Mobile Ad-hoc Networking with AODV: A Review

RUTVIJ H. JHAVERI
Research Scholar, Department of Computer Engineering,
CSPIT, Charotar University of Science & Technology, Changa,
Gujarat, India.
and
NARENDRA M. PATEL
Associate Professor, Department of Computer Engineering,
Birla Vishvakarma Mahavidyalaya, Vallabh Vidyanagar,
Gujarat, India.

Mobile Ad-hoc Networks (MANETs) are becoming a promising and popular way to carry out ubiquitous computing in numerous vital applications. Unique characteristics of these spontaneous networks induce several challenges in the resource constraint environment. In this paper, firstly, we discuss these challenges and research work carried out for various applications of MANETs. Operations of a routing protocol become vital in this unstable multi-hop environment. In this paper, we present classification of MANET routing protocols and study a popular reactive routing protocol, Ad-hoc On-demand Distance Vector (AODV). We also study basic operations of AODV and, present its variants and real world implementations. Furthermore, we study the design issues of AODV protocol and review the recent research works carried out to address these issues by modifying AODV protocol. In spite of the research work of over a decade on the AODV design, there still exist open challenges that pave the way for further research on this prominent on-demand protocol.

Keywords: MANETs, Routing Protocols, AODV protocol, Variants of AODV, Implementations of AODV, Recent Research on AODV, Research Scope.

1. INTRODUCTION

MANETs are self-organized, self-configuring, distributive, infrastructure-less and dynamic wireless networks having collection of autonomous mobile nodes [Gwalani et al. 2003; Shi et al. 2003] as shown in the Fig. 1. They are the solution to the requirement of spontaneous and adaptive network setup when nothing works [Gwalani et al. 2003; Simaremare et al. 2014]. Due to the limited communication range of these low-energy nodes, each node performs the dual task of being a source/destination of some packets and cooperating each other by acting as a router to forward the packets to another node towards the final destination, in a multi-hop way [Gwalani et al. 2003]. Cooperation between the mobile nodes is a key factor for successful data transmission in these temporary networks [Wu et al. 2007].

Low-cost infrastructure, rapid deployment capability, scalability and ease of installation make MANETs an important part of the next generation networks [Li et al. 2011; Prathapani et al. 2013]; they can be used for providing attractive services for variety of applications such as community networking, disaster relief management, interactive conference meetings, virtual classrooms, automated battlefields, military operations, mobile offices, vehicular computing, personal area and home networking, sensor networks, wild life monitoring, smart agriculture, ad hoc gaming and many more [Islam et al. 2013; Jhaveri et al. 2012a; Shi et al. 2003; Wu et al. 2007]. However, autonomous nature, wireless radio medium, dynamic topology, lack of central coordination,

Authors′ addresses: Rutvij H. Jhaveri, SVM Institute of Technology, Department of Computer Engineering, College Campus, Old N.H.-8, Bharuch-392001, Gujarat, India; Narendra M. Patel, Department of Computer Engineering, Birla Vishvakarma Mahavidyalaya, Vallabh Vidyanagar-388120, Gujarat, India.

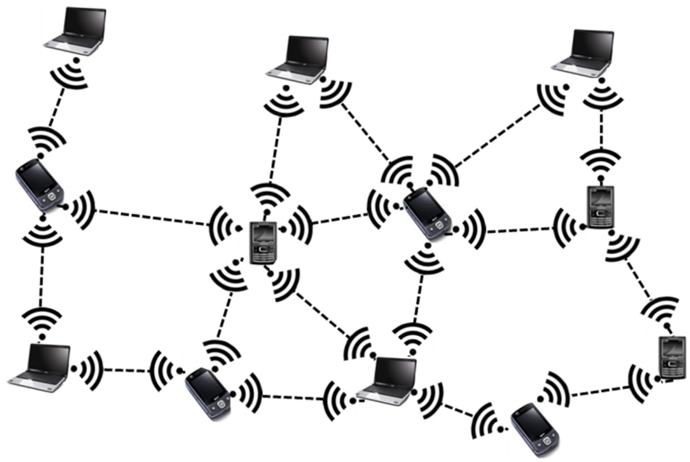


Figure. 1: A Mobile Ad-hoc Network.

resource constraints and limited physical security induce several challenges in MANETs.

Dynamic topology along with low bandwidth and limited battery power makes it difficult to organize communication in MANETs [Mishra et al. 2013]. Thus, routing becomes a key aspect which largely decides the performance of MANET with respect to packet delivery rate, end-to-end delay, routing overhead, throughput and so on [Li et al. 2011]. Therefore, the design of routing protocol plays a vital role in efficient functioning of the network. In 1996, the Internet Engineering Task Force (IETF) initiated the task to standardize IP routing protocol functionality for wireless routing applications for both static and dynamic networks [Wu et al. 2007].

Routing protocols in MANETs are generally classified into three categories [Jhaveri et al. 2010]: Proactive Protocols, Reactive Protocols and Hybrid Protocols. Proactive protocols [Li et al. 2011] are table-driven protocols that construct routes in advance. They constantly update the lists of destinations and routes by periodically broadcasting routing information. Routing tables of the nodes are updated every time when topology changes. Due to high overhead of updating routing tables, they are not suitable for network applications having real-time requirements. On the other side, reactive protocols [Jhaveri et al. 2012a] respond on demand when there is a requirement of sending data packets. To discover the path, request control packets are flooded in the network and seek for a reply packet from a node having path to the destination. As there is no requirement of frequent updates, overhead and bandwidth consumption are lower and therefore, they are widely used in a variety of applications. However, they need higher latency time during route construction. Hybrid protocols [Jhaveri et al. 2012a] combine the advantages of table-driven and on-demand routing protocols to establish best routes to the destination. Initially, proactive routing is used to establish routes; when there is a need to serve demands of other nodes, reactive flooding is used. Each node maintains routing information only for its own routing zone; the key disadvantage of this class of routing protocols is that, the rate of change in traffic volume decides the reaction to traffic demand. In this paper, we present the classification of routing protocols according to their designs and operations.

We focus on a popular and widely used routing protocol for mobile ad-hoc networks, AODV [Fehnker et al. 2012; Soni et al. 2013]. AODV is a reactive routing protocol which uses the concept of sequence numbers to ensure that latest route to the destination is established. It provides better energy efficiency and lower connection establishment delay compared to other reactive protocols. Due to its popularity, different variants have been proposed over the years, to satisfy application specific requirements. Moreover, various organizations have developed different implementations of AODV for its verification and use in real world applications. In spite of its popularity and advantages, there have been several loopholes in the original design of this protocol; therefore, researchers have focused on improvisation of AODV by addressing various design issues. In this paper, we discuss recent research work and open challenges that would assist researchers to carry out further research on AODV-based MANETs.

The remainder of paper is organized as shown in the Fig. 2. Section 2 contains overview of MANET technology, its challenges, classification of MANET routing protocols and applications research review; Section 3 describes working principles, variants, real world implementations and design issues of AODV; Section 4 surveys the recent research works carried out on AODV; Section 5 addresses future scope for improvement in the design of AODV and its variants; conclusions based on the study are provided in Section 6.

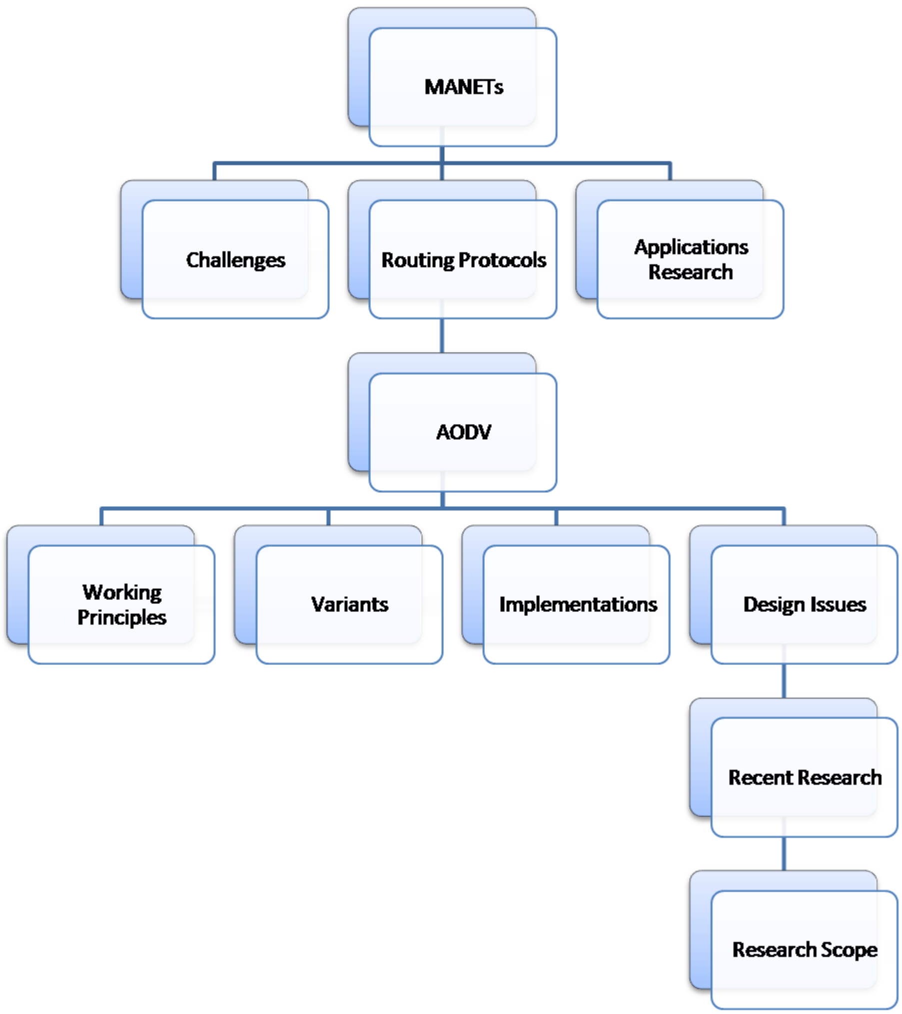


Figure. 2: Structural design of the paper.

2. MOBILE AD-HOC NETWORKING

Ad hoc networking is a rapidly growing field due to increase in the popularity of mobile devices and wireless networks in the past few years. This technology enables users to communicate in multi-hop environment regardless of their geographical location and without any fixed infrastructure [Goyal et al. 2011]. MANETs do not depend on a permanent base station for communication and broadcasting information. This temporary network may work in isolation or may have gateways/interface with a fixed network [Wu et al. 2007]. In this autonomous system, each mobile node is equipped with an antenna for wireless transmission/reception that may be omnidirectional (for broadcasting), highly-directional (point-to-point communication) or a combination [Wu et al. 2007]. Node mobility, adaption to transmission/reception parameters and arrivals/departures of nodes may change the network topology with time [Joshi et al. 2011]. Depending upon node capabilities, node responsibilities, mobility patterns, traffic characteristics and network characteristics, MANETs can have different variations as follows [Mamatha et al. 2010; Sivalingam et al. 2003]:

—If transmission and radio ranges of all nodes are equal, nodes in the network have symmetric capabilities. If the ranges are not equal, nodes have asymmetric capabilities.

—If all nodes perform the same role, they have symmetric responsibilities. In case of asymmetric responsibilities, few nodes may be appointed as cluster heads for the nearby nodes, or only some nodes may route the packets.

—Various mobility patterns can be possible depending upon the application (students sitting in class room, citywide taxi cabs, soldier movements or movement of disaster management team). It can be categorized by speed of mobile nodes, predictability or direction/ pattern of movement.

—Various MANETs may have different traffic characteristics such as timeliness or reliability requirements, bit rates requirements, unicasting/ multicasting/ geocasting or host-based/ content-based/ capability-based addressing.

—MANETs can also co-operate or co-exist with another infrastructure based network(s).

2.1 Unique MANET Challenges

MANETs face numerous challenges [Basagni et al. 2004; Conti et al. 2014; Goyal et al. 2011; Mamatha et al. 2010; Wu et al. 2007] due to node mobility, resource constraints, unreliable links, wireless radio medium, lack of infrastructure, absence of centralized entity and design of conventional routing protocols [Yang et al. 2004; Mohammad et al. 2014]:

—Node mobility: The network topology in MANETs may change quickly and unpredictably due to frequent node movements. Therefore, they suffer from frequent route changes and high packet loss. Moreover, frequently moving nodes may cause network partitions which in turn, degrade Quality-of-Service (QoS) levels; therefore, it becomes vital to improve QoS levels in this highly dynamic environment.

—Resource constraints: The light-weight mobile devices have limited battery power, bandwidth, storage capacity and CPU capability. Therefore, it is a challenge to design a power efficient system which optimally uses the available resources, balances traffic load among the nodes, provides QoS levels and controls selfish nodes from exploiting the resources.

—Unreliable links: Wireless links in the network are highly error prone and can often break down. Moreover, they may cause interference, frequent path breaks, increase in collisions, high bit error rate and high packet loss; controlling such factors to maintain reliability of wireless links is imperative.

—Wireless radio medium: The radio channel is broadcast in nature and shared by all nodes in the network. Thus, it is available to legitimate users as well as to attackers. Standard security mechanism can achieve wider protection and desirable network performance. Therefore, security aspect needs to be addressed in order to achieve these goals, to stop adversaries from exploiting the conditions and to build mutual trust among the nodes.

—Lack of infrastructure and centralized entity: Due to lack of infrastructure and centralized monitoring, security control and key management becomes a challenging task. Moreover, as network management has to be distributed across the network, fault detection and management becomes more challenging. In addition to this, it makes the design of routing protocol more challenging.

—Design of routing protocol: The role of routing protocol becomes vital with constantly changing network topology in a hostile environment. The conventional routing protocols consider co-operative trusted environment and therefore, they are prone to several network layer attacks. Furthermore, most of the routing protocols are designed for networks having fixed or small number of nodes. Thus, scalability presents some challenges in areas such as addressing, location management, configuration management, interoperability and supporting high-capacity wireless technologies. Therefore, designing of routing protocol becomes a vital job in order to set up a smooth and secured transmission across the network.

2.2 Routing Protocols in MANET

Role of a routing protocol becomes more challenging in a highly dynamic, scalable and hostile setting. Depending upon their design and operation criteria, routing protocols are classified [Mohammad et al. 2014] as follows:

2.2.1 *Source Initiated Vs Table-driven protocols.* On the basis of the method used to discover and maintain routes, MANET routing protocols can be classified as: Source initiated and Table-driven protocols [Jhaveri et al. 2013; Mohammad et al. 2014; Quispe et al. 2014].

As mentioned earlier, source initiated (reactive) routing protocols determine routes when needed and update the routing tables on-demand. They save energy of the mobile nodes as no frequent network updates are required; thus, they are useful in applications such as rescue scenarios where energy saving is imperative. However, the latency time required to initiate communications is higher and reaction to topological changes is slower. AODV and Dynamic Source Routing (DSR) are among the most prominent reactive protocols.

Table-driven (proactive) routing protocols keep pre-calculated updated routes for each node and maintain routing information of all routes, even though it is not required. There is frequent exchange of control information between the nodes to keep routing tables refreshed, and as a result, each node contains updated routes to other nodes in the network; as a consequence of this, bandwidth utilization and energy consumption get increased. Therefore, they require significant amount of resources to use them in emergency scenarios or in highly dynamic network applications [Raut et al. 2013]; they can be of good use in static topology. Destination-Sequence Distance-Vector (DSDV) and Optimized Link State Routing (OLSR) are most known proactive protocols.

In a hybrid routing protocol, initially proactively established routes are used and then, reactive flooding is used to establish route for additional demands of path establishment; Zone Routing Protocol (ZRP) is an example of hybrid protocols.

2.2.2 *Single path Vs Multipath protocols.* On the basis of number of routes computed between source and destination, the routing protocols can be categorized as: Single path and Multipath protocols [Mueller et al. 2004; Mohammad et al. 2014; Yi et al. 2011b].

Single path (unipath) routing protocols calculate a single route from the source to the destination; single path routing may not provide enough bandwidth for a connection. Moreover, they offer less resistance to fault tolerance and initiate frequent route discovery process for a source-destination pair, especially, in high density/mobility scenarios. AODV and DSR are the examples of single path routing protocols.

Multipath routing protocols provide multiple paths to route data packets simultaneously and satisfy the bandwidth requirement of an application by aggregating bandwidth of those paths. Their performance in terms of end-to-end delay gets improved due to higher bandwidth. Reactive multipath routing provides load balancing and energy efficiency. Furthermore, node-disjoint paths offer high degree of fault-tolerance. However, the achievable throughput may be limited by radio interference during transmissions; although, it is better than the single path routing in high density scenarios [Pham et al. 2003]. Ad-hoc On-demand Multipath Distance Vector (AOMDV) protocol is an example of multipath routing protocol.

2.2.3 *Flat Vs Hierarchical protocols.* On the basis of the role played by mobile nodes, routing protocols can be classified as: Flat and Hierarchical protocols [Al-Karaki et al. 2004; Mohammad et al. 2014].

Networks using flat routing protocols comprise of nodes having same role and routing functionality. The information is distributed and no effort is made to organize traffic or network. Though the methodology is efficient and uncomplicated for small networks, it takes a long time for routing information to reach to remote nodes in large networks due to volume of routing information. Routing Information Protocol (RIP) is an example of flat routing protocols.

Hierarchical (cluster-based) protocols solve the issues of flat routing protocols by creating clusters of mobile nodes on the basis of their functionalities and in turn, forming a hierarchy. In order to save energy, the cluster head, usually a resourceful node, performs aggregation and reduction of data. These protocols try to keep local information local, until it is really needed by another cluster or super cluster; this concept allows long distance data to transmit efficiently to other network partition which in turn, minimizes traffic congestion. Open Shortest Path First (OSPF) is an example of such protocols which can be configured as a hierarchical protocol.

2.3 Review on MANET Applications Research

With the wireless evolution and increase in the usage of lightweight mobile devices, ad-hoc technologies have gained importance for their usages in widespread applications in recent years [Helen et al. 2014]. Significant study and research is going on for developing MANET applications due to their high adaptability and ability to connect anytime and anywhere in infrastructureless environments [Ning et al. 2005]. Hoebeke et al. [2004] provided an overview of MANET applications in various scenarios such as fire fighting and policing, environmental disaster, military communication, automated battlefield, medical staff support system, e-payment, shopping mall system, mobile offices, dynamic database access, conferences and meeting rooms, inter-vehicle network, traffic monitoring system, communications during lectures or meetings, multiplayer gaming, robotic pets, animal tracking, call-forwarding, location specific services, outdoor Internet access and many more. A review of some research work carried out for a variety of MANET applications by various researchers is presented in Table I:

Table I: Review on research work carried out on MANET applications.

Authors	Objective	Description
Yi et al.[2011a]	Improving video content delivery services to destination	A multipath routing approach with Unequal Error Protection (UEP) is proposed to transmit H.264/SVC video stream over MANET; the proposed scheme protects the data with higher priority over the packet lossy networks.
Mohammed et al. [2012]	Modeling distributed database systems using MANETs	Issues such as optimizing mobile queries, caching and replicating data, managing transactions, power constraints, resource availability, response time, QoS and data broadcast are addressed; the proposed approach replicates data and would overcome the problems related to node mobility or link disconnection in MANET environments.
Budke et al. [2006]	Addressing challenges in real-time multiplayer gaming	QoS extensions such as priority queuing and backup route are evaluated using simulations; new extensions such as hop-constrained queuing timeouts and rate control policies are proposed for IEEE 802.11 MANETs.

Continued on next page

Table I – continued from previous page

Authors	Objective	Description
Rajabhushanam et al. [2011]	Analyzing the performance of MANET in battlefield environment	The use of MANETs is visualized in situation awareness systems for maneuvering war fighters and remote unmanned micro-sensor networks; Aiding the network with GPS-based location aware routing is recommended for addressing spatial location issues to improve QoS and security aspects in this hostile environment.
Chibelushi et al. [2013]	Embedding MANETs with identification management framework	The use of MANETs embedded with identification management framework is presented which uses remote healthcare devices with sensors for healthcare and medical applications on Internet of Things (IoT); critical implementation factors are examined such as organizational case, project management and technological infrastructure.
Kumar et al. [2013]	Modeling disaster management system	A view of disaster management architecture is presented; case studies of technologies used for satellite based weather warning in India, emergency response system in USA, pre-tsunami warning system and tsunami disaster information alert system in India are reviewed; the future emergency networks are envisioned to provide not only voice-centric services, but also to provide services such as live video streaming, location and status information, and voice-over-IP (VoIP) that demand high bandwidth and rapid deployment.
Kingsbury et al. [2009]	Investigating feasibility of MANETs to offer connectivity in air-craft to land-based communication infrastructure for airlines operators and air traffic control units	A model is built with airline schedule data to predict aircraft position and feasible communication links between aircraft and ground stations; simulation is carried out to address system issues such as optimal network location, aircraft mobility and communication link performance; important factors are found affecting performance of the system such as minimum number of connections, antenna steering restrictions and behavior of the system.
Wietrzyk et al. [2008]	Devising a cost-effective and secured delay tolerant store and forward architecture using body area network for cattle monitoring system	It was studied that wireless devices mounted on the animals can reduce reliance on human labor, and can increase profitability and efficiency of cattle production; the multi-hop communication increases battery life of light-weight devices and combat potential disconnections; the proposed system provides data retention, custom event detection, issue notifications, remote answers and in-situ queries.

Continued on next page

Table I – continued from previous page

Authors	Objective	Description
Hormati et al. [2013]	Devising an application layer architecture for disaster response system (DRS)	Due to unique characteristics of MANETs, the applications and services should be distributed which in turn, form overlays; it was discovered that by improving interoperability, automation and prioritization, the efficiency of rescue operations is enhanced and, it allows machines to perform complex operations and to allocate resources to emergency services.
Jang et al. [2009]	Modeling rescue information system for earthquake disasters	After analyzing the causes for paralysis of the communication system provided by ChungHwa Telecom during Jiji earthquake, a system using WiFi-ready notebook PCs is proposed which is owned by rescue volunteers to construct a P2Pnet based on MANET, to provide support in such a situation.
Bernardo et al. [2008]	Prototyping an Internet telephony application for voice over a MANET-extended JXTA Virtual Overlay Network (MANET-VoVON)	This peer-to-peer open platform can be used to employ real-time applications on a MANET; it shows that using MANET-RVP deferred search, it is simple to have call setup triggered by connection availability; a decentralized approach would be helpful to track user′s location and delay the call setup till availability of a path; however, due to huge bandwidth overhead, its use should be restricted to extreme situations.
Singh et al. [2012]	Building MANETs with Windows Phone 7 (WP7) devices	Issues such as device discovery, power management, security, usability, as well as ethical and legal issues are addressed; the emphasis was on developing a stable and coherent service for file transfer; the project was expected to provide file integrity, efficient detection of all available MANETs and scalability of the network.

3. EXPLORING AODV

AODV routing protocol [Perkins et al. 2003] was jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das [Kumar et al. 2009]. It addresses some key issues related to performance of network [Shetty et al.]. It is designed for use in ad-hoc networks where it discovers and maintains routes whenever needed [Anderson et al.; Mhala et al. 2010]. It provides a dynamic and rapid connection to network. Moreover, it consumes less bandwidth and memory, and provides lower processing loads [Su et al. 2011] as it collects limited amount of routing information [Mtibaa et al. 2006]. AODV is designed with the assumption that all nodes in the network are trusted nodes [Nadeem et al. 2011].

AODV inherits the concept of sequence numbers from Destination Sequence Distance Vector (DSDV) protocol to indicate freshness of the route and to avoid loop formation [Jhaveri et al. 2010; Perkins et al. 2003]. It retains the feature of DSR protocol by flooding route requests on demand to discover path to the destination [Shetty et al.]. However, unlike DSR, AODV uses conventional routing tables having one entry for each destination. Furthermore, unlike DSR, AODV localizes the propagation of change in the network and thus, it greatly reduces the system wide broadcasts [Shetty et al.]. AODV uses three types of routing messages [Su et al. 2011]:

Route Request (RREQ), Route reply (RREP) and Route error (RERR). The structures of RREQ, RREP, RERR and routing table are shown in the Fig. 3 [Kumar et al. 2009].

A node increments or updates its own sequence number if it is originating RREQ or generating RREP. If RERR is initiated due to link breakage or valid non-repairable route, destination sequence number of that routing entry is incremented.

Type	Flags	Reserved	Hop count
RREQ (Broadcast) ID			
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

(a) Structure of RREQ

Type	A	Reserved	Hop count
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

(b) Structure of RREP

Type	N	Reserved	DestCount
Unreachable Destination IP Address			
Unreachable Destination Sequence Number			
Additional Unreachable Destination IP Addresses (if needed)			
Additional Unreachable Destination Sequence Numbers (if needed)			

(c) Structure of RERR

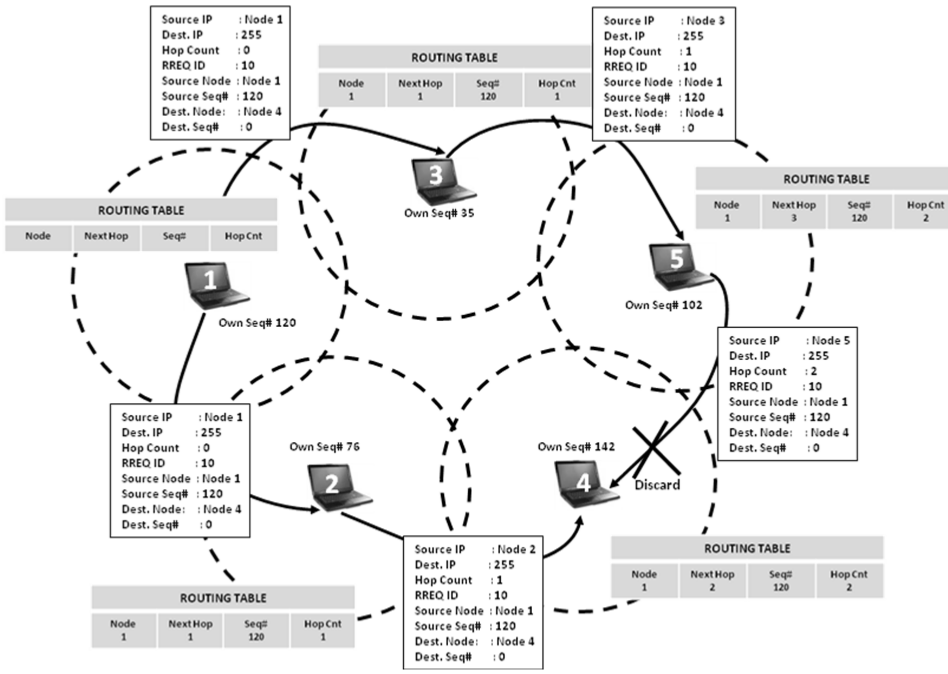
Destination IP address
Destination sequence number
Hop_count
Next hop
Precursor list
Expiration time

(d) Structure of routing Table

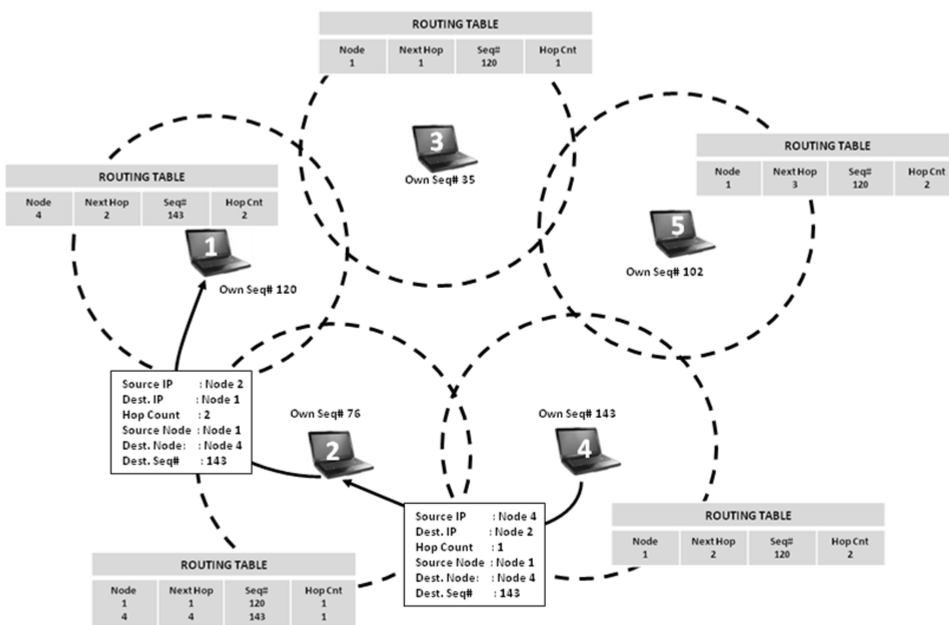
Figure. 3: Structures of AODV packets and routing table [Kumar et al. 2009].

3.1 Working Principles of AODV

3.1.1 *Route Discovery.* As shown in the Fig. 4 (a) [Dokurer et al. 2006], to establish connection to the destination, source node broadcasts a route request (RREQ) packet by flooding the network; each RREQ carries a Time-To-Live (TTL) value which indicates the maximum number of hops for which this message should be forwarded. When a node receives the broadcasted RREQ, it sets up a reverse path to the source for itself and rebroadcasts it in the network unless it is the destination or it has a fresher route to the destination in its routing table; this process is repeatedly carried out until RREQ is received by the destination node or an intermediate node having a valid route to the destination with higher destination sequence number or same destination sequence number with less hop counts. Such a node, then replies to the source by discarding the received RREQ and responding with a route reply (RREP) packet which is routed back to the original source on the reverse path [Jhaveri et al. 2012b; Shetty et al.] as shown in the Fig. 4 (b) [Dokurer et al. 2006]. Each node that participates in forwarding RREP towards the source creates a forward route to the destination. If a node receives another RREP, it updates routing information only if that RREP has higher sequence number or same sequence number with lower hop counts; otherwise, the RREP is discarded [Perkins et al. 2003]. The state of each node along the path from the source to the destination is hop-by-hop state which means that each node needs to remember only the next hop and not the entire route, as in the case of source routing [Elmoniem et al. 2011].



(a) RREQ propagation



(b) RREP propagation

Figure. 4: Route discovery process in AODV [Dokurer et al. 2006].

3.1.2 *Route Maintenane and Local Repair.* Due to frequent node movement, links can be broken which can be detected by checking local connectivity using special RREP messages, called HELLO message, with preset TTL value. During data transmission, if link breakage is detected for the next hop in the routing table, an RERR packet is sent to the source of the data in a hop-by-hop fashion for the unreachable destinations [Perkins et al. 2003]. Furthermore, if a route turns out to be inactive, an RERR packet is generated if that route is non-repairable with local repair mechanism. RERR is also sent if an RERR is received from a neighbor for one or more active routes. When the source node receives notification of a link breakage, it may reinitiate route discovery process, if it still requires route. If local repair is enabled in AODV, then on behalf of the source node, an intermediate node can initiate route discovery process for the destination [Effatparvar et al. 2010; Elmoniem et al. 2011]. Link failures can also be detected by link layer acknowledgements [Perkins et al. 2003].

A node also maintains a precursor list [Perkins et al. 2003] as a routing table entry for each valid route containing a finite hop count; precursors contain those neighboring nodes to which a route reply was generated or forwarded. Moreover, the list also contains precursors that may be forwarding packets on this route. In the event of link breakage, these precursors will receive notifications from the node. Also, if a route is unused for some specific time period, the node considers the route as invalid and removes the route from its routing table [Elmoniem et al. 2011].

3.1.3 *Data Transmission.* As soon as the first RREP is received by the source node, it can transmit data packets through the forward route in a hop-by-hop fashion. If the source node learns a better route, later on, it updates its routing information [Perkins et al. 2003]. Each node acts as a router to forward data packets to the next hop in the active route [Effatparvar et al. 2010; Elmoniem et al. 2011].

3.2 AODV Variants

3.2.1 *AOMDV.* AOMDV [Biradar et al. 2010; Marina et al. 2002; Marina et al. 2006] is a multipath extension of AODV routing protocol which computes multiple disjoint loop-free paths in a single route discovery process. It shares several characteristics with AODV except the number of paths found during the route discovery process.

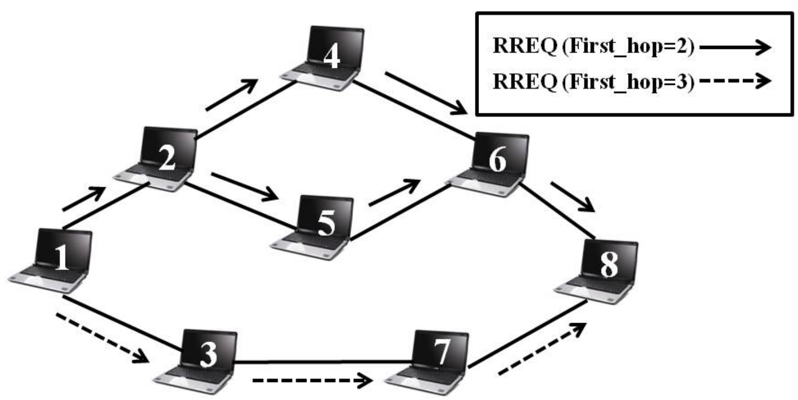
During the propagation of RREQ towards the destined node, multiple reverse paths are established both at the intermediate nodes and at the destined node. Moreover, multiple forward paths are built by multiple RREPs traversing from these reverse paths. AOMDV also discovers alternate paths for intermediate nodes. It attempts to reduce the occurrence of route discovery process. The routing table structure of AOMDV is shown in the Fig. 5 [Marina et al. 2002; Marina et al. 2006]. AOMDV is capable to discover node-disjoint or optionally link-disjoint routes [Hurni et al. 2008].

<table>
<tr><th colspan="4">Destination IP address</th></tr>
<tr><th colspan="4">Destination sequence number</th></tr>
<tr><th colspan="4">Advertised Hop_count</th></tr>
<tr><th colspan="4">Route List</th></tr>
<tr><td>$Next\_hop_1$
$Next\_hop_2$
.
.
.</td><td>$Last\_hop_1$
$Last\_hop_2$
.
.
.</td><td>Hop_count_1
Hop_count_2
.
.
.</td><td>$Expiration\ time_1$
$Expiration\ time_2$
.
.
.</td></tr>
</table>

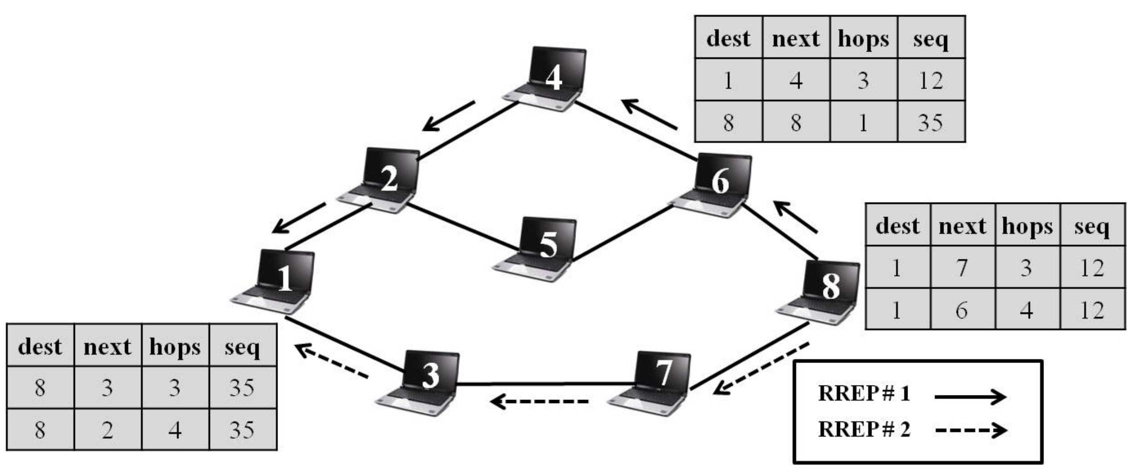
Figure. 5: Routing table structure of AOMDV [Marina et al. 2002; Marina et al. 2006].

Node-disjoint routes have no common intermediate nodes between them which make them suitable for dense environments [Almobaideen et al. 2009]. To discover node-disjoint routes, each node does not straight away reject duplicate RREQs. The strategy is modified in AOMDV by appending the first hop information (information about the node which first receives RREQ sent by the source) to the RREQ header. Furthermore, nodes never rebroadcast the duplicate RREQs which guarantee that any two RREQs arriving via different neighbors of the source have not traversed the same node. Thus, nodes receiving duplicate RREQs by different neighbors can determine whether paths are node-disjoint [Hurni et al. 2008].

Link-disjoint routes have no common links while they can have common nodes. Due to common nodes, more alternative paths are possible in this scheme which can be useful in sparse environments. The destination replies to duplicate RREQs from different neighbors. The route of each RREP takes a diverse reverse path to the source [Hurni et al. 2008; Trung et al. 2007]. Fig. 6 depicts the route discovery process of AOMDV when node 1 wants to communicate with node 8. Fig. 6 (a) shows that RREQ broadcasted by node 1 is received by its first hops node 2 and node 3; thus, RREQs flow from different paths to the destination. In AOMDV, node 8 sends multiple RREPs as shown in the Fig. 6 (b), which flow to source 1 via node 6 and node 7 and thus, node 1 discovers and stores two different paths to node 8.



(a) RREQ propagation



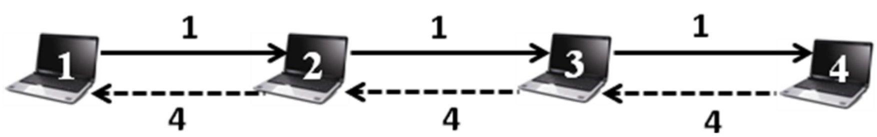
(b) RREP propagation

Figure. 6: Route discovery process in AOMDV [Hurni et al. 2008].

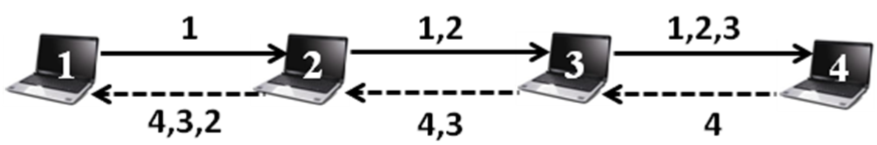
AOMDV allows intermediate nodes to reply to RREQs, and still selects disjoint paths. The protocol attempts to improve energy efficiency and packet delivery rate. On the other hand, due to increased flooding and multipath nature, it increases message overhead during route discovery.

3.2.2 *AODVv2.* AODVv2 [Dowdell et al. 2013] is the revised version of AODV protocol intended for stub of disconnected (with Internet) MANETs using memory constrained devices. It is popularly known as Dynamic MANET On-demand Routing (DYMO). It handles a wide variety of mobility as well as traffic patterns. It determines unicast routes on-demand and it is adaptable to topological changes [Martins et al. 2010]. It inherits the feature of Path Accumulation from DSR and simplifies AODV by removing needless RREP, precursor lists and HELLO messages [Sivakumar et al. 2009]. It achieves path accumulation by storing information about intermediate nodes along with the destination, for a newly discovered path [Sommer et al. 2008]. Though, AODVv2 is closely related to AODV and inherits some of the features of DSR, it is not interoperable to either of these two.

Fig. 7 represents comparison of route discovery processes of AODV and AODVv2 [Sommer et al. 2008]. In AODV, as RREQ flows from the source to the destination, it does not keep information about intermediate nodes as shown in the Fig. 7 (a); same thing applies when RREP flows from the destination to the source. In AODVv2, as shown in the Fig. 7 (b), both the control messages keep track of all intermediate nodes during their propagation and as a result, nodes receiving these control messages store the related information about all these nodes in their routing tables.



(a) RREQ and RREP operations in AODV



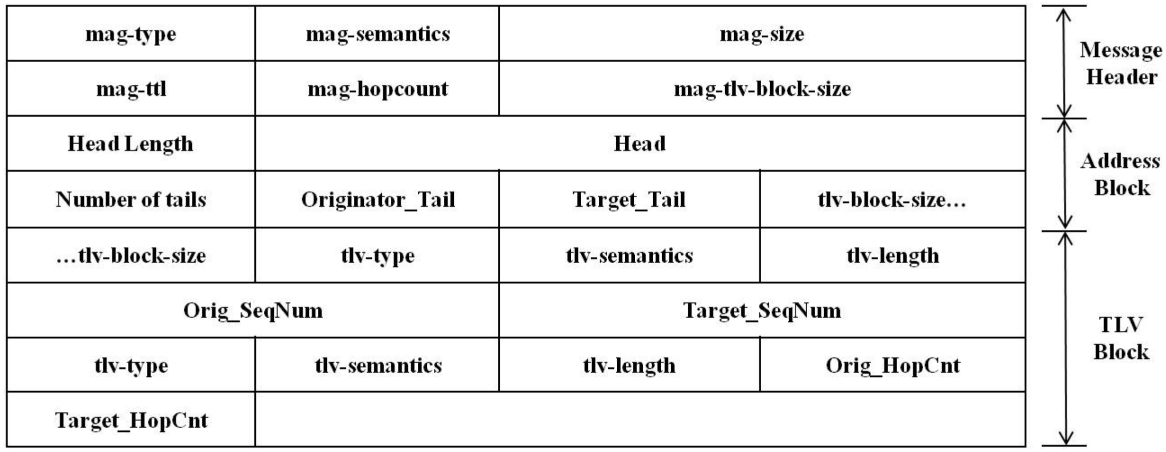
(b) RREQ and RREP operations in AODVv2

Figure. 7: Comparison of route discovery processes in AODV and AODVv2 [Sommer et al. 2008].

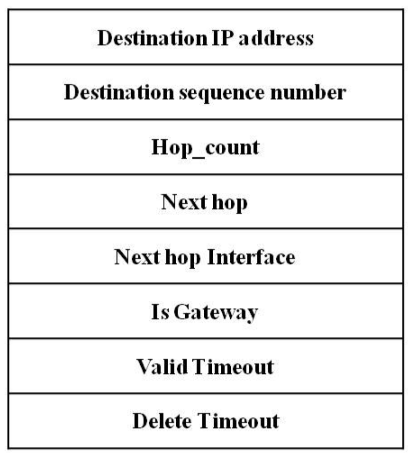
AODVv2 employs RFC 5444 message and type-length-value triplet (TLV) formats, unlike AODV [Dowdell et al. 2013]. An address block contains a set of addresses and following it, a TLV block contains the associated attributes [Thorup et al. 2007]. Structures of RREQ and routing table of AODVv2 are shown in the Fig. 8 (a) and in the Fig. 8 (b) [Thorup et al. 2007] respectively.

As AODVv2 works with source routing, nodes have to read the routing packets during route discovery process to acquire knowledge of the paths and may write in the packet about the hops needed to reach to its destination. This clearly increases the size of the routing packets with the intention of reducing the number of retransmissions [Martins et al. 2010]. Moreover, this revision of AODV still does not address many issues including the security issue.

3.2.3 *Summary of AODV and its variants.* A summary of AODV and its variants is presented along with their features in the Table II:



(a) Structure of RREQ



(b) Structure of routing table

Figure. 8: Structures of RREQ and routing table in AODVv2 [Thorup et al. 2007].

Table II: Summary of AODV and its variants.

Variant	**Developed By**	**Routing Type**	**Features**
AODV	C. Perkins, E. Royer, S. Das	Unipath	It has quick adaptation to dynamic link conditions, low network utilization, low processing and low memory overhead; it uses destination sequence numbers to ensure loop freedom and avoids problems such as "counting to infinity" associated with classical distance vector protocols.
AOMDV	M. Marina, S.Das	Multipath	It establishes multiple loop-free and link-disjoint paths to destination; it reduces end-to-end delay as compared to AODV.
AODVv2	E. Royer, I. Chakeres, D. Johnson, C. Perkins	Unipath	It can work as a pro-active or as a reactive routing protocol; it requires only the most basic route discovery and maintenance processes; it acquires the feature of path accumulation; it intends to reduce number of packet retransmissions.

3.3 AODV Implementations

AODV in itself is a proposal by the IETF (RFC 3561) and not an implementation [Brolin et al. 2008]. Testing a routing protocol in real world environment presents numerous challenges, and therefore, most of the research works to test performance of AODV in a variety of repeatable scenarios have been carried out with simulations [Mhala et al. 2010]. According to Lundgren et al. [2002], it is a good practice to evaluate protocols with mature and real world implementations. Table III provides a review on various implementations of AODV such as MAD-HOC, Kernel-AODV, AODV-UU, AODV-UCSB and AODV-UIUC.

Table III: Review on various implementations of AODV.

Type	Developed By	Description	Drawback
MAD-HOC [Chakeres et al. 2004; Gupta et al. 2010]	Fredrik Lilieblad, Oskar Mattsson, Petra Nylund, Dan Ouchterlony, Anders Roxenhag	It resides in the user-space and uses snooping to determine the AODV events; the method of snooping ARP and data packets is performed; it runs on a Linux 2.2 kernel, but does not support multicast.	While using ARP, it is found to perform poorly due to bugs; it is not interoperable properly with the later implementations.
Kernel-AODV [Glabbeek et al. 2013; Gupta et al. 2010]	NIST, Department of Commerce′s Technology Administration U.S. and Wireless Communications Technologies Group	It runs on the Linux platform with 2.4 kernel and uses Netfilter; as no packets are required to traverse from the kernel to the user-space, it is fastest and efficient in terms of packet handling, amongst all the implementations; it also supports multiple interfaces, multi-hop Internet gateway and a basic multicast protocol.	It contains bugs such as mishandling malloc failures, memory leaks and generating invalid packets.
AODV-UU [AODV-UU, AODV; Brolin et al. 2008; Gupta et al. 2010; Lee et al. 2003]	Erik Nordstrm at Uppsala University	It was implemented as a user space daemon with loadable kernel modules; it runs on the Linux platform with 2.4 kernel which has two kernel components: kaodv and ip_queue_aodv; it supports multicasting with a patch implemented; Netfilter library is used in the user space to capture incoming and outgoing packets; AODV-UU includes Internet gateway support as well as multiple interface support; it is very stable and well tested.	All the packets must pass the boundary between the kernel and the user space twice.

Continued on next page

Table III – continued from previous page

Type	Developed By	Description	Drawback
AODV-UCSB [Borgia et al. 2005; Chakeres et al. 2004; Glabbeek et al. 2013; Gupta et al. 2010]	University of California, Santa Barbara	It is the newest daemon developed on Linux 2.4 kernel; it is implemented as a user space daemon similar to the UU implementation; the implementation directly uses the UU input user space packet queuing module and the kaodv/packet_queue_aodv kernel modules.	The processing of RERR messages does not follow the RFC specification; the throughput achieved is lower and the latency associated is greater than AODV-UU.
AODV-UIUC [Glabbeek et al. 2013; Kawadia et al. 2003]	University of Illinois, Urbana-Champaign	It uses Netfilter and is based on the Ad hoc Support Library (ASL); this Linux specific library eliminates the complexity of the user space ad-hoc routing module as it allows development of other ad-hoc routing protocols; even though its design is similar to AODV-UU and AODV-UCSB, it separates the routing and forwarding functions; it handles packet forwarding in the kernel and routing protocol logic in the user-space; this provides immediate handling of forwarded packets and facilitates traversal of fewer packets from the kernel to the user-space boundary.	The processing of RERR packets does not follow the RFC specification.

3.4 Issues in AODV Design

Even though AODV is a prominent routing protocol, its basic design induces various issues which may lead to degradation in the network performance with respect to packet delivery rate, throughput, routing overhead and delay.

AODV does not have a mechanism that considers residual node energy or balances the load amongst the nodes [Feng et al. 2013; Sarkar et al. 2014]. Inefficient local repair, congestion, flooding effects and route errors cause degradation in various metrics which in turn, reduce network life time [Devi et al. 2013; Jhaveri et al. 2015; Liu et al. 2013; Nand et al. 2011; Shastri et al. 2013]. A variety of attacks can be launched during route discovery phase, route maintenance phase or data transmission phase [Joshi et al. 2011; Yi et al. 2005] just by not following the protocol rules of AODV [Dhurandher et al. 2013]; Blackhole and Grayhole attacks are two of the most talked about attacks on AODV-based MANETs in recent years [Ding et al. 2014; Jhaveri et al. 2013]. In the following section, we present review of the recent research works carried out by various researchers that address some of these issues.

4. RECENT RESEARCH ON AODV

Several research works have been carried out in recent times to enhance design of AODV protocol as presented in Table IV.

Table IV: Review of recent research on AODV.

Authors	Description	Metrics
Feng et al. [2013]	Based on energy and load, Advanced-AODV performs route establishment; a node may choose optimal route by delaying received RREQ; the protocol balances the routing load.	Packet delivery rate, end-to-end delay
Hui et al. [2013]	J-AODV is devised for engineering applications; based on energy level and number of neighbors of a node, a willing parameter is calculated; the node with higher energy level and less number of neighbors is given larger willing value; as a result, the next node updates that node as the reverse route node during RREQ propagation.	Throughput, end-to-end delay
Sridhar et al. [2013]	EN-AODV selects route by calculating energy levels of nodes based on their sending/receiving rates and sizes of the transmitted data; the protocol transfers data reliably and improves QoS.	Packet delivery rate, end-to-end delay
Barma et al. [2013]	This adaptive routing algorithm selects best path using residual node energy, hop count and aggregate interface queue length of nodes; the mechanism allows only the destination node to respond to the RREQ which significantly reduces the number of control packets transmitted.	Packet delivery rate, routing overhead, throughput
Alrayes et al. [2013]	The protocol supports multi-radio interfaces and selects best interface for sending packets on the basis of traffic direction and router type; it aims to select best path having less probability of buffer overflow at queue interfaces.	Packet delivery rate, routing overhead, throughput, end-to-end delay
Liu et al. [2013]	B-AODV aims to improve route discovery and local repair of AODV; information about pre-hop node and next two-hop node is recorded using RREQ and B-RREQ for rapidly rebuilding routes.	Routing overhead, end-to-end delay
Shastri et al. [2013]	The scheme attempts to reduce regenerations of control packets and to heal route quickly and intelligently in case of link breakage; it records all the active routes to the destination which helps to update routing table and to discover the optimal path during link failures.	Packet delivery rate, throughput
Devi et al. [2013]	The protocol improves route error tolerant mechanism of AODV; an RERR is sent to the pre-hop node in the route and not to the source node so that it can handle route failures along with the source node; moreover, the solution can also detect a malicious node while constructing the path.	Packet loss, throughput

Continued on next page

Table IV – continued from previous page

Authors	Description	Metrics
Cuong et al. [2013]	MAR-AODV aims at improving network flows and reducing the probability of packet congestion; mobile agents are incorporated into nodes to update traffic density at each node; the algorithm chooses a route which reduces overall traffic density of the network.	Probability of packet blocking
Dandotiya et al. [2013]	This intelligent AODV conducts route selection in two phases; in the first phase, an RREQ is accepted only if its signal strength between nodes is greater than the threshold; if no routes are discovered, it switches to second phase and works like the normal AODV; the method selects a strong route to the destination to increase network life span.	Packet delivery rate, throughput, routing overhead
Nand et al. [2011]	This probability based broadcasting technique diminishes the effects of flooding problems in AODV; it controls rebroadcasts of packets by calculating rebroadcast probability based upon the nodes′ residual energy and threshold random delay; it uses limited channel bandwidth to efficiently discover route and to improve lifetime of the network.	Broadcast packets sent, end-to-End delay
Choi et al. [2013]	GAODV protocol designed for maritime multihop ad-hoc networks aims at improving throughput of the networks having limited bandwidth capacity; it uses the position information to selectively broadcast RREQ; as the ship density increases, the routing overhead-traffic of the protocol is reduced.	Routing overhead
Jhaveri et al. [2015]	To detect suspicious nodes, SNBDS heuristically calculates a threshold value using time information, sequence number of RREP and that of the routing table; suspicious nodes are marked as malicious nodes if they reply to the bait request sent by monitoring nodes; performance of the protocol is evaluated against three distinct adversary models.	Packet delivery rate, routing overhead
Nadeem et al. [2014]	IDAR mechanism uses routing information, packet delivery ratio, dropped control packets and throughput to measure level of confidence in attack detection, severity of attack and degradation of network performance; this flexible response system prevents malicious nodes from performing further attacks; the system is tested with various types of attacks.	Attack detection rate, response action rate, performance degradation rate, overhead

Continued on next page

Table IV – continued from previous page

Authors	Description	Metrics
Tan et al. [2013]	In SRD-AODV, the source node analyzes the sequence numbers in multiple RREPs received from the intermediate nodes or from the destination node; it calculates a threshold based on that and discards RREPs having greater sequence number than the threshold; furthermore, the destination also cross checks the sequence number of the received RREQ prior to generating an RREP.	Packet delivery rate
Jhaveri et al. [2012b]; Jhaveri et al. [2013]	R-AODV dynamically calculates a threshold value using number of sent out RREQs, number of received RREPs and routing table sequence number to identify a malicious node; the scheme uses modified RREQ to propagate information about malicious nodes to other nodes in the network.	Packet delivery rate, routing overhead, end-to-end delay
Manoranjini et al. [2013]	This trust-based approach chooses a cluster head having higher trustee value; this node acts as a representative of the group; the cluster data are collected and behavioral analysis is performed; this approach with hybrid condition based automatic detector and Kalman Bucy filters detects the malicious nodes more speedily and accurately regardless of mobility of the nodes.	Attack detection consistency
Bar et al. [2013]	This trust-based scheme ranks a node according to the trust value which is calculated using the number of forwarded packets by the node; a route is established by avoiding untrusted nodes and selecting trusted ones; the scheme aims to transmit data reliably through the trusted nodes and attempts to improve QoS.	Packet loss, percentage of untrusted nodes
Wang et al. [2014]	TQR is designed with a distributed heuristic algorithm; it estimates trust using direct observations and neighbors′ recommendations using packet forwarding behavior; a QoS parameter called link delay is combined with the calculated route trust; after receiving multiple RREQ packets, the destination node decides an optimal route through which the RREP is to be sent to the source node.	Packet delivery rate, routing overhead, end-to-end delay, attack detection rate
Yitayal et al. [2014]	BBU-AODV uses residual energy and hop count to improve network life time; a route is selected based upon the maximum difference of average sum of residual energy and a pre-defined threshold; however, when the nodes in possible routes have low remaining energy, the route is selected on the basis of maximum difference of the average minimum residual energy and threshold.	Packet delivery rate, routing overhead, end-to-end delay, network lifetime, energy

Continued on next page

Table IV – continued from previous page

Authors	Description	Metrics
Mohapatra et al. [2015]	SEAR-AODV computes route reliability factor using nodes′ energy and route stability; it selects the route with highest reliability factor for data transmission; if the principal route fails, alternative routes are selected according to their reliability factor values; it uses make-before break route maintenance mechanism; it attempts to reduce control overhead.	Packet delivery rate, routing overhead, end-to-end delay, energy, hop count

Fig. 9 summarizes the reviewed papers according to the percentage frequency of each parameter considered to modify the AODV protocol.

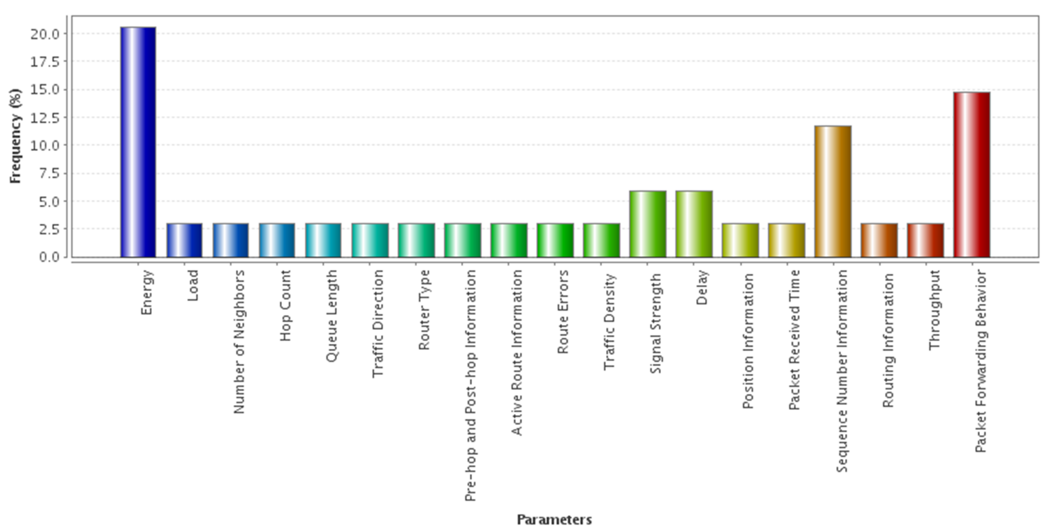


Figure. 9: Percentage frequency of each parameter in the reviewed papers.

Fig. 10 summarizes the reviewed papers according to the percentage frequency of each metric used to evaluate the performance of the modified AODV protocol.

5. RESEARCH SCOPE

In the last decade, significant research work has been carried out on AODV, focusing on various design criteria; however, each of the proposals has its own assumptions and limitations. On the whole, there is still immense scope for improvement in the design of AODV and its variants:

—There have been several proposals addressing security issues of AODV against various active attacks, but each works under specific conditions such as with certain network density, traffic load, node mobility, number of attackers, or number of powerful backbone nodes. Moreover, very few of them effectively address exploitation of AODV against selfish nodes. Thus, a defense mechanism for AODV that works equally well in all scenarios is still to be addressed.

—Various authentication and key distribution mechanisms have been proposed, but very few of them consider resource constraints. Moreover, they work under certain assumptions. Hence, developing a well-rounded and efficient mechanism to incorporate authentication by secure distribution of keys across the network still remains an open challenge.

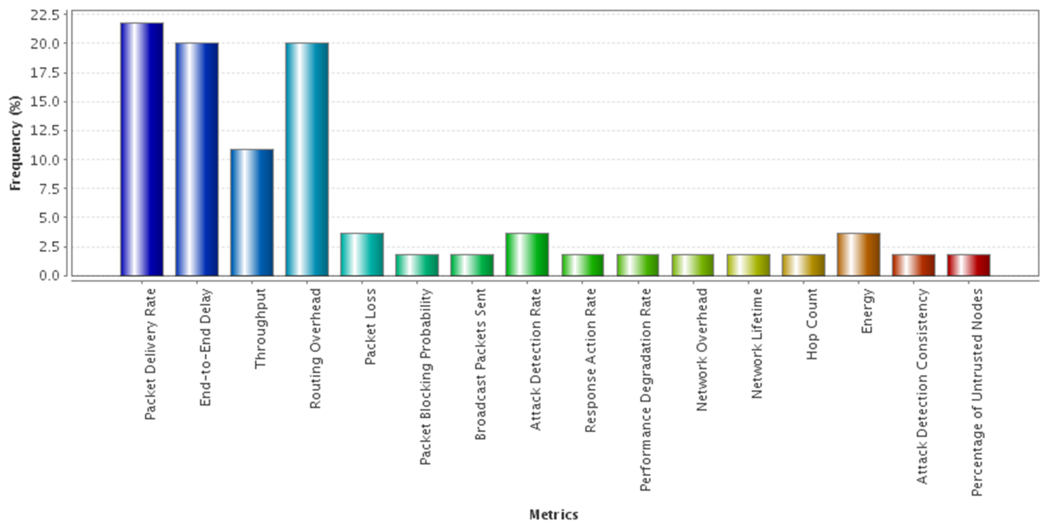


Figure. 10: Percentage frequency of each metric in the reviewed papers.

—Research works have been carried out on energy conservation of mobile nodes in AODV-based MANETs, but some mechanisms use up high computation power of the node in calculating various parameters. Some mechanisms require additional control packets from neighbors to verify their willingness for data transfer, which in turn, increases routing overhead. Therefore, the issue of designing a solution that takes lesser computation power and minimal increase in control packets is still unaddressed.

—Few algorithms focus on adaptive and intelligent techniques that work efficiently only for specific type of applications, but the same may prove to be inefficient for other applications. Therefore, building up an algorithm which works well in most types of applications still remains an open challenge.

—A number of schemes have been proposed to optimize packet delivery ratio, throughput, normalized routing overhead or average end-to-end delay in the network, but optimization of one metric may lead to imbalance of one or more other metrics. As a result, it becomes imperative to optimize AODV such that the network performance gets improved by balancing the key performance metrics.

—It is to be remembered that security is a continuous and endless process. It is an open challenge for researchers to aim at making AODV more and more robust by investigating and improving current countermeasures.

—AODVv2 and AOMDV attempt to eliminate some of the limitations of AODV under high traffic load and high mobility scenarios. However, performance of AODVv2 gets degraded during low node mobility and random traffic flow [Gupta et al. 2013]. On the other side, AOMDV considers hop count during route establishment and ignores path stability [Aalam et al. 2012]. Moreover, both the AODV variants ignore security aspect. Therefore, there is still an ample scope to carry out further research on these AODV variants.

6. CONCLUSION

MANETs are becoming an integral part for several critical applications and with that many issues emerged that require different solutions. In this paper, we introduce MANET technology and provide its classification. From the study on MANET application research we can state that the applications are constrained by limited resources that affect the performance and life span of the networks and, still there are challenges left in employing MANETs for important applications. The papers studied and reviewed, year-wise and publisher-wise, are shown in Fig. 11.

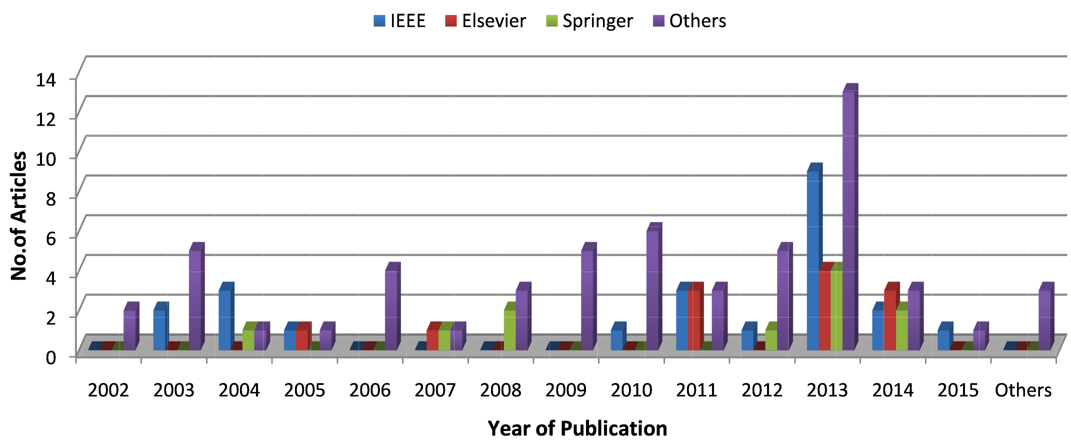


Figure. 11: Year-wise and publisher-wise frequency of the articles cited in the paper.

We categorize routing protocols according to their designs and operations and, briefly discuss the working of each type of protocols. We thoroughly study the working principles of AODV routing protocol which is one of the widely used routing protocols. We provide a brief study of AOMDV and AODVv2 which are the variants of AODV. We found that the multipath variant AOMDV attempts to improve energy efficiency and packet delivery rate at the cost of increase in message overhead. Another variant, AODVv2 with source routing, intends to reduce number of retransmissions for a variety of mobility and traffic patterns at the cost of increase in routing packet size. Both the variants leave several issues unaddressed, like AODV. We also examine real world implementations of AODV such as MAD-HOC, KERNEL-AODV NIST, AODV-UU, AODV-UCSB and AODV-UIUC, and observe that AODV-UU is one of the most popular implementations.

We survey recent research works carried out on AODV by investigating several mechanisms attempting to solve different issues. We draw the conclusion that still there is a huge room for further research on AODV and its variants to enhance their performance by incorporating efficient energy conservation schemes, authentication and key distribution mechanisms, security solutions, improved route discovery techniques and performance optimization techniques. Hence, extensive research ought to be carried out to devise a routing mechanism which provides smooth, secure and efficient transmission between the mobile nodes for a variety of applications considering resource constraint environment and different traffic scenarios. This paper throws light on various aspects of mobile ad-hoc networking with AODV that can be helpful for researchers wishing to explore this area.

ACKNOWLEDGMENTS

The authors of this paper would like to thank the management of Charotar University of Science & Technology, Changa, India and the management of SVM Institute of Technology, Bharuch, India for providing the necessary resources to complete this survey. Special thanks go to Prof. (Dr.) D.C. Jinwala of SVNIT, Surat, India, Prof. (Dr.) Robert van Glabbeek of NICTA, Australia and Charles Perkins of Nokia Research, USA for their able guidance and motivation. The authors are grateful to the anonymous reviewers and the journal editors.

REFERENCES

Aalam, S.S., and Victorie, T.A.A. 2012. Path Optimization using Gamma Distribution in MANETs. Journal of Applied Sciences 12, 7 (2012), 627-635.

Al-karaki, J.N., and Kamal, A.E. 2004. Routing techniques in wireless sensor networks: a survey. Wireless Communications, IEEE 11, 6 (Dec. 2004), 6-28.

Almobaideen, W. 2009. SPDA: stability based partially disjoint AOMDV. European Journal of Scientific Research 27, 3 (2009), 342-348.

Alrayes, M., Biswash, S., Tyagi, N., Tripathi, R., Misra, A., and Jain, S. 2013. : An Enhancement of AODV with Multi-Radio in Hybrid Wireless Mesh Network. ISRN Electronics(2013). Hindawi Publishing Corporation, (2013), 1-13.

ANDERSSON, E., AND LJUNGDAHL, E. Porting AODV-UU into NS-Miracle. *http : //www.cs.kau.se/cs/prtp/pmwiki/uploads/MeshWikipage/aodvuu2nsmiracle.pdf* Accessed on Oct. 16, 2015.

AODV-UU, A. O. D. V. Linux Implementation, University of Uppsala.

Bar, R.K., Mandal, J.K., and Singh, M.M. 2013. QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack. Procedia Technology 10 , (2013), 530-537.

Barma, M., Chowdhuri, R., Debbarma, N., Sen, S., and Roy, S. 2013. : Enhancing the Performance of AODV Using Node Remaining Energy and Aggregate Interface Queue Length. In *Proceedings of the IEEE International Symposium on Computational and Business Intelligence (ISCBI), (2013). 77-80.*

Basagni, S., Conti,M., Silvia Giordano, S., and Stojmenovic, I. 2004. Mobile ad hoc networking. John Wiley & Sons (2004).

Bernardo, L., Oliveira, R., Gaspar,S., Paulino,D., and Pinto, P. 2008. A Telephony Application for Manets: Voice over a MANET-Extended JXTA Virtual Overlay Network. E-Business and Telecommunication Networks. Springer Berlin Heidelberg, (2008), 347-358.

Biradar, S.R., Majumder, K., Sarkar, S.K., and Puttamadappa, C. 2010. Performance evaluation and comparison of AODV and AOMDV. (IJCSE) Int. J. Comput. Sci. Eng 2, 2 (2010), 373-377.

Borgia, E. 2005. : Experimental evaluation of ad hoc routing protocols. In *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications Workshops, (2005). PERCOM. 2005 Workshops, 232-236.*

BROLIN, J., AND HEDEGREN, M. 2008. Packet Aggregation in Linux. PhD diss., Karlstads universitet, Karlstad. 2008.

Budke, D., Farkas, K., Plattner, B., Wellnitz, O., and Wolf, L. 2006. : Real-time multiplayer game support using QoS mechanisms in mobile ad hoc networks. In *Proceedings of the 3rd Annual Conference on Wireless On-demand Network Systems and Services: WONS, (2006). 32-40.*

Chakeres, I., and Belding-royer, E. 2004. : AODV routing protocol implementation design. In *Proceedings of the 24th IEEE International Conference on Distributed Computing Systems Workshops, (2004). 698-703.*

Chibelushi, C., Eardley, A., and Arabo, A. 2013. Identity Management in the Internet of Things: the Role of MANETs for Healthcare Applications. Computer Science and Information Technology 1, 2 (2013), 73-81.

Choi, Y. and Lim, Y. 2013. : Geographical AODV protocol for multi-hop maritime communications. In *Proceedings of the OCEANS-Bergen, MTS/IEEE, (2013). 1-3.*

Conti, M., and Giordano, S. 2014. : Mobile ad hoc networking: milestones, challenges, and new research directions. In *Proceedings of the Communications Magazine, IEEE 52, 1 (2014). 85-96.*

Cuong, C., Tu, V., and Hai, N. 2013. : MAR-AODV: Innovative Routing Algorithm in MANET Based on Mobile Agent. In *Proceedings of the 27th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), (2013). 62-66.*

Dandotiya, H., Jain, R., and Bhatia, R. 2013. : Route Selection in MANETs by Intelligent AODV. In *Proceedings of the International Conference on Communication Systems and Network Technologies (CSNT), (2013). 332-335.*

Devi, S.S., and Sikamani, K.T. 2013. : Improved route error tolerant mechanism for AODV routing protocol in MANET. In *Proceedings of the IEEE International Conference on Current Trends in Engineering and Technology (ICCTET), (2013). 187-190.*

Dhurandher, S., Woungang, I., Mathur, R., and Khurana, P. 2013. : GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs. In *Proceedings of the 27th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA), (2013). 357-362.*

Ding, Y., Qu, H. and Wang X. 2014. NS2-Based Black Hole Attack Modeling and Simulation of Ad Hoc Network. In Advanced Materials Research 846 (2014), 1697-1700.

Dokurer, S., 2006. Simulation of Black hole attack in wireless Ad-hoc networks. Master′s Thesis, Atlm University. 2006.

Ratliff, S., Dowdell, J., and Perkins, C. 2013. Dynamic MANET On-demand (AODVv2) Routing. Internet Draft. (2013), 1-60.

Effatparvar, M., Effatparvar, M., Darehshoorzadeh, A., Zarei, M., and Yazdani, N. 2010. : Load balancing and route stability in mobile ad hoc networks base on AODV protocol. In *Proceedings of the IEEE Intl Conf on Electronic Devices, Systems and Applications (ICEDSA), (2010). 258-263.*

Elmoniem, A.M., Ibrahim, H.M., Mohamed, M.H., and Hedar, A.R. 2011. Ant Colony and Load Balancing Optimizations for AODV Routing Protocol. Research article international journal of sensor networks and data communication 1, (2011), 1-14.

Fehnker, A., Van Glabbeek, R., Hfner, P., Mciver, A., Portmann, M., and Tan, W. 2012. Automated analysis of AODV using UPPAAL. In Tools and Algorithms for the Construction and Analysis of Systems, Springer Berlin Heidelberg, (2012), 173-187.

Feng, Z., Wang, L., and Gao, X. 2013. : An improved routing protocol Ad-AODV Based on AODV. In *Proceedings of the International Conference on Information Science and Computer Applications (ISCA 2013), Atlantis Press, (2013).*

Van Glabbeek, R., Hfner, P., Tan,W., and Portmann, M. 2013. : Sequence numbers do not guarantee loop freedom: AODV can yield routing loops. In *Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems (MSWiM '13), ACM, (2013). New York, NY, USA, 91-100.*

Goyal, P., Parmar, V., and Rishi, R. 2011. Manet: vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management 11 , 32-37.

Gupta, A.K., Sadawarti, H., and Verma, A.K. 2013. Implementation of DYMO routing protocol. International Journal of Information Technology, Modeling and Computing (IJITMC) 1, 2 (2013), 49-57.

Gupta, M.P., and Tuteja, R.K. 2010. Design Strategies for AODV Implementation in Linux. (IJACSA) International Journal of Advanced Computer Science and Applications 1, 6 (2010), 102-107.

Gwalani, S., Belding-royer, E., and Perkins, C. 2003. : AODV-PA: AODV with path accumulation. In *Proceedings of the IEEE International Conference on Communications, ICC'03., 1 (2003). 527-531.*

Helen, D., and Arivazhagan, D. 2014. Applications, Advantages and Challenges of Ad Hoc Networks. Journal of Academia and Industrial Research (JAIR) 2, 8 (2014), 453-457.

Hoebeke, J., Moerman, I., Dhoedt, B., and Demeester, P. 2004. An overview of mobile ad hoc networks: Applications and challenges. Journal-Communications Network 3, 3 (2004), 60-66.

Hormati, M., 2013. Application Layer Architectures for Disaster Response Systems. PhD diss., Concordia University. 2013.

Hui, L., Xiaoyun, T., Haifeng, Z., and Wei, W. 2013. : Improved AODV for engineering applications in Wireless Ad Hoc Network. In *Proceedings of the International Conference on Information, Business and Education Technology (ICIBIT 2013) (2013). 1322-1325.*

Hurni, P., and Braun, T. 2008. Energy-efficient multi-path routing in wireless sensor networks. In Ad-hoc, Mobile and Wireless Networks, Springer Berlin Heidelberg, (2008), 72-85.

Islam, N., and Shaikh, Z. 2013. Security Issues in Mobile Ad Hoc Network. In Wireless Networks and Security, Springer Berlin Heidelberg, (2013), 49-80.

Jang, H., Lien, Y., and Tsai, T. 2009. : Rescue information system for earthquake disasters based on MANET emergency communication platform. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, ACM, (2009). 623-627.*

Jhaveri, R.H. 2013. Reliable approach to prevent blackhole and grayholes attacks in mobile ad hoc networks. In Dynamic Ad Hoc Networks, IET Editorial Book, H.F. Rashvand and H.-C. Chao, Eds. Stevenage, (2013), pp. 261-280.

Jhaveri, R.H., and Patel, N.M. 2015. A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. Wireless Networks (Feb. 2015), 1-18.

Jhaveri, R.H., Patel, A.D., Parmar, J.D., and Shah, B.I. 2010. MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security 10, 4 (2010), 12-18.

Jhaveri, R., Patel, S., and Jinwala, D. 2012. : Dos attacks in mobile ad hoc networks: A survey. In *Proceedings of the 2nd IEEE International Conference on Advanced Computing & Communication Technologies (ACCT) (2012). 535-541.*

Jhaveri, R.H., Patel, S.J.,, and Jinwala, D.C 2012. Improving route discovery for aodv to prevent blackhole and grayhole attacks in manets. INFOCOMP Journal of Computer Science 11, 1 (2012), 1-12.

Joshi, P. 2011. Security issues in routing protocols in MANETs at network layer. Procedia Computer Science 3, (2011), 954-960.

Kawadia, V., Zhang, Y., and Gupta, B. 2003. : System Services for Implementing Ad-Hoc Routing: Architecture, Implementation and Experiences. In *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys), ACM, (June,2003). San Francisco, CA, 99-112.*

Kingsbury, R., 2009. Mobile Ad hoc networks for oceanic aircraft communications. PhD diss., Massachusetts Institute of Technology. 2009.

KUMAR, D., AND SRIVASTAVA, A. 2013. A Study Of Disaster Management System With View Of MANET Application. IEEE Trans. on Journal of Advances in Physics. 3, 3 (2013), 249-256.

KUMAR, V., 2009. Simulation and Comparison of AODV and DSR routing protocols in MANETs. PhD diss., Thapar University Patiala. 2009.

LEE, M., 2003. Implementing AODV Ad Hoc Routing Protocol for IPv6. PhD diss, Simon Fraser University. 2003.

LI, G., AND CHEN, J. 2011. The research of routing algorithms based on NS2 in mobile ad hoc networks. In *Proceedings of the 2nd IEEE International Conference on Software Engineering and Service Science (ICSESS) (2011). 826-829.*

LIU, S., YANG, Y., AND WANG, W. 2013. Research of AODV Routing Protocol for Ad Hoc Networks1. In *Proceedings of the AASRI Conference on Parallel and Distributed Computing and Systems 5, (2013). 21-31.*

LUNDGREN, H. 2002. Implementation and real-world evaluation of routing protocols for wireless ad hoc networks. IT Licentiate theses. Uppsala University. 2002. 1-74.

MAMATHA, G.S., AND SHARMA, D.S.C. 2010. Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues. International Journal of Computer Science & Engineering Survey (IJICSES). 1, 1 (2010), 14-21.

MANORANJINI, J., CHANDRASEKAR, A., AND RAJINIGIRINATH, D. 2013. Hybrid Detector for Detection of Black Holes in Manets. IERI Procedia. 4, (2013), 376-382.

MARINA, M.K., AND DAS, S.R. 2002. Ad hoc on-demand multipath distance vector routing. ACM SIGMOBILE Mobile Computing and Communications 6, 3 (2002), 92-93.

MARINA, M.K., AND DAS, S.R. 2006. Ad hoc on-demand multipath distance vector routing. Wireless Communications and Mobile Computing 6, 7 (2006) 969-988.

MARTINS, J., CORREIA, S., AND CELESTINO, J. 2010. Ant-DYMO: A bio-inspired algorithm for MANETS. In *Proceedings of the 17th IEEE international Conference on Telecommunications (ICT) (2010). 748-754.*

MHALA, N.N., AND CHOUDHARI, N.K. 2010. An Implementation Possibilities For AODV Routing Protocol In Real World. International Journal of Distributed and Parallel Systems. 1, 2 (2010), 118-127.

MISHRA, A., JAISWAL, R., AND SHARMA, S. 2013. A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network. In *Proceedings of the 3rd IEEE International Conference on Advance Computing Conference (IACC) (2013). 499-504.*

MOHAMMAD, S., ALSANBANI, M., AND ALAHDAL, T. 2014. Comparison Study of Routing Protocols in MANET. International Journal of Ad Hoc, Vehicular and Sensor Networks. 1, 1 (2014), 1-9.

MOHAMMED, Q., AND KHAN, M. 2012. Distributed Database Systems MANETS. In *Proceedings of the International Conference on Computing and Information Technology (ICCIT).*

MOHAPATRA, S., SWIN, B., MAHAPATRA, S., AND BEHERA, S. 2015. : Stability and energy aware reverse AODV routing protocol in MANETS. In *Proceedings of the 2nd IEEE International Conference on Recent Trends in Information Systems (ReTIS) (2015). 526-531.*

MTIBAA, A., AND KAMOUN, F. 2006. MMDV: Multipath and MPR based AODV routing protocol. In *Proceedings of the IFIP 5th Annual Mediterranean Ad Hoc Networking Workshop (2006). 137-144.*

MUELLER, S., TSANG, R., AND GHOSAL, D. 2004. Multipath routing in mobile ad hoc networks: Issues and challenges. In Performance Tools and Applications to Networked Systems, Springer Berlin Heidelberg, (2004), 209-234.

NADEEM, A., AND HOWARTH, M. 2013. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommunication Systems 52, 4 (2013), 2047-2058.

NADEEM, A., AND HOWARTH, M. 2014. An intrusion detection & adaptive response mechanism for MANETs. Ad Hoc Networks 13, (2014), 368-380.

NAND, P., AND SHARMA, S. 2011. Probability based improved broadcasting for AODV routing protocol. In *Proceedings of the IEEE International Conference on Computational Intelligence and Communication Networks (CICN) (2011). 621-625.*

NING, P., AND SUN, K. 2005. How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. Ad Hoc Networks 3, 6 (2005), 795-819.

PERKINS, C., BELDING-ROYER, E., AND DAS, S. 2003. RFC 3561-ad hoc on-demand distance vector (AODV) routing. Internet RFCs. (2003), 1-38.

PHAM, P., AND PERREAU, S. 2003. : Performance analysis of reactive shortest path and multipath routing mechanism with load balance. In *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, INFOCOM 2003 1, (2003).251-259.*

PRATHAPANI, A., SANTHANAM, L., AND AGRAWAL, D. 2013. Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents. The Journal of Supercomputing 64, 3 (2013), 777-804.

QUISPE, L.E., AND GALAN, L.M. 2014. Behavior of Ad Hoc routing protocols, analyzed for emergency and rescue scenarios, on a real urban area. Expert Systems with Applications 41, 5 (2014), 2565-2573.

RAJABHUSHANAM, C., AND KATHIRVEL, A. 2011. Survey of wireless MANET application in battlefield operations. International Journal of Advanced Computer Science and Applications (IJACSA) 2, 1 (2011).

Raut, S.H., and Ambulgekar, H.P. 2013. Proactive and Reactive Routing Protocols in Multihop Mobile Ad hoc Network. International Journal of Advanced Research in Computer Science and Software Engineering 3, 4 (2013), 152-157.

Sarkar, S., and Datta, R. 2014. A secure and energy-efficient stochastic routing protocol for wireless mobile ad-hoc networks. In *Proceedings of the20th IEEE National Conference on Communications (NCC) (2014). 1-6.*

Shastri, A., and Shrivastava, G. 2013. : Implementation and Performance Comparison of Improved Route Maintenance Strategy in AODV for Quick Route Healing. In *Proceedings of the International Conference on Communication Systems and Network Technologies (CSTN). IEEE Computer Society (2013). 299-302.*

Shetty, D.. RO-AODV: Route Optimized Ad-hoc On-demand Distance Vector Routing Protocol.

Shi, F., Liu, W., Jin, D., and Song, J. 2014. A cluster-based countermeasure against blackhole attacks in MANETs. Telecommunication Systems 57, 2 (2014), 119-136.

Simaremare, H., Abouaissa, A., Sari, R. F., and Lorenz, P. 2014. Security and performance enhancement of AODV routing protocol. International Journal of Communication Systems (2014).

SINGH, S., DAVIES, B., AND LIN, T. 2012. MANET application for Windows Phone. *http://pubs.cs.uct.ac.za/honsproj/cgi-bin/view/2012/davies_lin_singh.zip/groutWebsite/group/Project%20Proposal.pdf* Accessed on Oct. 16, 2015.

Sivakumar, N., and Jaiswal, S. 2009. Comparison of DYMO protocol with respect to various quantitative performance metrics. In *Proceedings of the IRCSE, 2009.*

Sivalingam, K. 2003. Readings in Tutorial on Mobile Ad Hoc Networks.

Sommer, C., Dietrich, I., and Dressler, F. 2008. A simulation model of DYMO for ad hoc routing in OMNeT++. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (March 8-12, 2005). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 76.*

Soni, B., Sarkar, B., and Rajput, A. 2013. Improvising the Ad hoc on Demand Distance Vector Routing Protocol When Nodes or Links Fails. In *Proceedings of the All India Seminar on Biomedical Engineering (AISOBE 2012). Springer, India (2013). 285-292.*

Sridhar, S., Baskaran, R., and Chandrasekar, P. 2013. Energy Supported AODV (EN-AODV) for QoS Routing in MANET. Procedia-Social and Behavioral Sciences 73 (2013) , 294-301.

Su, M. 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications 34, 1 (2011), 107-117.

Tan, S., and Kim, K. 2013. Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In *Proceedings of the IEEE International Conference on ICT Convergence (ICTC) (2013). 1027-1032.*

Thorup, R. 2007. Implementing and evaluating the DYMO routing protocol. PhD diss., Aarhus Universitet, Datalogisk Institut. 2007.

Trung, H.D., Benjapolakul, W., and Duc, P.M. 2007. Performance evaluation and comparison of different ad hoc routing protocols. Computer Communications 30, 11 (2007), 2478-2496.

Wang, B., Chen, X., and Chang, W. 2014. A light-weight trust-based QoS routing algorithm for ad hoc networks. Pervasive and Mobile Computing. 13 (2014), 164-180.

Wietrzyk, B. 2008. Practical mobile ad hoc networks for large scale cattle monitoring. PhD diss., University of Nottingham. 2008.

Wu B., Chen, J., Wu, J., and Cardei, M. 2007. A survey of attacks and countermeasures in mobile ad hoc networks. Wireless Network Security (2007), Springer US. 103-135.

Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. 2004. Security in mobile ad hoc networks: challenges and solutions. Wireless Communications, IEEE Trans 11, 1 (2004), 38-47.

Yi, J., Parrein, B., and Radu, D. 2011a. : Multipath routing protocol for manet: Application to H. 264/SVC video content delivery. In *Proceedings of the 14th IEEE International Symposium on Wireless Personal Multimedia Communications (WPMC). 1-5.*

Yi J., Adnane, A., David, S., and Parrein, B. 2011b. Multipath optimized link state routing for mobile ad hoc networks. Ad Hoc Networks 9, 1 (2011), 28-47.

Yi, P., Dai, Z., Zhang, S., and Zhong, Y. 2005. A new routing attack in mobile ad hoc networks. International Journal of Information Technology 11, 2 (2005), 83-94.

Yitayal, E., Pierson, J., and Ejigu, D. 2014. A Balanced Battery Usage Routing Protocol to Maximize Network Lifetime of MANET Based on AODV. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems (2014). Springer International Publishing, 266-279.

Rutvij H. Jhaveri is a Ph.D. scholar in the Department of Computer Engineering, CSPIT, CHARUSAT University, Changa, India. He has completed his Master′s degree in Computer Engineering from Saradar Vallabhbhai National Institute of Technology, Surat and Bachelor of Engineering from Birla Vishvakarma Mahavidyalaya, V.V.Nagar in India. Since 2002, he is working as an Assistant Professor in SVM Institute of Technology, Bharuch, India affiliated to Gujarat Technological University.
He serves as a reviewer in high quality journals such as *Wireless Networks (Springer)* and as a program committee member/reviewer in renowned International conferences. He authored several papers/book-chapter(s) published by prominent publishers such as *Springer*, *Elsevier*, *IET* and *IEEE*. Some of these articles are published in renowned international journals such as *Wireless Networks (Springer)* and *INFOCOMP Journal of Computer Science*. His papers have received 320+ peer citations as of November, 2015. He is also a member of various technical organizations such as ISTE, IDES, IACSIT, ICST and others. His research interests include issues and challenges in wireless ad-hoc networks and information security.

Narendra M. Patel received his B.E. degree in electronics engineering from M.S. University, Baroda in 1993 and M.E. degree from M.S.University, Baroda in 1997. He received Ph.D degree from SVNIT, Surat in 2012. He is currently Associate Professor in Computer Engineering Department, B.V.M. Engineering College, V.V.Nagar, India. His research interests include Digital Image Processing, Real Time Operating Systems, Distributed Systems and Computer Graphics. He authored more than 40 papers which are published in prominent international journals and conference proceedings. He has guided more than 50 Master′s dissertations in Computer Engineering.