ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2013

A Conceptual Survey of MANET Routing Protocols

Manimegalai T[1], Dr. Jayakumar C[2]

Assistant Professor, Department of Computer Applications, SSN College of Engineering, Chennai, TamilNadu, India. [1]

Professor, Department of Computer Science and Engineering, RMK Engineering College, Kavaraipettai, Tamil Nadu, India.[2]

Abstract: Mobile Adhoc Network (MANET) is a dynamic network formed by a collection of wireless nodes. As it is a dynamic network all the nodes involved in the network must play the role of a router at some point of time. Path must be constructed by each node if it needs to communicate with the other node. A node can find path to other node either by a proactive or a reactive or a hybrid routing protocol. Many mobility models and protocols are available to find path. Each mobility model and protocol has its own strength and weakness pertain to MANET environment. Functionality of discussed and advantages and disadvantages are compared.

Keywords: Routing, overhead, path, size

I. INTRODUCTION

MANET is a network with no permanent infrastructure. The nodes participate in the network are of wireless and mobile in nature. Since the network operates without a fixed infrastructure, each node in the network should act as a router to forward the packets of the other nodes. These nodes can move in any direction, at any speed and at any time. Many routing protocols are in existence in order to discover a path. The performance can be analysed using certain performance metrics like packet loss, delay, overhead and throughput.

A node which needs communicate with another node is responsible to find the path between them. Assurance cannot be given for the path which is been constructed because of node mobility and other issues. In general multiple paths are found between same pairs or path may be reconstructed with the existing nodes after a failure. Though there are many types of protocols and classification, they can be classified into three types in major based on the time of path construction [1,2,3,4,5,6].

- Proactive Routing Protocols: Protocols find path between each individual node before they plan to communicate. Similarly the routing information is updated periodically in a routing table to retain the path found. When there is a need for communication, nodes can immediately start to communicate without a delay as the path is already found.

- Reactive Routing Protocols: Protocols find path between a pair after they plan to communicate. Nodes do not construct path unless a need arrives. When there is a need, nodes should find path and then only they can start to communicate. The routing information of the active routes is only maintained.

- Hybrid Routing Protocols: The features of both the protocol types are combined to satisfy the requirement based on the scenario. These protocols can act as reactive or proactive in different situations like increase in network size and density.

II. ROUTING PROTOCOLS

This section describes the nature of each and every protocol considered for comparison. In a MANET environment the routing protocols use three types of control packets to find and maintain the path.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2013

- Route requisition is done from source using route request packet (RREQ)
- Reply sent from destination node using route reply packet (RREP)
- Route update is done using hello packet
- Route failure or error is intimated using route error packet (RERR).

A. Adhoc Ondemand Distance Vector (AODV)

Route is initiated by the node which needs to communicate with a destination only on a demand. The source initiates path finding through RREQ to its one hop neighbors. The packet is forwarded by an intermediate node its one hop neighbors if it is not a destination. On reception of this RREQ at destination, A RREP is generated and sent back to the source. Nodes store only the active route information which results in reduced control overhead [7].

B. Dynamic source Routing (DSR)

In DSR path finding is almost similar as in AODV. No periodic exchange of control packets. During packet forwarding in intermediate nodes, not like AODV, they store their ID and update their cache with the active routing information. Route discovery and recovery are done only when it is required. Routing overhead is scaled to the actual size [8].

C. Cluster-based routing protocol (CBRP)

Nodes are organized in a hierarchical manner and grouped into clusters. Each cluster is represented using a cluster-head. Data transmission is done through the cluster heads between the clusters which reduces the control overhead [9].

D. Fisheye State Routing (FSR)

Each node stores the link state for every destination in the network. This link state update of a destination is periodically broadcasted to its neighbors. Update messages contain information only about closer nodes and not farther [10].

E. Zone Routing Protocol (ZRP)

This hybrid protocol acts as both reactive and proactive routing protocols. Within a zone it acts as a proactive routing protocol using Intra Zone routing protocol (IARP). Between zones it acts as a reactive protocol using Inter Zone Routing Protocol (IERP). Path can be constructed to destination node within the local region using the proactively cached routing information. If the destination is away from the local region then the route discovery is done reactively through the border nodes. The border nodes pass the request by adding their ID to the RREQ to the next zone if the destination is not within the local zone [11].

F. Link Aided Routing (LAR)

Network identifies two zone namely requested zone and expected zone. Instead spreading the RREQ packets to the entire network, the packets are sent to the zones where the destination is expected to be. Using an algorithm with the GPS location the requested zone is obtained. The source node estimates the expected zone of the destination based on the previous location. The RREQ is flooded only to the requested zone inclusive of the expected zone [12].

G. On-Demand Anonymous Routing in Ad Hoc networks (ODAR)

Initial routing process of ODAR follows DSR algorithm. The protocol uses a data structure called bloom filter which stores a set of element. Each element is tested if it is a member of the set or not. Elements involved in the set or permanent. Once if the source hashes the route information it cascades it to the bloom filter. An intermediate node will forward the packet if and only if its ID is in the bloom filter, otherwise it will simply drop the packet [13].

H. Link State Routing (LSR)

Route is found using Dijkstra's shortest path method based on current conditions. Each node has topology view of the entire network and is updated regularly through link state packet (LSP). This is circulated among the neighbour nodes till all are updated [14].

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2013

I. Optimal Link State Routing (OLSR)

OLSR is a proactive routing protocol. The routing information is updated periodically through the nodes one hop neighbor selected namely multipoint relay (MPR). The traffic and control overhead is reduced as the packets are sent through the MPRs [15].

J. Destination-Sequenced Distance Vector (DSDV)

In DSDV sequence numbers are assigned by each source while route request packets are sent to neighbours, which avoid looping and help to select a latest route. Global view of network topology is not available. All the nodes in the network maintain routing information to all known destinations and route updates are done periodically [16].

K. Privacy-Preserving Location-Based On-Demand Routing in MANETs(PRISM)

Routing is done based on AODV and do not propagate topology information. PRISM mainly concentrates on the security aspect against the insider and outsider attacks. Hash of RREQ, RREP is used as a route identifier and group signatures are used for authentication [17].

L. Secure Position Aided Ad hoc Routing (SPAAR)

Along with the destination ID, distance from the source and exact coordinates are included. Specialty of SPAAR is that the routing information is encrypted with a group encryption key. The receiving node decrypts the information and the successful nodes informing the sender are the one hop neighbors. Similarly the remaining route estimation is done at the intermediate nodes by adding their IDs to the RREQ. The route cache is maintained for the reverse path. RREP generated at the destination is also in an encrypted form of details like sequence number, velocity, destination's coordinates and timestamp [18].

M. Anonymous On-Demand Routing in Mobile Ad Hoc Networks (MASK)

The node identities are masked with the help of a group pseudonym. In order to find the path, first the node which needs to communicate authenticates the neighboring node by sending a challenge with the pseudonym selected in random. Then the master key is calculated by the challenged node and gives authentication to the sender. Based on the master key both of them generate link ID and session keys [19].

N. Anonymous Routing Protocol for mobile ad hoc networks (ARM)

The RREQ is generated in such a way that the nodes except destination cannot be aware of the destination. With the help of the pseudonym the intermediate nodes can conclude that they are not the destination node. For each communication a secret key and current pseudonym are shared between the source and destination. The destination sends the RREP in an encrypted for with its broadcast ID [20].

O. Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks (AnonDSR)

The communication process involves three protocols in different levels. At first level a shared key and a nonce is generated between the source and the destination. Using this trapdoor is created in second level. Each intermediate node has a shared session key. Finally after the route discovery the communication is done using this session key [21].

P. Anonymous Location-Aided Routing in Suspicious MANETs (ALARM)

Nodes are grouped on location basis and are lead by a group manager. Each node register itself with the group manager gets a group signature. The protocol sends Location Announcement Messages (LAM) from time to time to the nodes in the group. The LAM message has details like nodes current position, time stamp and a session key. Only valid members with the signature can decrypt the packets and read. Concatenation of nodes temporary ID and the group signature forms the pseudonym [22].

Q. A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID (GeoGRID)

Geographic area is divided as a number of grids. Each grid has a grid leader. Only the leader can propagate the packets tp the members in the grid. GeoGRID is available I two versions namely flooding-based and ticket-based. GeoGRID is appreciated well in crowded MANET [23].

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2013

R. Security Aware Routing protocol (SAR)

SAR aims at security based on the trust values and trust relationships associated with adhoc nodes and this value is used to take routing decisions. Security is provided through symmetric encryption method. Routing is done only through trusted nodes to which trust values are already assigned. Nodes which satisfy the required level of security only can participate in routing [24].

S. Signal Stability Based Adaptive Routing (SSA)

In SSA the routes are analyzed and categorized as strong and weak nodes based on their signal stability. This protocol works on an on demand basis. During path finding the node selection is done through the strong nodes. Channeling the packets through the strong signal nodes avoid link failure due to signal level [25].

T. Temporally-Ordered Routing Algorithm (TORA)

TORA follows a hierarchical topology of nodes. Route construction is done on a directed acyclic graph (DAG) form. Information always flows from the higher level to the lower level as a fluid. The node which requires communicating with the destination node will find path through the upper node in upper level [26].

III. COMPARATIVE STUDY

Each routing protocol is distinguished based on its functional complexity and the flexibility. The following is a detailed comparison of the twenty routing protocols discussed in the section II. They are compared over the parameters like category, security advantage and disadvantage.

TABLE I
ANALYSIS OF PROTOCOLS

#	Protocol	Type	Security / Privacy	Advantage	Disadvantage
1	AODV	Reactive	Not specific	Reduced control overhead	Suitable only for less dense network
2	DSR	Reactive	Not specific	No periodical flood to the network	Connection setup delay is higher Performance degrades rapidly with increasing mobility
3	CBRP	Hybrid	Not specific	Reduced control overhead	Communication is possible only through cluster head
4	FSR	Reactive	Not specific	Consumes less bandwidth Reduced control overhead Reduced message size	Poor performance in small sized network
5	ZRP	Hybrid	Not specific	hybrid approach provides combined advantage of other protocols	Delay is more
6	LAR		Not specific	Reduced memory and control overhead	Knowledge over physical location of nodes required
7	ODAR	Reactive	Key & Encryption	Identity, topology and routing details are secured	False positive results in unnecessary packet forwarding
8	LSR	Proactive	Not specific	Loop free Fast route discovery	Considerable memory demand
9	OLSR	Proactive	Not specific	Immediate availability of routes	More overhead and usage of resources
10	DSDV	Proactive	Not specific	Loop free Dynamic reaction to topology changes	More overhead due to unwanted information storage
11	PRISM	Reactive	Node movement cannot be	Path discovery is done independent of current topology	Source node should determine the destination location Routing overhead is little

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2013

			traced		higher
12	SPAAR	Proactive	Third party certificate	No injection false routing information by intruders Loop Free	More Overhead
13	MASK	Reactive	Nodes are unlocatable and intractable	Source and destination anonymity End-to-end flow cannot be tracked	Resilient to wide range of attacks
14	ARM	Reactive	Destination privacy	Simple cryptographic process Done only by source and destination.	Many assumption with practical difficulty like shared secret key, pseudonym, permanent ID
15	AnonDSR	Reactive	Not specific	Good level of anonymity Scalable	Assumption of secret key
16	ALARM	Proactive	Node communication cannot be traced	Protection against outsider and insider attacks	Not suitable in large networks
17	GeoGRID	Proactive	Not specific	Better suited for crowded environment	No security measures
18	SAR	Reactive	Not specific	Suitable to different environments	Not suitable for with high-risk background
19	SSA	Reactive	Not specific	Reduces path failure by signal stability	More overhead
20	TORA	Reactive and partially proactive	Not specific	Multiple paths Suitable for dense networks	Communication is possible only by upper hierarchy

IV. CONCLUSION

There are many protocols in existence for the MANET. Each has a different working principle pertain to an environment. Working principle of 20 routing protocols are discussed here. From the study it is observed that no single protocol is best amongst all, as each has better performance over the other at a particular metric and time. Advantages and disadvantages of those protocols are compared in a table for better understanding of the protocols, which helps in selecting a protocol suitable for the environment and the scenario.

REFERENCES

[1] Mario Gerla, "Ad Hoc Networks", Springer, "Ad hoc Networks Technologies and Protocols", Chapter 3,pp. 1-22, 2005.
[2] Nadir Shah, Depei Qian and Khalid Iqbal, "Performance evaluation of multiple routing protocols using multiple mobility models for mobile ad hoc networks", Proceedings of IEEE International Multi topic Conference, pp. 56-59, 2008.
[3] Avni Khatkar, Yudhvir Sing, "Performance Evaluation of Hybrid Routing Protocols in Mobile Adhoc Networks", Proceedings of 2nd International Conference on Advanced Computing & Communication Technologies, pp. 542 – 545, 2012.
[4] Namrata Marium Chacko, Shini Sam, P.Getzi Jeba Leelipushpam, "A survey on various privacy and security features adopted in MANETs routing Protocol", Proceedings of IEEE International Muti Conference on Automation, Computing, Communication, Control and Compressed Sensing, pp. 508-513, 2013.
[5] Geethu Mohandas, Dr Salaja Silas, Shini Sam, "Survey on Routing Protocols on Mobile Adhoc Networks", Proceedings of IEEE International Muti Conference on Automation, Computing, Communication, Control and Compressed Sensing, pp. 514-517, 2013.
[6] Karmel A, Jayakumar C, "Analysis of MANET Routing Protocols Based on Traffic Type", IJREAT International Journal of Research in Engineering & Advanced Technology, Vol.1, Issue 1,pp. 1-4, 2013.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2013

[7] S.A. Hussain, K. Mahmood and E. Garcia, "Factors affecting performance of AODV", Information Technology Journal, Vol. 6, Issue 2, pp 237-241, 2007.
[8] Narendra Singh Yadav and R.P. Yadav, "The Effects of Speed on the Performance of Routing Protocols in Mobile Ad-hoc Networks", International Journal of Electronics, Circuits and Systems, Vol. 1, Issue 2, pp 79-84, 2009.
[9] Yogesh Chaba, Yudhvir Singh, Manish, "Performance Evaluation and Analysis of Cluster Based Routing Protocols in MANETs" Proceedings of IEEE/ACEEE ACT, pp. 64-66, 2009.
[10] R. Mkhija and R.Saluja, "Performance Comparison of Ad-Hoc Routing Protocol in Different Network Size", Proceedings of 2nd National Conference of Mathematical Techniques: Emerging Paradigms in Electronics and IT Industries, 2008.
[11] Ashish K. Maurya, Dinesh Singh, "Simulation based Performance Comparison of AODV, FSR and ZRP Routing Protocols in MANET", International Journal of Computer Applications, Volume 12– Issue 2, pp.23-28, 2010.
[12] Young-Bae Ko and Nitin H. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks", Springer – verlog, New York, "Wireless Networks", vol. 6, pp. 307–321, 2000.
[13] D. Sy, R. Chen, and L. Bao, "Odar: On-demand anonymous routing in ad hoc networks" , IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 267–276, 2006.
[14] C. Adjih, E. Baccelli, P. Jacquet, "Link State Routing In Wireless Adhoc Networks", Proceedings of the IEEE conference on Military communications, Volume 2 ,pp. 1274-1279, 2003.
[15] Jacquet. P, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, " Optimized link state routing protocol for ad hoc networks" Proceedings of IEEE Multi Topic International Conference on Technology for the 21st Century, pp. 62–68, 2001.
[16] Guoyou He., "Destination-sequenced distance vector (DSDV) protocol", Technical report, Helsinki University of Technology, Finland.
[17] Karim El Defrawy and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE journal on selected areas in communications, Vol. 29, Issue 10, pp. 1923-1934, 2011.
[18] S. Carter and A. Yasinsac, "Secure position aided ad hoc routing," Proceedings of IASTED International Conference on Communications and Computer Networks (CCN02), pp. 329–334, 2002.
[19] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Mask: anonymous on-demand routing in mobile ad hoc networks," IEEE Transactions on Wireless Communication, Vol. 5, Issue 9, pp. 2376–2385, 2006.
[20] S. Seys and B. Preneel, "Arm: anonymous routing protocol for mobile ad hoc networks," International Journal of Wireless and Mobile Computing., vol. 3, Issue 3, pp. 145–155, 2009.
[21] R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," Proceeding of the 3rd ACM workshop on Security of ad hoc and sensor networks, NewYork, pp. 33–42, 2005.
[22] K. El Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious MANETs", IEEE International Conference on Network Protocols, pp. 304–313, 2007.
[23] Wen-Hwa Liao, Yu-Chee Tseng, Kuo-Lun Lo, and Jang-Ping Sheu, "GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID", Journal of Internet Technology, Vol. 1, Issue 2, pp.23-32, 2000.
[24] Seung Yi, Prasad Naldurg, Robin Kravets, "Security - Aware Ad hoc Routing for Wireless Networks", Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, pp.299-302, 2001.
[25] R. Dube, C. D. Rais, K-Y. Wang and S. K. Tripathi, "Signal Stability Based Adaptive Routing for Ad Hoc Mobile Networks", IEEE Personal Communication, vol. 4, Issue 1, pp. 36-45, 1997.
[26] V.D.Park and Scott.M.Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proceedings of 16th IEEE Annual Joint Conference of Computer and Communications Societies, Vol.3, pp.1405-1413, 1997.

BIOGRAPHY

Manimegalai T received the MCA degree from University of Madras, Master of Engineering in CSE from College of Engineering, Guindy and currently pursuing PhD from Anna University. She has 19 years of teaching and industry experience. Her career commenced as a programmer at Chennai for a period of one and a half years. After her PG she changed her career to the academia with tenure of Lecturer. In 2001, she joined SSN College of Engineering and currently working as an Assistant Professor in the Department of Computer Applications.