DATA FORWARDING IN OPPORTUNISTIC NETWORK USING MOBILE TRACES

B.Poonguzharselvi[1] and V.Vetriselvi[2]

[1,2]Department of Computer Science and Engineering, College of Engineering
Guindy, Anna University Chennai, Chennai-600025
biselvi@gmail.com
vetri@annauniv.edu

ABSTRACT

Opportunistic networks are usually formed spontaneously by mobile devices equipped with short range wireless communication interfaces. The idea is that an end-to-end connection may never be present. Designing and implementing a routing protocol to support both service discovery and delivery in such kinds of networks is a challenging problem on account of frequent disconnections and topology changes. In these networks one of the most important issues relies on the selection of the best intermediate node to forward the messages towards the destination. This paper presents a mobile trace based routing protocol that uses the location information of the nodes in the network. Using the trace information, next hop is selected to forward the packets to destination. Data forwarding is done via the selected nodes. The effectiveness is shown using simulation.

KEYWORDS

Opportunistic network, mobile trace, routing protocol, delay tolerant network.

1. INTRODUCTION

Opportunistic network is a type of Delay tolerant network (DTNs), where data will be routed with tolerant delay from source to destination [5]. This type of network is used for emergency applications. An opportunistic network (oppnet) is a network of mobile as well as fixed nodes. Opportunistic network are different from traditional network. In traditional network, nodes are deployed together and end to end path exist for data forwarding. But in opportunistic network there is no fixed path between source and destination due to mobile nodes. It is an extension of mobile ad hoc network.

In opportunistic network[11], first seed oppnet is deployed like typical ad hoc network. Then it detects foreign devices for completing the emergency applications with tolerant delay. The detected devices are evaluated for their usability and resource availability. If it is satisfied the device is integrated into the oppnet as a helper. This helper integration process is continued until enough devices are found for completing the task. Once the integration process is completed, routing will be done with the help of helper nodes. Helper nodes are used as intermediate nodes for forwarding data from source to destination. Different nodes make collaboration to exchange data from source to destination.

In this type of network, a data holding node (source node/neighbour node) finds an opportunity to forward data. The devices exchange data in a spontaneous manner whenever they come in close. When there is no direct connection between source and destination, data holding node will

Sundarapandian et al. (Eds): CoNeCo,WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT 07,
pp. 425–430, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2441

discover its nearest neighbour node and uses it to forward messages toward the destination node. Message is delivered hop by hop closer to the destination. In an opportunistic network, routes are determined at each hop when packets traverse through different hops. Each node is equipped with local knowledge of the best nodes around it and it uses this knowledge to determine the best path to transmit the message to the destination. In the absence of any such nodes, the node currently holding the message simply stores the message and waits for an opportunity.

The data holding node forwards data through intermediate helper nodes. These helper nodes can be able to hand over the data packet to the destination. In opportunistic network the routing is done with the help of intermediate helper nodes to deliver the data packets to destination before the TTL of that data can be reached. Once TTL expires, the data will be lost and it cannot be delivered to the destination. To avoid such a kind scenarios and to solve emergency applications, intermediate nodes are used for data forwarding from source to destination. The applications of opportunistic network are typically used in an environment that is tolerant of long delay and high error rate. Routing in opportunistic network is composed of two factors:

1. *To find a path to destination:* There is no fixed path between source and destination in the opportunistic network. Intermediate nodes are used to form paths dynamically.
2. *Selection of next hop forwarder:* Finding a helper node which can forward data to destination as earlier as possible.

The messages may have to be buffered for a long time by intermediate nodes, and the mobility of those nodes must be exploited to bring messages closer to their destination by exchanging messages between nodes as they meet.

This paper is organized as follows. Section 2 focuses on related work, it contains various proposed methods for routing in opportunistic networks. Section 3 focuses on System architecture for proposed method. In Section 4 the implementation details are discussed and performance has been evaluated. Section 5 concludes the paper.

2. RELATED WORK

Several routing algorithm for opportunistic networks have been proposed. Initially Spyropoulos et. al. [7] proposed a simple single-copy routing called direct transmission routing for opportunistic networks. The main advantage of this scheme is that it incurs minimum data transfers for message deliveries. On the other hand, although having minimal overhead, this scheme may incur very long delays for message delivery since the delivery delay for this scheme is unbounded.

To reduce long delivery delay, Vahdat et. al.[10] proposed Epidemic routing that utilizes the epidemic algorithm which was originally proposed for synchronizing replicated databases. The Epidemic Routing is similar to the flooding routing because it tries to send each message to all nodes in the network. For this reason, Epidemic Routing incurs significant demand on both bandwidth and buffer. LeBrun et al. [2] proposed a method using the motion vector (MoVe) of mobile nodes to predict their future location. As compared to epidemic routing, this approach has less control packet overhead and buffer usage.

Burgess et al. [3] proposed a protocol called MaxProp for effective routing of messages. A node uses MaxProp to schedule packets transmission to its peers and determines which packets should be deleted when buffer space is almost full. Lindgren et al. [1] proposed a probabilistic routing protocol, called PROPHET (Probabilistic Routing Protocol using History of Encounters and Transitivity). PROPHET estimates a probabilistic metric called delivery predictability. They showed in their simulation results that the communication overhead of PROPHET is lower than that of Epidemic Routing[10]. Jianwei et al. [4] proposed Predict and spread algorithm by combining both prediction and flooding concepts to achieve reduced message delivery delay. It employs Markov chain to model the node mobility patterns using Mobile Traces and then predicts the contact probability and contact time. Then it selects 2 neighbor nodes with high prediction value and forwards message to those nodes. It Improves the Delivery ratio and reduces the delivery latency based on Simulation traces (not real traces).

Some of the existing routing algorithms were not using real mobile traces. Still there is a need for the improvement in packet delivery ratio and reduced overhead. This paper proposes a mobile trace based routing algorithm to provide solution to the routing problems in opportunistic networks. It utilizes the concept of regularity in node's movement and stability time to forward data from source to destination. In order to improve packet delivery ratio, the proposed routing algorithm uses mobile traces and gives reduced overhead as compared with existing routing algorithms in opportunistic networks.

3. MOBILE TRACE BASED ROUTING PROTOCOL

Opportunistic network is composed of mobile devices with local wireless interfaces, these devices are carried by mobile users. In this paper, it is assumed that the users have some regularity in movements and this regularity in movement is captured as mobile trace file.

3.1. Trace File Incorporation

Trace file contains the static locations and corresponding time unit of mobile nodes in opportunistic network, it shows the regular movements of the mobile nodes.

Table 1. Mobile trace file

Time	**X position**	**Y position**	**Stability Time**
T1	X1	Y1	S1
-	-	-	
Tn	Xn	Yn	Sn

The mobile trace file is shown in Table-1 which contains stability information about the nodes. The stability of the node is predicted using trace based mobility (TBM) model [12]. The TBM model is used to exploit the regularity in movement of a node and arrive at the trace file. We use the trace file obtained from the TBM model for the routing protocol.

The trace file represents that a node stays at location (X_i,Y_i) at the defined time for S_i seconds and then moves to another location which is defined in that file. The trace file contains only the positions and time where the node stays for a long time. All the nodes in opportunistic network are assumed to have their own trace file that contains the regularity in movement. A node which can forward data to destination is identified using this trace file information.

3.2. Neighbour Node Identification

Neighbour node identification is the process whereby a node identifies its current neighbours within its transmission range. For a particular node, any other node that is within its radio transmission range is called a neighbour. All nodes consist of neighbour set which holds details of its neighbour nodes. Since all nodes might be moving, the neighbours for a particular mobile node are dynamic.

The neighbour set is dynamic and needs to be updated frequently. Generally, neighbour node identification is realized by using periodic beacon messages. The beacon message consists of node ID, node location and timestamp. Each node informs other nodes of its existence by sending out a beacon message periodically.

3.3. Data Forwarding

Data forwarding in opportunistic network follows “Store and Forward” mechanism. Since there is no end to end path between source and destination, the data to the destination can be forwarded through the intermediate nodes. It is assumed that the seed nodes have the trace file information of the other seed nodes. Hence the source node knows the probable position of the destination from the trace file of the destination. The major task is the selection of next hop forwarder.

Once the trace file of the destination is available with the source node, the movement of the destination node can be predicted by looking up its trace file. Instead of broadcasting a data in all directions, the source node and the intermediate nodes can use directional information to forward data to destination. This helps to reduce the load on the network. An additional field containing the destination’s probable position can be added in the message header. The modified message header format is shown in Figure 1.

Source address	Destination address	Packet ID	Packet size	TTL	Path information	**Destination position**	**Next hop address**

Figure 1. Message header format

The additional fields in this packet (highlighted in the figure), when compared to any routing protocol, are the destination position, and the address. The data is forwarded to the next hop that moves in the direction of the destination.Using the trace file of the neighbour nodes the next hop node to forward the data is identified. From the trace file of the neighbour node, the source node identifies the neighbour node that moves in the direction of the destination. Similarly the selected neighbour node forwards the data to the next neighbour who is moving in the direction of the destination. If the destination node is found then the neighbour node forwards the data to the destination. If the detected neighbours are not moving in the direction of destination node then it floods the packets to all its neighbours, so that the data reaches the destination.

Routing is done by selecting the node that meet the destination earlier or that will go in the direction of destination. Data to any destination can be forwarded using the selected next hop forwarder to reduce the overhead ratio and to increase the packet delivery ratio.

4. Implementation and Performance Analysis

The proposed method is simulated using ONE simulator [6] which combines movement modelling, routing simulation, visualization and reporting in one program. It is agent-based discrete event simulation engine and provides interface for developing new routing algorithms and mobility models. The total simulation time is 3000 seconds. New messages are generated by the Message_Event_Generator in ONE. The trace file incorporation is done with the help of External_Movement class in ONE simulator. The simulation parameters are shown in Table 2.

Table 2. Simulation parameters

Parameter	**value**
Simulation time (sec)	3000s
Simulation area	1000,1000
No. of nodes	50
Nodal minimum speed(m/s)	10
Interface	btInterface
Mobility Model	External Movement
Nodal maximum speed(m/s)	20
Transmit range (meters)	6
Transmit Speed (m/s)	250

The delivery ratio and the overhead ratio parameters are used to evaluate the proposed routing algorithm. To assess the performance of the proposed algorithm, the simulation results of Prophet and Direct deliver algorithms is compared with our proposed protocol.

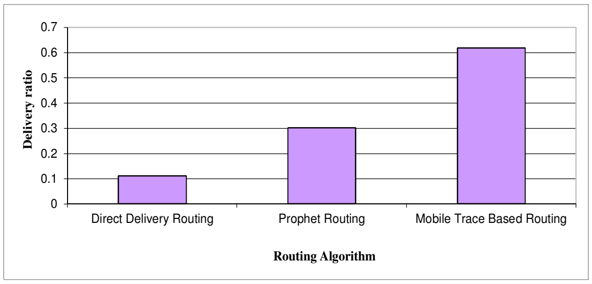

Figure 2. Comparison based on delivery ratio

From figure 2, the proposed mobile trace based routing algorithm has improved packet delivery ratio as compared with other existing algorithm. Since it forwards packets to neighbour nodes that move in the direction of the destination that is based on the trace file information. Improvement in delivery ratio is also accomplished due to the selection of next hop forwarder who can meet the destination earlier than the source or other nodes in the network. Direct delivery routing has less delivery ratio as compared with all routing algorithms. Since the source node forwards data to destination only when there is a connection between communicating parties. If source node not able to meet the destination before time out expires then the data packet is dropped out. It leads the direct delivery routing to have less delivery ratio. The delivery ratio of Prophet routing protocol is less compared to our proposed routing but better compared to direct delivery routing. This is because it forwards the packet based on the predicted delivery probability of the neighbour.

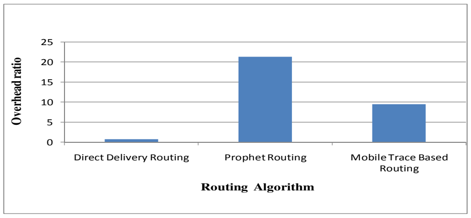

Figure 3. Comparison based on overhead ratio

The figure 3 shows that proposed routing algorithm has less overhead compared with the existing algorithms. Prophet Routing floods the same packet to one or more nodes that have high delivery probability hence overhead ratio is high. Whereas direct delivery routing handovers the data directly to the destination when they directly meet each other. Hence it has less overhead ratio as compared with other methods. The proposed algorithm forwards data to the helper node which is going in the direction of destination. So it has a less overhead as compared with prophet routing algorithm.

5. CONCLUSION AND FUTURE WORK

Mobile devices with local wireless interfaces can be organized into opportunistic networks which have the properties of social networks. To take advantage of this attribute, this paper proposes a mobile trace based routing algorithm which uses mobile traces for node movements.

Using the mobile trace file, the direction of the destination is predicted as well the neighbour node that moves in that direction is selected as the forwarding node. This in turn improves the performance of message forwarding in opportunistic networks. Experimental results show that proposed algorithm improves the delivery ratio and reduces the packet overhead significantly. The proposed algorithm selects the next hop forwarder based on the trace file information, there may be a malicious node in the network and that can degrade the performance of the opportunistic network. In future, trust mechanisms can be incorporated with the proposed approach to detect and eliminate the malicious nodes in the network.

REFERENCES

[1] A. Lindgren, A. Doria & O. Scheln,(2003) " Probabilistic Routing in Intermittently Connected Networks", ACM *Proceedings Newsletter on Service Assurance with Partial and Intermittent Resources*, Vol. 7, No.3, pp 19-20.

[2] B. Burns, O. Brock & B. N. Levine, (2005) "MV routing and capacity building in disruption tolerant networks", IEEE *Conference on Computer and Communications and Societies*, Vol. 1, pp. 398–408.

[3] J. Burgess, B. Gallagher, D. Jensen & B. N. Levine,(2006) "Maxprop:Routing for vehicle-based disruption-tolerant networks", IEEE *International Conference on Computer Communications*, pp. 1–11.

[4] N. Jianwei, G. Jinkai & C. Qingsong, (2011) "Predict and Spread: an Efficient Routing Algorithm for Opportunistic Networking", IEEE *Conference on Wireless Communications and Networking*, pp. 498–503.

[5] K. Fall, (2003) "A delay-tolerant network architecture for challenged Internets", ACM *Conference on SIGCOMM*, pp. 27-34.

[6] KER ¨ANEN, A., OTT, J., AND K ¨ARKK ¨AINEN, T, (2009) " The ONE simulator for DTN protocol evaluation", ICST *Proceedings of the 2nd International Conference on Simulation Tools*, pp. 1–10.

[7] T. Spyropoulos, K. Psounis & C. S. Raghavendra, (2004) "Single-copy routing in intermittently connected mobile networks", IEEE *Conference on Sensor and Ad Hoc Communications and Networks*, pp 235 – 244.

[8] T.Spyropoulos, Thrasyvoulos & Psounis, (2009) "Spray and Focus: Efficient Mobility Assisted Routing for Heterogeneous and Correlated Mobility", IEEE *International Conference on Pervasive Computing and Communications Workshops*, pp 79-85.

[9] T. Spyropoulos, K. Psounis & C. S. Raghavendra, (2005) "Spray and wait: Efficient routing in intermittently connected mobile networks", ACM *Proceedings of SIGCOMM workshop on Delay Tolerant Networking*, pp 252-259.

[10] A. Vahdat & D. Becker, (2000) "Epidemic Routing for Partially-Connected Ad Hoc Networks", Technical Report CS-200006, Duke University.

[11] L. Lilien, Z.H. Kamal, V. Bhuse & A. Gupta, (2007) "Opportunistic networks: The Concept and Research Challenges in Privacy and Security", Chapter in: Mobile and Wireless Network Security and Privacy, Springer Science & Business Media, Norwell.

[12] V.Vetri Selvi & Ranjani Parthasarathi, (2007) "Trace Based Mobility Model for Ad Hoc Networks", IEEE *International Conference on Wireless and Mobile Computing, Networking and Communications*, pp 81.