

A Study on Working of Prominent Routing Protocols in WANETs

Randeep Kaur¹, Dr. Gagandeep Jagdev^{2*}

¹Research Scholar, PhD (Comp. Appl.), Guru Kashi University, Talwandi Sabo (PB)

²Dept. of Comp. Science, Punjabi University Guru Kashi College, Damdama Sahib (PB)

***Corresponding Author:** Dr. Gagandeep Jagdev, Dept. of Comp. Science, Punjabi University Guru Kashi College, Damdama Sahib (PB)

Abstract: WANET (Wireless Ad hoc Network) is a decentralized wireless network. WANET does not have any pre-existing infrastructure. Each node in WANET forward data to other nodes in the network. The research paper is focused on discussing the working of proactive and reactive protocols involved in WANETs. The research paper elaborates the strong features of WANETs like high performing capacity, use of unlicensed frequency spectrum, quick circulation of information around sender, and no single point of failure. The research paper details the working of prominent proactive routing protocols (DSDV, WRP, CGSR) and reactive routing protocols (DSR, AODV, TORA).

Keywords: AODV, DSDV, DSR, TORA, WANET, WRP.

1. INTRODUCTION

WANET (Wireless Ad-hoc Network) makes use of radio frequencies in air to transfer data between receiver and sender instead of using physical cables. WANETs are decentralized kind of networks. There is no defined infrastructure in WANETs [1, 2]. In such networks, the need for laying wires and cables is eliminated. As the devices connect spontaneously, the network keeps on building and changing. The nodes involved in the network forward packets to and from each other and are connected dynamically in a random manner. Each node of network acts as a router and participate in discovery of routes to other nodes involved in the network. The primary benefits of ad-hoc networks is its low cost, flexibility, and robustness. Ad-hoc networks are preferred where there is no infrastructure or it's expensive to build it. Ad-hoc are useful in emergency rescue and search operations, in meetings where people intend to quickly share information, and carrying out data acquisition operations in inhospitable environment [3]. Such networks can operate standalone and can even be connected with internet. So, it can be concluded that WANET is a decentralized kind of wireless network where all devices involved within the network has equal status. The key features of WANETs are mentioned as under [4].

- WANET is a self-configuring infrastructure less network.
- WANET is a self-healing and self-forming network.
- The data is transmitted via multiple hops.
- The scalability enhances because of its decentralized nature.

In WANETs, the nodes are not acquainted with the topology of their networks and are supposed to discover it. A newly formed node broadcasts its presence and listens for announcements broadcasted by its neighbors. Each node learn about other nearby nodes and how to approach them. Fig. 1 shows the setup of a WANET [5, 16].

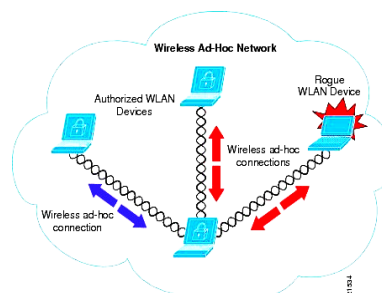


Fig1. The figure shows the set up for a WANET

2. TYPES OF WANETS

WANET can be classified into three different categories as shown in Fig. 2.

- Wireless Mesh Network (WMN)
- Mobile Ad-hoc Network (MANET)
- Vehicle Ad-hoc Network (VANET)
- Intelligent Vehicle Ad-hoc Network (InVANET)
- Wireless Sensor Network (WSN)

The research paper elaborates the working of MANET.

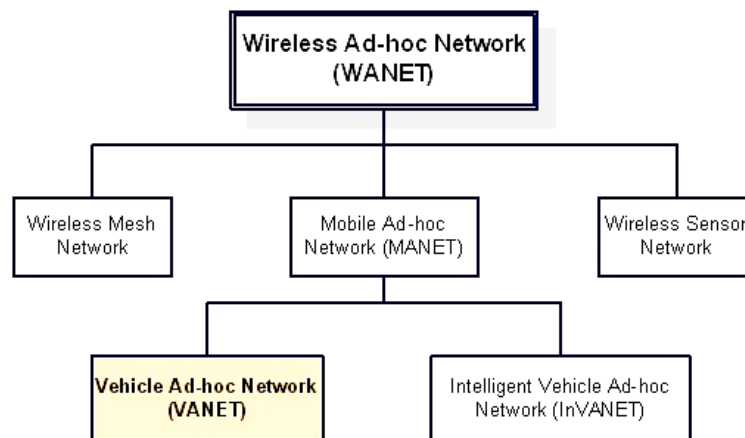


Fig2. The figure depicts the classification of WANET

MANET is a kind of WANET where each node is free to move autonomously in any direction. A node can change its connections with other nodes frequently. Each node acts as a router as it forward traffic isolated to its own use. The biggest challenge concerned with MANET is to equip each device to regularly preserve the information needed to properly route traffic [6, 7, 16, 17]. The ad-hoc routing protocols related with MANET are categorized as under.

- Proactive (Table-driven) protocols
- Reactive (On-Demand) protocols
- Hybrid protocols

2.1. Proactive Routing Protocols

In proactive routing protocols, the information relevant with routing is stored in routing table and rarely changed when there is a topology change. If a route is present with the node before the traffic arrives, the transmission takes place instantly. But if this is not the case, the traffic packets are forced to wait in queue until the corresponding node receives routing information to particular destination. This kind of protocol is not favored in case of networks comprising large number of nodes as it is hard to maintain the routing information of each node in node's routing table and additional overhead cost involved in maintaining up-to-date information. The few prominent routing protocols are mentioned as under [8, 9, 10].

- Destination Sequenced Distance Vector (DSDV)
- Wireless Routing Protocol (WRP)
- Cluster-head Gateway Switch Routing (CGSR)

a) DSDV (Destination Sequenced Distance Vector)

DSDV is developed by Pravin Bhagwat and Charles E. Perkins. The transmission of packets take place between mobile nodes by utilizing routing tables stored with mobile node. Every routing table consists list of all possible destinations along with number of hops to each. Every route table entry has a sequence number (SN) initiated by the destination node. Routing information is promoted by multicasting the packets communicated periodically as topological changes are noticed. Consider Fig. 3 where node A wants to transmit data to node C which is not in the coverage region of node A. But

both node A and node C are in coverage region of node B. Therefore, node A transmit packet to node B which acts as routing agency for forwarding the same packet to node C.

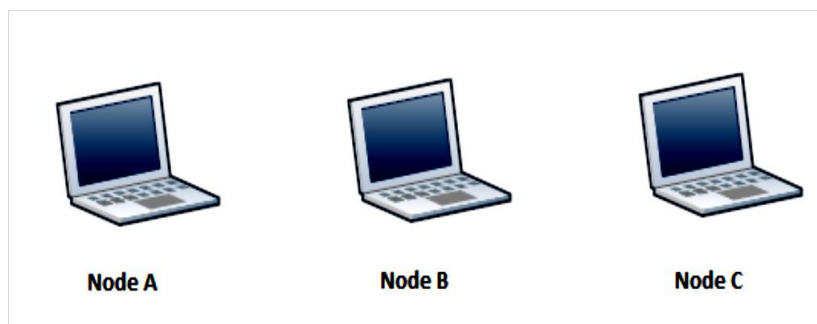


Fig3. The figure depicts the set up for MANET

b) WRP (Wireless Routing Protocol)

In WRP, each node needs to maintain the below mentioned four tables.

- Distance Table – It contains the network view of the neighbors of the node.
- Routing Table – It contains network view for all known destinations like shortest distance to destinations, the successor node, the predecessor node, and the flag indicating the status of the path.
- Link Cost Table – It includes cost relevant information like number of hops involved to reach destination and number of update periods passed since last successful update of the link.
- Message Retransmission List (MRL) – It includes counter for each entry and with each update message the counter is decremented.

Fig. 4 and Table 1 depicts the figure and its routing table respectively.

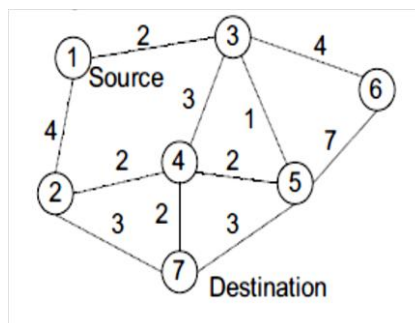


Fig4. The figure depicts the graph under study having node 1 as source and node 7 as destination

Table1. Routing table as per the graph shown in Fig. 4

Dest	Next	Pred	Cost
7	7	7	0
6	3	5	8
5	7	5	3
4	7	4	2
3	5	5	4
2	7	2	3
1	3	5	6

Fig. 5 shows a link break between node 5 and node 7. Whenever a node detects a link break, it transmits an update message to its neighbors with link cost set to 1. The affected nodes update their respective routes as they receive an update message. The node responsible for initiating the update message finds another route from its distance table. The node updates its routing table and transmits the updated message to its neighbors. The update takes place only if this newly received route is better than the already existing one. The updated routing table is shown in Table 2 as per Fig. 5.

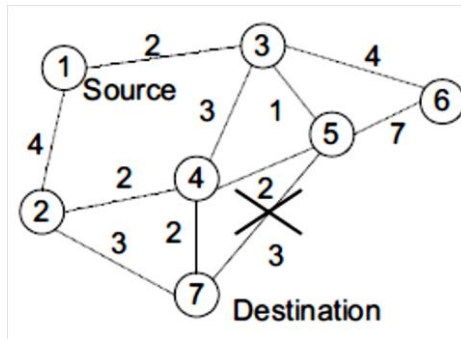


Fig5. The figure depicts the graph with a broken link

Table2. Updated routing table as per Fig. 5

Dest	Next	Pred	Cost
7	7	7	0
6	3	4	9
5	4	4	4
4	7	4	2
3	4	4	5
2	7	2	3
1	2	2	7

c) CGSR (Cluster-head Gateway Switch Routing)

In this protocol, the nodes are organized into clusters with each cluster having an elected cluster head. The responsibility of cluster head is to provide coordination within its transmission range. The bandwidth is shared between nodes using token based scheduling. Each communication that takes place is bound to pass through cluster head. The communication between clusters takes place using the common nodes, i.e. the gateways having two interfaces as shown in Fig. 6. This protocol comprises of cluster member table responsible for containing the destination cluster head for every node and routing table comprising the next hop node for the destination cluster. A node obtains a token from its respective cluster head. If the node has a packet to transmit, it sets the destination cluster and the next hop. The routed packet moves alternatively between the cluster head and the gateway as shown below.

A -> H1 -> G1 -> H2 -> G2 -> -> Hi -> Gi -> -> Gn -> Hn -> B

Where Gi refers to the gateway I and Hi refers to the cluster head i

Route reconfiguration takes place only when there is any alteration in cluster heads and the cluster member table consists of stale entries.

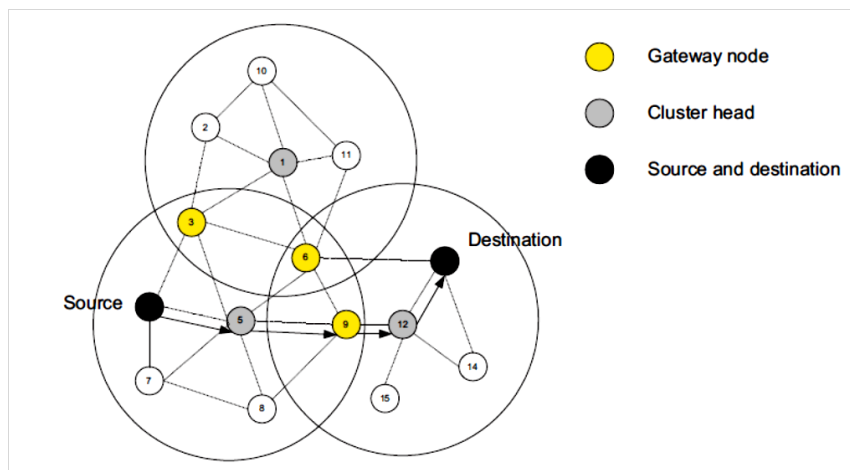


Fig6. The figure implements the working of CGSR protocol

2.2. Reactive Routing Protocols/ on-Demand Routing Protocols

The on-demand routing protocols suggested for MANETs, such as Dynamic Source Routing (DSR) Protocol, Ad-Hoc On-Demand Distance Vector (AODV) Routing, Temporally Ordered Routing Algorithm (TORA) and Associativity Based Routing (ABR) etc., basically make use of broadcast based methods for route discovery. They differ in their routing packet formats, data structures maintained by each node, various optimizations applied in route discovery and in their approach for maintaining routes. But reactive routing protocols find a route only when it is required. Whenever there is a path failure, an optional route is chosen [11, 12, 13, 16].

a) AODV (Adhoc On-Demand Distance Vector)

The AODV routing protocol builds route between nodes only on the request of the source nodes. It is because of this that AODV does not create any extra traffic on communication links. As long as the sources require the routes, the routes are maintained. In case of multicast group members, the trees are formed. The sequence numbers are used to guarantee route freshness. These are loop-free and self-starting and are capable of scaling to number of mobile nodes [14, 15, 17].

The networks remain silent until connections are established. The network nodes interested in connections broadcast a request for connection. The nodes left behind are responsible for forwarding the message and recording the node that requested the connection. Thus, series of temporary routes are created back to the requesting node.

A node that holds a route to the desired node and receives such messages sends a backward message to the requesting node via temporary routes. The node that started the request uses the route encompassing the least number of hops through other nodes. The unused entries in the routing tables are recycled after some time. In case of link failure, the routing error is send back to the transmitting node and the process is repeated.

Let us consider the case of a reactive routing protocol (AODV) and check the possible route of a route reply packet (RREP) from a destination to a source. Here the node A need to set up a route to node J (Fig. 7).

1. To establish the route, A needs to broadcast RREQ packet to all the other neighboring nodes in the network.
2. When node J receives the RREQ packet, it sends back a RREP packet.
3. This packet is unicasted to the sender node (i.e. A) through the other neighboring nodes.

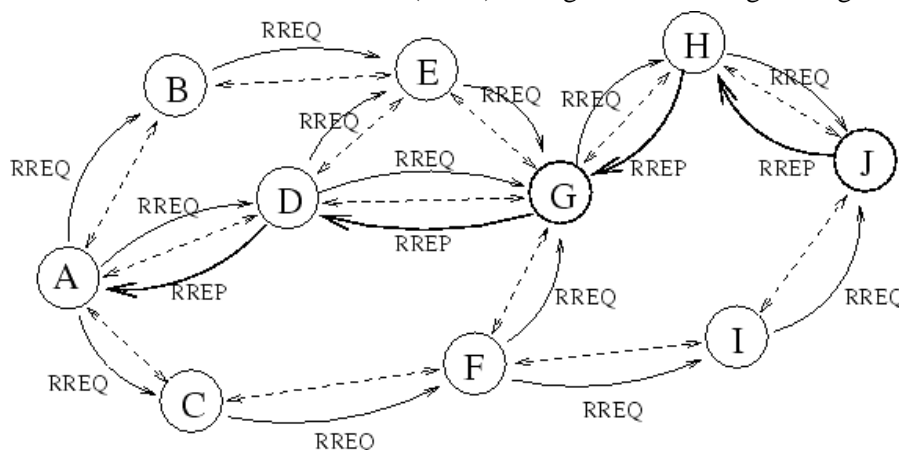


Fig7. The figure illustrates the route set up process from node A to node J

b) DSR (Dynamic Source Routing)

DSR is precisely designed for multi-hop wireless ad hoc networks. DSR enables the network to be self-configuring and self-organizing without the requirement for any existing network infrastructure. This protocol is composed of the two main mechanisms of discovering the route and maintaining it. As the protocol operates completely on-demand, it allows reduction in routing packet overhead to only those that need to react to the changes in the routes currently in use. The protocol enables multiple routes to destination and enables sender to select and govern the routes used in routing its

packets. It provides loop-free routing and fast recovery when routes witnesses network change. It works well for MANETs having up to 200 nodes and work well with higher mobility rates.

In the Fig. 8, the route discovery procedure is shown where S1 is the source node and S7 is the destination node.

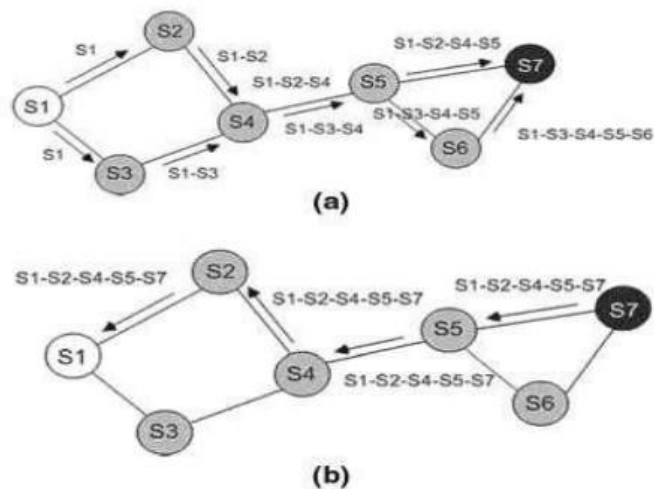


Fig8. The figure depicts the route discovery (a) and the route reply (b) as per working of DSR routing protocol

In this example, the destination S7, gets the request through two paths. One path is chosen based on route records and the reply is send back to the source path in reverse direction. At each hop, the best route with minimum hop is stored. Example shows the route record status at each hop to reach the destination from the source node. Here, the chosen route is S1-S2-S4-S5-S7.

c) TORA (Temporally Ordered Routing Protocol)

TORA works well in dynamic network. Its objective is to limit control message propagation in dynamic computing environment. Whenever a node has to send data to particular destination, it has to initiate a query. Three primary tasks performed by TORA are mentioned as under.

- Creating route from source to destination
- Maintaining the created route
- Removing the route when it is no longer valid

3. CONCLUSION

WANETs have a bright future and is been widely utilized in different sectors like industry, educational institutes, on roads, shopping malls, military, health care etc. because of ease in deploying it where infrastructure is impractical. The research paper illustrated working of different pro-active and reactive routing protocols. Each protocol has its own pros and cons related to it. The prominent characteristics of both proactive and reactive protocols are summarized as under.

Proactive Protocols

- Consistent; up to date routing information
- Table driven; maintains one or more routing tables to store routing information
- No latency in route discovery
- Continuously evaluates routes
- Involves large number of control packets which are necessary to keep network information current
- A lot of routing information may never be used

Reactive protocols

- On-demand operation

- Route discovery is done by global search
- There are delays due to route discovery
- No control packet for routing table maintenance
- Most appropriate for environments in which nodes move around a lot
- Involves route discovery process
- Involved maintenance of routes

REFERENCES

- [1] Ismail, Nurul Halimatul Asmak, and Rosilah Hassan. "6LoWPAN local repair using bio inspired artificial bee colony routing protocol." *Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on. IEEE, 2012.*
- [2] Gupta, Kunal, Mukesh Sharma, and Parmanand Sharma. "Lossless compression based Kmp technique." *Procedia Technology*11 (2013): 281-287.
- [3] Ramamoorthy, H. Vignesh, and H. Karthikeyani. "Hybrid routing scheme of multi agent ant based system in MANET combination of proactive and reactive." *Optimization, Reliability, and Information Technology (ICROIT), 2014 International Conference on. IEEE, 2014.*
- [4] Alexandros Giagkos, and Myra S. Wilson, "BEEIP –Swarm Intelligence based routing for wireless ad hoc networks", *Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014. Information Sciences* 265 (2014): 23-35.
- [5] Nai-Wei Lo and Fang-Ling Liu "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET", *Vol 234, 2013, pp. 59-65.*
- [6] Mistry N. H., Jinwala D. C., Zaveri M. A., "MOSAODV: Solution to Secure AODV against Blackhole Attack", *International Journal of Computer Science and Network Security*, Vol. 1, No. 3 December 2009, pp. 42–45.
- [7] Aditi Kumar, Parveen Thakur, "Routing attacks and their Counter Strategies in MANET" ,*International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 5, May 2014.
- [8] Raj P. N., Swadas P. B., DPRAODV," A Dynamic Learning System against Blackhole Attack in AODV Based MANET ", *International Journal of Computer Science Issues*, Vol. 2,2009, pp. 54-59.
- [9] Bhoomika Patel, Khushboo Trivedi, "Improving AODV Routing Protocol against Black Hole Attack based on MANET", *International Journal of Computer Science and Information Technologies*, Vol. 5 (3) , 2014,pp.3586-3589.
- [10] Q. Nadia, S. Fatin, A. Hamid, "Mobile Ad Hoc Networking Protocols' Evaluation Through Simulation for Quality of Services", *IAENG International Journal of Computer Science*, 36: 1, IJCS_36_1_10, Feb. 2009.
- [11] H. P. Wang and L. Cui, "An Enhanced AODV for Mobile Ad Hoc Network" ,*7th International Conference on Machine Learning and Cybernetics, Kunming, China, 12-15 July 2008*, pp. 1135-1140.
- [12] Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit, " A Novel Approach for Detection of Blackhole Attacks" ,*IOSR Journal of Computer Engineering (IOSR-JCE) , Volume 16, Issue 2, Ver. V , Mar-Apr. 2014 ,pp. 69-74.*
- [13] A. A. Pirzada and C. McDonald, "Secure Routing with the AODV Protocol" ,*2005 Asia-Pacific Conference on Communications, Perth, WA, 2005, pp. 57-61.*
- [14] Nital Mistry, Devesh C Jinwala, "Improving AODV Protocol against Blackhole Attacks", *International MultiConference Of Engineers and Computer Scientists 2010 ,Vol 2 IMECS 2010, March 17 - 19, 2010.*
- [15] J. CAI, P. YI, J. CHEN, Z. WANG, N. LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Networks ", *2010 24th IEEE International Conference on Advanced Information networking and Application, 2010. <http://www.eexploria.com/routing-protocols-in-manets/>; Last Accessed: 22nd March 2018.*
- [16] Saket, Satish Kumar Negi et al.; "A Comparison of AODV Routing Protocols to Prevent Black Hole Attack in Manet"; *International Journal of Future Revolution in Computer Science & Communication Engineering*, Vol. 4 Issue 1, January 2018.

AUTHOR'S BIOGRAPHY



Dr. Gagandeep Jagdev, is a faculty member in Dept. of Computer Science, Punjabi University Guru Kashi College, Damdama Sahib (PB). His total teaching experience is above 11 years and has 123 international and national publications in reputed journals and conferences to his credit. He is also a member of editorial board of several international peer-reviewed journals and has been active Technical Program Committee member of several international and national conferences conducted by renowned universities and academic institutions. His field of expertise is Big Data, ANN, Biometrics, RFID, Cloud Computing, Cryptography, and VANETS.

Citation: Randeep Kaur & Dr. Gagandeep Jagdev, (2018) "A Study on Working of Prominent Routing Protocols in WANETs", *International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)*, 5(1), pp.26-33. DOI: <http://dx.doi.org/10.20431/2349-4859.0501004>

Copyright: © 2018 Randeep Kaur & Dr. Gagandeep Jagdev, This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.