Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Routing Protocols in Infrastructure-less Opportunistic Networks

Ritu*
M.Tech Scholar
CGC,
Mohali, India

Manjot Kaur Sidhu
Associate Professor
CGC,
Mohali, India

Abstract— Opportunistic networks provide communication facilities by the intermittent connectivity among mobile nodes. Opportunistic network is an extension of MANET where complete path between two nodes wishing to communicate is unavailable. Opportunistic networks (OPPNET) consider mobility, partitions, disconnections, etc. as norms instead of the exceptions. Due to the disconnections and re-connections between the nodes, routing is another challenge due to unreliable wireless links in this type of networks. In Opportunistic networks nodes does all the computation for the next hop selection, which consumes a lot of battery power. So, in this paper we present a review on a number of existing routing protocols for infrastructure-less opportunistic networks in terms of energy consumption.

Keywords— Opportunistic networks, Opportunistic Routing, Routing Protocols.

I. INTRODUCTION

In recent years, most of the work has been done in the design of Mobile Ad-hoc Networks (MANET) technologies. MANET is infrastructure-less wireless networks where nodes communicate with each other's radio range and they use intermediate nodes to relay the packet. These networks have no central authority or fixed infrastructure. Mobile Ad-hoc Networks are characterized by self-configuration, stringent resource constraints, highly dynamic network topology, and shared wireless medium. These characteristics make them vulnerable to security attacks. The designed security solutions cannot directly applied to MANETs. The goal of security solutions is to provide security services like authentication, integrity, availability and confidentiality to mobile users.

Opportunistic network has been emerged as interesting evolutions of the Mobile Ad-hoc Networks paradigm. Thus they have challenges and issues faced by MANET along with some other challenges of their own. As in MANETs, the nodes which want to communicate remain connected with each other through common inter-network which is rarely possible in pervasive scenarios. During such type of environment devices carried out by users are partially connected to the network as users may turn them off their energy or due to high mobility nodes may move out of the radio range of the other nodes. So, traditional MANET routing protocols will fail to work in Oppnets. Opportunistic networks consider mobility, disconnections, partitions, etc. as norms instead of the exceptions. In opportunistic network mobility is used as a technique to provide communication between disconnected groups of nodes, rather than a drawback to be solved.

In opportunistic networking a complete path between two nodes wishing to communicate is unavailable. These networks try to allow such nodes to exchange messages by removing the assumption of end-to-end connectivity. In this case nodes are built dynamically which act like store-carry-forward paradigm, and intermediate nodes communicate like routers that store messages when no forward opportunity addressed to other nodes and exploit any future contact opportunity with other mobile devices to bring the messages closer and closer to the destination. In Opportunistic network any node can opportunistically be used as next hop to bring the message closer to the destination. These requirements make network a challenging research field. In this paper we survey the existing routing protocols in opportunistic networks.

Opportunistic Networks can have both fixed nodes as well as mobile nodes but generally they are mobile in nature. Opportunistic Networks (OPPNETs), such as delay tolerant networks, vehicular communication networks, and ubiquitous mobile social networks, have received considerable research attention in recent years. As an interesting evolution of MANETs, OPPNETs are more pervasive and distinguishably characterized by non-exist end-to-end connection, but intermittent connectivity among mobile nodes during their opportunistic contacts. However, due to the extremely dynamic and unstable network topology, the packet propagation in OPPNETs usually follows a "store-carry-and forward" manner and the packets can only be opportunistically relayed to their destinations with high transmission delay and low delivery ratio. In order to reduce the transmission delay and increase the delivery ratio, extensive research

efforts have recently been put into OPPNET routing and dissemination, and a variety of efficient routing and dissemination protocols [5]–[7], which either rely on network and mobility characteristics or utilize pre-existing social network information, have been proposed for OPPNETs.

Routing of messages in Oppnets is based on the contact opportunity between the nodes that arises due to their mobility. Due to sparse nature of opportunistic networks, it is possible that the intermediate nodes do not encounter other nodes frequently or consistently [8]. It may also happen that there might not be intermediate nodes which can be selected as a next hop to make the message closer to the destination or to the destination itself. In such situations either message will be directly forward to the destination whenever a direct link found or message will be store by nodes for a long period of time in the buffer when there is no forward opportunity towards the destination. Due to which messages may suffer longer delays while waiting for the path to be available towards the destination [8]. Routing and forwarding is the challenging task in Opportunistic Networks due to uncertain mobility and intermittent behaviour of the nodes. Most of the research work in oppnets has been done in routing and forwarding. There are various protocols that have been designed for Oppnets that is energy efficient and consumes power of nodes in forwarding the message. The routing protocols used in Oppnets can be classified in to two categories- Infrastructure based protocols and Infrastructure-less protocols[16]. In this paper we have only considered the routing protocols which make changes in the performance of opportunistic networks.

II. ISSUES IN MOBILE OPPORTUNISTIC NETWORKS

Mobile Opportunistic Networks (MobiOpps) are an extreme generalization of Mobile Ad-Hoc Networks (MANETs) that aim at enabling communication between mobile nodes in highly challenged conditions, which raise new networking and security issues due to:

A. *Heterogeneity:* as in MANETs, nodes cannot rely on a global infrastructure and on top of that they belong to heterogeneous networks that rely on various communication technologies. This means in particular that naming is an issue, because nodes don't have a unique address across the different networks and furthermore raises the requirement for new authentication and trust establishment mechanisms.

B. *High mobility:* nodes are extremely mobile and disruptions in paths are frequent. It is thus impossible to establish a stable end-to-end route: routing and security solutions should be highly dynamic and flexible, and should not depend on a pre-defined path.

C. *Delay tolerance:* since nodes belong to heterogeneous networks, an end-to-end path might simply never exist. Messages can still be delivered by adopting a store and forward strategy, where intermediate nodes store messages when communication is impossible and forward them when a communication opportunity arises, for example thanks to mobility. Such a strategy trades a higher delay for a higher delivery ratio, but this also means, from a security point of view, that direct interactions cannot be assumed: end-to-end key agreements are thus unpractical and all protocols relying on an on-line authority need to be revisited.

Because of these characteristics, MobiOpps call for a radical revision of all the aspects of communication, and in the following we present a review of routing protocols used in Opportunistic Networks.

III. RELATED WORK

In this section an overview of routing protocols used for infrastructure-less Oppnets, namely First Contact [9], Direct Delivery [18], Epidemic [20], Spray and Wait [19], ProPHET [14], MaxProp [3] , Adaptive Fuzzy Spray and Wait[15] , OLSR [11]

A. *First Contact*

This protocol [9] is the simplest of all the routing protocols available in Opportunistic Networks. In this, source node and the intermediate nodes forward the message to the neighbouring node which they encounter first in the radio range irrespective of the fact that it may not be a good forwarder towards the destination. If two or more nodes come in contact with the sender at the same time then message is forwarded along a path chosen randomly. If path is not available, the message waits for path to become available and then assigned to the first available contacts. In this method local copy of message is removed after a successful transfer of message which leads to lesser resource consumption and low congestion in the network. In this single copy scheme, if intermediate nodes carrying the message fails then the message will be lost. The delivery ratio is poor as the next hop is chosen randomly without considering the ability of a node to carry the message. The forwarding along the selected path may not make progress which also increases the message delivery delay.

B. *Direct Delivery*

In this protocol [18], source node does not pass the message to the intermediate nodes, but keeps it with itself until it comes direct in contact with the destination node. This scheme is simple, easy to deploy and, utilizes minimum bandwidth and network resources for message transfer since each message is transmitted at most once to the destination node. On the other hand, there may be a long delays for message delivery either in the case the source

never meets the destination or there may not be a direct contact between the source and the destination, but a path exists through intermediate nodes for the message passing. If the source node fails then the message will be lost as there is only one copy available in the network. In this scheme probability of delivery is poor so, it is not best for the situation where high delivery probability is required.

C. Epidemic

The Epidemic routing [20] protocol uses the concept of complete flooding for message transfer in Oppnets. Each node maintains two buffers in which first buffer is used for storing the messages generated by the node itself and the second one is used for the messages received from other nodes. Each message has a unique message ID associated with it and each node also maintains a list of the message IDs of all the messages carried in its buffer, and whose delivery is pending in the form of summary vector. When two nodes meet with each other they exchange their Summary Vectors by comparing, which they do not have in common. The multiple copies of the same message flow in the network after the completion of message exchange. All the nodes have the same messages in their buffers. In this way, all messages are spread in the network to all nodes including destination in an epidemic (like disease) manner. This protocol has significant demand on both bandwidth and buffer capacity due to large number of redundant messages. This protocol has high delivery ratio, low delay if sufficient resources are available.

D. Spray and Wait

The Spray and Wait protocol [19] provides an improvement over the Epidemic routing protocol by controlling the level of flooding. In this protocol there are two phases: the Spray phase and the Wait phase. As in Spray phase, every message originated at the source node is passed to L distinct relays in the network i.e. L copies of the message are spread over the network by the source code. If the destination was not found in the spray phase, then in Wait phase each relay node having a copy of message performs the direct transmission of the message to the destination itself. The performance of this protocol depends on the value of L, smaller the value of L makes it similar to Direct delivery protocol and larger the value of L makes it similar to the Epidemic protocol. This protocol has less number of transmissions and delay as compared to Epidemic Routing.

E. ProPHET

In ProPHET (Probabilistic Routing Protocol using History of Encounters and Transitivity) [14], each node before sending a message, calculates a probabilistic metric called Delivery Predictability for each known destination. This metric calculates the probability of successful delivery of a message from source node to the destination node on the basis of history of encounters between the nodes or their visits to certain locations. When two nodes meet they exchange their Delivery Predictability with each other. A node will forward the message to another node if it has a higher value of Delivery probabilistic to the destination node. The Delivery Predictability value must decrease with time. The delivery predictability has a transitive property based on the observation that if node A frequently encounters node B and node B encounters node C then node B is good forwarders for node A's messages to node C.

F. Adaptive Fuzzy Spray and Wait

This protocol [3] does not assume any prior knowledge about the network connectivity and uses the local information, mobility of nodes to select the next best-hop for message delivery. This protocol was designed for vehicle-based disruption tolerant networks which forward the message to any node which having maximum probability of delivering the message towards the destination. MaxProp is divided into three parts namely Estimating Delivery likelihood, Complementary mechanisms and managing buffers.

In the first part of this protocol, an optimal delivery path is found by constructing a directed graph of nodes connected by edges towards the destination. A variation of Dijkstra's algorithm [9] is used to determine the shortest path out of given paths at any given point of time. The second part describes the priority order in which different type of messages are exchanged between two nodes when they discover each other. In the third part an acknowledgement is used for flushing the redundant messages when buffer is almost full. The buffer management scheme defined above leads to lowered rate of packet dropping.

G. OLSR

Optimized Link State Routing (OLSR) [11] is a well known proactive link-state single-path routing protocol that forwards packets over a minimum-cost path. In this protocol, node maintains the global topology information of the network, and using shortest hop forwarding paths each node computes the next hop for all the nodes in the network. In order to decrease the network overhead, OLSR uses Multi-Point Relays (MPRs) that prevent flooding of the broadcast messages. Because of the use of MPRs, OLSR is better for large and dense mobile networks.

The advantage of OLSR over the reactive protocols such as AODV and DSR is that the route is computed in a proactive way because it does not introduce route-discovery delay for a flow. The OLSR protocol is adapted to the network where communication is assumed to occur frequently between a large numbers of nodes. When the number of nodes increases overheads also increases. OLSR removes some of the redundancy of the flooding process, by using MPRs to flood topology information, which may be a problem in networks with weak wireless links.

IV. CONCLUSIONS

Opportunistic network (OPPNET) is the intermittent connectivity among mobile nodes from their unpredictable mobility. Opportunistic network improves the performance of wireless communication by enhancing packet forwarding in wireless links. Due to disconnection and reconnection, routing and forwarding the message is a challenging task. In this paper we present a review on the different routing protocols which has been used to improve the performance of routing in opportunistic networks. Opportunistic network may achieve significant performance in a wireless environment. by studying the various protocols it has been observed that the varying number of nodes, message size, message generation interval and node's speed affects the performance of the routing protocols.

From the results of previous paper we observed that: 1) The average residual energy is maximal for the direct delivery protocol and minimal for the maxprop protocol. 2) The average residual energy increases with increase in message generation interval and decreases with increase in message size and number of nodes. 3) When the maxprop is used, number of dead nodes is maximum and when the direct delivery protocol is used, number of dead nodes is zero.

REFERENCES

[1] Renu Dalal,Yudhvir Singh and Manju Khar, "A Review on Key Management Schemes in MANET" International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.

[2] Panagiotis Papadimitratos , Zygmunt J. Haas., "Secure message transmission in mobile ad hoc networks."

[3] J. Burgess, B. Gallagher, D . Jensen, and B. N. Levine. MaxProp: "Routing for vehicle-based disruption-tolerant networks". In P*roc. of the 25th IEEE International Conference on Computer Communication (INFOCOM'06), Barcelona, Spain,* pages 1-11. IEEE, April 2006."

[4] I. Parris and T. Henderson, "Privacy-enhanced social-network routing," *Computer Communications*, vol. 35, no. 1, pp. 62–74, 2012.

[5] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003.

[6] Ranjeet Singh, and Prof. Harwant Singh Arri, "COMPARISON OF AAMRP AND IODMRP USING SBPGP" International Journal of Computer Science and Management Research, Vol 2 Issue 3 March 2013.ISSN 2278-733X.

[7] VLADIMIR BERMAN, "Enhancing Data Security in Mobile Ad Hoc Networks via Multipath Routing and Directional Transmission".

[8] C.-M. Huang, K. chan Lan, and C.-Z. Tsai. "A survey of opportunistic networks". In *Proc*. Of the 22nd International Conference on Advanced Information Networking and Applications-Workshops (AINAW'08), GinoWan, Okinawa, Japan, pages 1672-1677.IEEE, March 2008.

[9] Rongxing Lu, Xiaodong Lin, Zhiguo Shi, Bin Ca, and Xuemin (Sherman) Shen, "IPAD: An Incentive and Privacy-Aware Data Dissemination Scheme in Opportunistic Networks" 2013 Proceedings IEEE INFOCOM.

[10] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[11] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, a. Qayyum and L. Viennot. "Simple Opportunistic Routing for wireless mesh networks". *Wireless Mesh Networks, 48-54,* Reston, VA, USA, 2006.

[12] Danai Chasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET".

[13] Vineetha S. H. and Shebin Kurian, " Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 4, Issue 4, April 2013].

[14] A. Lindgren, A. Doria, and O. Schelen. ," Probabilistic routing in intermittently connected networks". *ACM SIGMOBILE Mobile Computing and Communication* Review, 7:19-20, July 2003.

[15] J. Makhlouta , H. Harkous, F. Hutayt, and H. Artail. "Adaptive fuzzy Spray and Wait: Efficient routing for opportunistic networks". *In Proc. of the 2011 IEEE International Conference on Selected Topics in Mobile and Wireless Networking (iCost'11),* Shanghai, China, pages 64-68, IEEE, October 2011.

[16] L. Pelusi, A. Passarella, and M. Conti. ,"Opportunistic Networking: data forwarding in disconnected mobile ad-hoc networks." *IEEE Communications Magazine,* 44:131-141, Nov 2006.

[17] R. Lu, X. Lin, H. Zhu, X. Shen, and B. R. Preiss, "Pi: a practical incentive protocol for delay tolerant networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1483–1493, 2010.

[18] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 134 – 141, 2006.

[19] T. Spyropoulos , K. Psounis, and C. S. Raghavendra. Spray and wait : "An efficient routing scheme for intermittently connected mobile networks". In *Proc. of the 2005 ACM SIGCOMM Workshop on delay-Tolerant Networking (WDTN'05), Philadelphia, Pennsylvania, USA, pages 252-259.ACM Press, august 2005.*

[20] A. vahdat and D. Becker, " Epidemic Routing for partially connected ad hoc networks. Technical reportCS-2000-06, dept. of Computer Science, Duke University, 2000.

[21] S. Thadvai, D.N.Tiwari, D.Jena, M.Ma "A novel authenticated Encryption scheme with convertibility," Mathematical and Computer Modelling, vol. 58 Issue 1,July pp. 178-185 Elsevier (2012).

[22] M.A.Matin, Md.Mohir Hossain et al "Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN" IEEE Technical postgraduates (2009) International conference.

[23] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA, Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012.

[24] Ranjeet Singh, and Prof. Harwant Singh Arri, "COMPARISON OF AAMRP AND IODMRP USING SBPGP" International Journal of Computer Science and Management Research, Vol 2 Issue 3 March 2013.ISSN 2278-733X.

[25] Shiva Murthy G.Robert John D'Souza, Golla Varaprasad "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks" IEEE sensors Journal vol.12.No.10, October2012.

[26] Merin Francis, M. Sangeetha, and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013, ISSN: 2277 128X.

