman, “Fixed point opportunistic routing in delay tolerant networks,” IEEE Journal on Selected Areas in Communications, vol. 26, no. 5, pp. 773–782, 2008.

[19] M. Ibrahim, P. Nain, and I. Carreras, “Analysis of relay protocols for throwbox-equipped dtns,” in WiOPT, 2009

[20] D. Kotz, T. Henderson, I. Abyzov, and J. Yeo, “CRAWDAD data set dartmouth / campus (v. 2009-09-09),” Downloaded from http://crawdad.cs.dartmouth.edu/dartmouth/campus, Sep. 2009.

[21] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, “Modeling time-variant user mobility in wireless mobile networks,” in IEEE INFOCOM, 2007.

[22] C. Liu and J. Wu, “An optimal probabilistic forwarding protocol in delay tolerant networks,” in ACM MobiHoc, 2009.

[23] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Efficient routing in intermittently connectedmobile networks: the single-copy case,” IEEE/ACM Transactions on Networking, vol. 16,no. 1, pp. 63–76, 2008

[24] K. Jahanbakhsh, G. C. Shoja, and V. King, “Socialgreedy: A socially-based greedy routing algorithm for delay tolerant networks,” in MobiOpp,2010.

[25] H. Cai and D. Y. Eun, “Crossing over the bounded domain: From exponential to powerlaw inter-meeting time in manet,” in ACM Mobi- Com, 2007.