

# Study of Mobile Ad hoc Network Routing Protocols in Smart Environment

Munisha Devi<sup>1</sup>, Nasib Singh Gill<sup>1</sup>

<sup>1</sup> Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India.

\*Corresponding author

## Abstract

The two primary strategies for designing any wireless network are Protocol Selection and Path Routing. The protocol selected in the network should be the best, in terms of data integrity and data delivery. Therefore, before selecting any protocol, we should analyze its performance. The main problem with most of the routing protocols is that, they rely on mobile nodes and based on the assumption that nodes will cooperate or behave appropriately but there might be circumstances where some particular set of nodes may not cooperate appropriately. Most of the MANET protocols becomes ineffective and presents the declined performance while mitigating with large number of malicious nodes. Such set of malicious nodes interrupt the data flow, but support the flow of route discovery traffic, causing the protocol to select another route or to restart the route discovery process. There are various types of attacks in network like Impersonation Attack, Selfish Node Misbehaving, Denial of Service (Dos), Routing Table Overflow Attack, Flooding Attack, Sybil Attack, Black Hole Attack, Wormhole Attack.etc. Hence to deal with such types of attack mobile ad Hoc network must have an effective and better security mechanism. In this paper various research gaps have been summarized for different MANET algorithms along with their performance in recent years.

**Keywords:** MANET, AODV, TORA, DSR, LAR, DSDV, IoT, GPS

## INTRODUCTION

MANET contain autonomous mobile nodes that group together to create a wireless mobile network without the help of any fixed infrastructure or any centralized management. To maintain secure, robust and efficient routing, protocols becomes one of the huge concerns in MANET, and many researchers attracted by it. Routing protocols are usually needed for retaining effective and well organized transmission between source to destination and also for maintaining the routes among mobile nodes and designing path for forwarding packets. The main problem of most of the routing protocol is that, routing protocols depends upon the mobiles nodes, and depending on the situation, that these mobile nodes will work properly, but due to their mobile behavior there is higher feasibility of circumstances where particular node group may not work properly[1]. While communicating with large scale of malicious nodes, most of the routing protocols are witnessed for reduced performance, which certainly maintains

the course of exploration routing, but also distort the path of the data providing the routing protocol to chose an unconventional route (in case it is available) or to resume again the route exploration procedure.

## CATEGORISATION OF MANET PROTOCOLS

MANET routing protocols can be categorized into various types as shown below:

*Location Based Routing:* LAR (location aided routing) protocol is an example of location based routing. Location information of a particular object can be detected by various systems like GPS (Global positioning system). Location based routing uses the real location of nodes, to make routing decisions routing decisions in mobile networks.

*Energy Awareness Based Routing:* Multiple entries of routing in routing tables are supported by each node in the network. Routing assessing power levels of network nodes is available for choosing best path in the wireless medium. In this situation, routing table corresponding to the energy level of nodes and retained by sending hello packets among nodes at the energy level. Hence the number of network nodes is provided by the total number of entries in routing tables.

*Topology Based Routing:* Here the routing types are: On Demand (Reactive) Routing Protocol, Table Driven (Proactive) Routing Protocols, and Hybrid Routing Protocols [2]. The routing protocols of MANETs are expressed in the below figure.

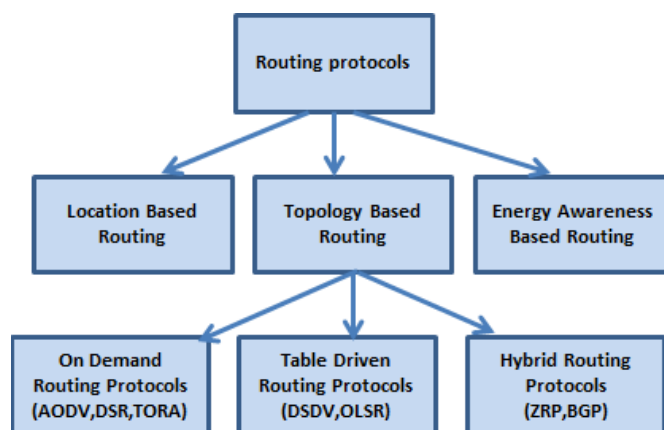
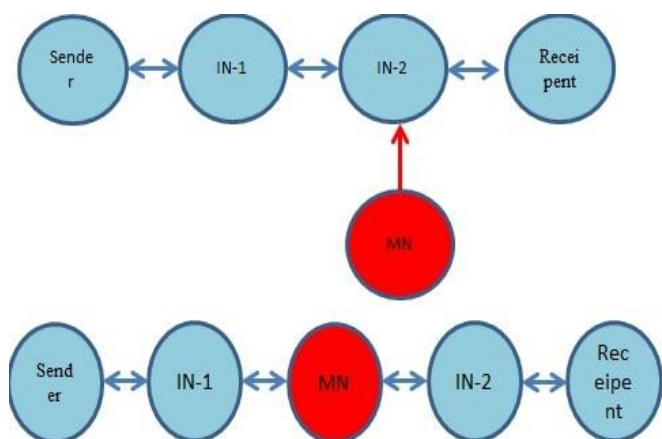


Figure 1: Routing Protocols in MANET

## ROUTING ATTACKS

Routing attacks are network layer attacks such as wormhole attacks, Sybil attacks, black hole attack, spoofing information etc. There is an urgent need to ensure routing security in Ad-Hoc mobile networks, so that the success of the routing operation can be guaranteed. Due to the absence of infrastructure in target network protecting routing work becomes more challenging. The routing attack can be expressed in the below figure. The network traffic can be completely absorbed by a malicious node (MN). The malicious nodes introduce themselves within the link between sender and recipient along with the middle nodes (IN-1, IN-2) and perform unauthorized access in the network.



**Figure 2:** Routing attack in network

There are various types of attacks in the network layer for example packet forwarding and routing attack [3]. An attack can be initiated by the malicious or infected routing nodes in MANET by deploying different ways some of the main types of routing attack are as follows:

*Route Catch Poisoning Attack:* It uses the advantages of promiscuous mode to update the routing table, which typically occurs when confidential information in the routing table is erased, modified, or randomly written with forgery content.

*Rushing Attack:* Reactive routing protocols are highly targeted by these attacks.

*Replication of Packet:* Here (old or out of date) packets are duplicated by the malicious node for unwanted resource consumption and bandwidth consumption.

*Poisoning of Routing Table:* In this type of attack, fake routing updates are sent by the malicious nodes

*Routing Table Overflow Attack:* It usually take place in table driven routing protocols, the prominent job of this types of attack is to make large set of routes so that creation of new path can be resisted.

## Attacks on Particular Routing Protocol

Prior research work represented various attacks in Ad Hoc networks. The routing protocol specific to the attacks are as follows:

*AODV:* AODV is on Demand Protocol. To disrupt the routing process fake routing information is broadcasted by the attacker or we can say that instead of broadcasting original information, attacker broadcast a route with less distance parameter [4].

*DSR:* Here attacker easily modifies the source route info, given in the control message (Route Request, Route Reply)

*SEAD:* It is based on DSDV. It cannot stand for wormhole attack [5].

*ARIADNE:* It is based on DSR, it is reactive protocol it is mainly targeted by rushing and wormhole attack, but robust for denial of service attack [5].

Location Disclosure Attack, Resource Consumption Attack, Rushing Attack, Byzantine Attack, Black hole Attack, Wormhole Attack are some other types of attack other types of attack commonly used in Literature.

## SURVEY OF EXISTING TECHNIQUES

Dr. Ajay Jangra et. al. [6] referred to the problem of routing protocols in detail. They have taken various performance metrics like energy consumption; route Optimization and latency for comparison analysis of various routing protocols. They discussed that in dense or sparse area there is interconnectivity among various gadgets and movement models can be used for controlling device movement purpose and hence stated that routing process is clearly affected by movement of nodes in the network.

In [7] two very important protocols of MANETs (Destination-sequenced distance-vector and Ad Hoc On-Demand Distance Vector Routing) have been reviewed by authors. And a comparison between DSDV and AODV has been done by them. By studying their review work, we can choose protocols according to performance and scenarios, and we can tell which routing protocol could better perform in particular circumstance.

Khattab M. Aliet. al. [8] presented a novel strategy in which new approach has been brought to the smart environment to save the consumer power of devices. In wireless sensor networks a novel scheme is proposed for managing the sleep of nodes in networks. So that network connectivity can be kept and energy can be stored for future. The key feature of the scheme is its simplicity. The effectiveness and convenient feature makes this approach more beneficial and this has been successfully applied to many places of the networking.

Authors in [9] presented a new AODV-EHA algorithm that enhanced the quality of service as well as enhanced the life time of sensor node under different energy condition and

variable traffic load for mass deployment of mobile network they considered energy harvesting (EH) as the key enable technology, in the network.

Authors in [10] presented a paper in which they enhanced the performance of AODV protocol. Comparison has been done between enhanced AODV protocol and existing MANET protocols. Improvement is done under the area of various attacks on AODV. And they have also discussed the black hole attack in detail.

Authors in [11] presented a paper, which was completely based on security of smart environment and its requirements in the upcoming networks. They discussed how the network can be successfully implemented in Smart City, smart building, Smart home, smart car and they mentioned the risk and challenges attached with IoT system.

It is always very expensive to find a new route for transferring packets in network. Hence a new approach for cache updating using distributed route cache update algorithm is proposed by V. V. Mandhare, R. C. Thool [12]. In UDSR distributed cache replacement algorithm, route error information of size sixty bytes was broadcasted by a source node to all its neighbors. Hence stale route was replaced by all the neighbor nodes in their cache. Using different quality of service parameters the performance has been improved up to thirty forty percent by the new proposed approach.

Dr. P. Venkata Krishna et. al. [13] proposed a new method for Delay tolerant in Mobile ad hoc networks. They proposed a new opportunistic adaptive routing protocol. They used a proactive method for routing mechanism and by including a new concept called HUB they had chosen a new route between source and destination. The fitness value of all the nodes in the network has been found by the routing protocols and the nodes having highest fitness value are chosen for the further process.

Samiksha Nikam, B. T. Jadhav [14] used DSDV (destination-sequenced distance-vector) protocol to analyze the delay factor in mobile network. The delay was observed in both, low and high conditions by taking various factors like speed pause time, total number of nodes, connection between the nodes, etc.

Mohd.Imran, Mohammed Abdul Qadeer [15] presented a comprehensive study for two routing protocols DSDV and AODV. Characteristics of both protocols have been compared. For analyzing trace file, trace graph tool of ns-2 simulator have been used. The conclusion shows that under high mobility scenario AODV attains better performance and efficiency than DSDV.

In this paper [16] two types of network has been used, one was local Ad Hoc Network and other was Overlay networks. Overlay networks performed better than local Ad Hoc networks. And performance comparison analysis has also been done. The prominent task was to improve the efficiency of routing protocol in mobile network.

Security becomes an important topic in routing protocols in adhoc networks. Brijendra Kumar Joshi et. al in [17] presented performance analysis of routing protocols and also presented security analysis under various types of attacks.

To control the congestion problem of mobile network two solutions has been given by Syeda nyma ferdous et. Al. [18]. Drop factor has been used for simulation of energy based scheme. We can easily conclude from the result that proposed solution is far better than the existing AODV protocol with respect to delay, throughput, delivery ratio etc.

Dr. P.M. Jawandhiya et. al. [19] focused on the importance of deficiency related consideration. Comparative performance analysis of routing protocols has been done.

Prakhyalakhya Das et. al. [20] reviewed three widely used routing protocols (Dynamic MANET on Demand (DYMO), Dynamic Source Routing (DSR), Ad-hoc On Demand Distance Vector (AODV)). Evaluation has been done using various factors ex. mobility and traffic density.

Ashish Kumar Awadhya et. Al.[21] provided a survey on the effects of mobility on the links lifetime. Hou Songfan et. Al. [22] used a real multichip smart (Internet of Thing) environment to compare the performance of two routing protocols.

Vanita Bokhare et. Al. in [23] came up with new concept of innovative broadcast method, and solved tumble down routing blockage problem.

Mechanisms of some widely used existing MANET routing protocols (such as OLSR, DSR, AODV) have been studied here [24]. And there execution is exploited in internet of things circumstances to find an accurate mechanism of routing for IoT future.

Sudhir Goswami et. al. [25] proposed a new location based energy efficient technique with an AODV protocol. Here the routing ability of AODV protocol was improved by energy dependent nodes with the help of LAR protocol.

They Pravanjan Das et. al. [26] modifies the existing SEAR-AODV routing protocol, and proposed a new multipath protocol with less consumption of energy.

Sang-Hyun Park et. al. [27] proposed a new algorithm, energy efficient probabilistic routing probabilistic routing (EPR). Under the flooding algorithm to decrease the packet loss problem and to increase the network lifetime and to control the transmissions of routing request they used EPR algorithm.

For the evaluation of two active Manet routing protocols (AODV, DSR) and one proactive routing protocol (DSDV) a mathematical model is presented [28] here, which work for performance evaluation and presimulation TCL files.

This paper [29] examine through transmission power, mobility models and simulation the fundamental factors, which have a great effect on the performance of location

based routing protocol. Here performance analysis has been done under two different mobility models.

After observing the old wireless sensor network interoperability efforts for urban sensing, Paolo Bellavista et. al. [30] came up with new solution for impromptu and MANETs delays.

Considering the power consumption factor, evaluation of MANET routing protocol have been done. The proposed method [31] reduces the network delay and minimizes twenty percent of total energy consumption.

Authors in [32] presented a performance comparison of ad-hoc networks protocols with respect to different parameters.

After observing the result of [33] we can conclude that for large client mesh network, where more throughputs is needed, we should use the AODV routing protocol for the video streaming applications.

Sheng Liu, Yang Yang, Weixing Wang [34] presented B-AODV (improved approach), a new optimized routing protocol. Which was based on the concept of finding the shortest route in network. This paper presents key techniques of mobile adhoc network, its basic characteristics, and compared it with the mobile communication system.

Here [35] author's Presented a paper in which energy consumption problem in adhoc network is solved by the proposed algorithm and it also helpful for solving routing problem in network. In static network they also presented energy optimal path algorithm using greedy method. And the proposed algorithm presented better simulation result.

R. Madhan Mohan et. al. [36] presented a paper in which a modified and enhanced version of AODV protocol is invented and the protocol is modified in such a way that only target node can respond to route request. And this was helpful in reducing control data messages into the networks. Using modified AODV protocol they have presented an adaptive routing concept in mobile network.

For multicasting networks, reliable and more energy efficient congestion control protocol is proposed by K. Srinivasa Rao et. al. [37]. This paper concentrates on congestion control in MANET. Authors have mentioned Energy Efficiency, challenges, properties of MANET. Various type of algorithm along with their properties has been also discussed here.

Yicong tian's [38] proposed work shows that, AOMDV-IoT protocol shows better simulation result as compared to AOMDV. A method was designed, which used to take function of both network node as well as routing destination.

David Espes et. al. [39] presented a paper, here the numbers of control packets were reduced, and backbone network was used by an AODV based protocol for minimization of control packets. GPS has given the destination location which was transmitted to the initial node by backbone network.

In this paper [40] security of protocols are enhanced and ensures that the data is not taken through malicious nodes that

are known for Misbehave. A direct and recommendations trust model is used as trust mechanism and it is incorporated inside Ad Hoc on demand distance vector routing protocol, which help to find a trustworthy routing path.

Authors [41] presented comprehensive study of various MANET routing protocols and they represented some important features, characteristics. Protocols performance is analyzed and compared using mobile scenario. MANET features are also discussed by the authors.

## MANET CHALLENGES

In addition to the attractive Application, there are many drawbacks within the network, which should be studied carefully. Mobile ad Hoc Network faces many challenges some of these challenges are as follows:

*Fault Tolerance:* protocol should be adaptable according to the dynamic network station. In unfavorable environment, a host may fail due to lack of energy or due to certain problems. If the host fails it is duty of routing protocol to adjust these changes in network.

*Physical Resource Constraints:* More energy consumption and Limited battery power is the main issue in mobile Ad Hoc Network.

*Ad Hoc Deployment:* Hosts are randomly established in adhoc networks without any prior infrastructure and topology information. In a specific area establishment varies according to the application.

*Scalability:* the routing protocol should be flexible enough to add, operate and respond large number of hosts in the network. When the network expands it is important that the protocol handle it reliably and smoothly.

*Quality of Service:* The quality of service is very important factor for most of the applications like video and audio streaming. Here it is very important that the data packets sent by sender reach the destination reliable reach the destination reliable and timely.

*Routing:* Due to the constantly changing topology, it is difficult to route packets between pair of nodes. So most protocols should be based on On demand routing instead of table driving routing. Multicasting routing has also become a big challenge. Many applications of the network uses, many to many and one to many communication pattern. The routing of packets in this situation becomes very difficult.

*Security:* Security has become a very important issue of the network, for various applications like military, battlefield operations, security is the main issue. The inherent features of mobile networks such as limited physical security, resource constraint capability, distributed corporation, highly mobile topology, wireless medium poses number of privacy challenges to the network.

Following are the different MANET techniques with their benefits and limitations.

**Table 1:** Prior research work (various research gaps summarized for different MANET algorithms)

Author	Year	Technique	Benefits	Limitations
Nidhi Divecha	2017 [10]	Bluetooth network expansion using AODV	Implementing prevention technique of black hole attack gives higher security and less packet drops and throughput.	With large no. of nodes consumes almost the entire bandwidth. Packet drop ratio could be further reduced. Not so much applicable for large network.
Anjana Tiwari, Inderjeet Kaur	2017 [42]	Performance Evaluation of Energy Efficiency For MANET	The Result of proposed method is much better than the existing AODV routing protocol. Compute the best outcome characteristics.	This proposed method can be simulated in different routing protocols with multiple security mechanism. For Ex. Secure communication. Also extend this work by proposing more efficient methods.
V.V Mandhar and R.C. Thool	2016 [12]	Cache Replacement Algorithm	Stale route Problem solved up to certain level. Proposed approach improved performance up to 30%.	Performance decreases as the network increases. Drop more packets even if the network had few malicious users.
Mohd. Imran, Mohammed Abdul Qadeer	2016 [15]	Comparison of Topology based Routing Protocol	Simulation results show the performance of two main protocols with respect to the average end to end Delay, Throughput.	Work has been done using two parameters. More numbers of parameters could be taken.
S. S. Asole	2016 [43]	Comparison of routing protocol.	Provide an outcome as to which routing protocol is better.	Has not mention packet drop rate and applicable to limited system size.
Samiksha Nikam	2016 [14]	A fuzzy approach used	Reduce the delay in mobility.	More numbers of parameters could be taken.
Sudhir Goswami & Chetan Agarwal	2015 [25]	Energy efficient scheme for maximize routing capability.	Work has been done for energy conservation. Work has been done to increase the network lifetime.	Still issue of power aware or energy efficiency. Performance low due to congestion occurs in network.
Hrishabha Raj	2014 [44]	Energy efficient secure multiply path EESM, AODV	Energy consumption less.	AODV rout discovery latency is high.
Eman S. Alwadiyeh	2013 [45]	Uses the technique of ESDMR, EDMR.	Improvement in throughput. Improves packet delivery ratio, reducing the impact of hidden terminal problem.	More difficult to configure, implementation require additional planning a configuration.
Dr.Asha shripadambhai ka	2012 [46]	Randomized energy based AODV protocol for wireless adhoc network.	Improved AODV protocol for solving link failure problem in MANET.	Work has been done with small number of nodes.
Bikesh Chandra Singh	2011 [47]	Analysis of UDP performance in MANET.	Comparison done between DSDV, DSR, AODV.	Impersonation attacks problem. No any method provided for improving efficiency of protocols.

Amrit Suman	2011 [48]	Analyzed FISHEYE, AODV, DYMO against Wormhole attack in Manet.	Better result for Worm Hole Attack.	N/A
Moitreyee Dasgupta Choudhury Chaki	2010 [49]	Designed Mechanism of route request (RREQ) forwarding.	Better result for Rushing attack.	Designed mechanism provides better result for Rushing attack Only.
M. Ramakrishnan & S. S. Hanmugavel	2006 [50]	FPGA implementation of DSDV.	React quickly to dynamic topology changes.	High network routing overhead. We can further enhance the functioning.

## CONCLUSION

MANET should have an effective and better security services, because various upcoming applications of MANET are on the way in future. Reducing the routing problems will develop a secure, efficient and better application in MANET. We have summarised almost all the existing MANETs techniques. After Extensive literature survey, we realized that there are a lot of security problems in mobile ad hoc network and various challenges need more attention. We will have to take more action for better performance in upcoming smart environment.

## REFERENCES

- [1] G. N. Anil, "Semantic Probabilistic Modelling of novel routing Protocol with Implication of Cumulative Routing Attack in Mobile adhoc network," 2012, vol. 9, no. 1, pp. 340–349.
- [2] R. Balakrishna, Z. Hussain. A survey on manets-types, characteristics, applications and protocols used. National Conference on Frontiers and Advances in Information Science and Technology FAIST13; 23–24 May, 2013;. Bangalore, India: RRCE; 2013.
- [3] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s):38- 47, ISSN: 1536-1284
- [4] Nishu Garg and R.P.Mahapatra, "MANET Security Issues," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.
- [5] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.
- [6] N. Jeba and V. Kamala, "A Survey on Routing Protocols for Internet of Things," in *International Journal of Advanced Research in Science, Engineering and Technology*, 2016, vol. 3, no. 5, pp. 1993–1996.
- [7] S. J. Patil, "Available Online at [www.ijarcs.info](http://www.ijarcs.info) A Review On Trust Based Secure Routing Protocols In Ad-Hoc Networks," 2017, vol. 8, no. 976, pp. 661–668.
- [8] K. M. A. Alheeti, "Conservation Based on Routing Protocol," 2017, pp. 69–74.
- [9] T. D. Nguyen, J. Y. Khan, and D. T. Ngo, "An effective energy-harvesting-aware routing algorithm for WSN-based IoT applications," in *IEEE International Conference on Communications*, 2017.
- [10] Nidhi DIVECHA "Solution to Bluetooth Network Expansion using AODV- Ad HOC Routing Protocol," 2017, vol. 7, no. 4, pp. 10683–10688.
- [11] S.-R. Oh and Y.-G. Kim, "Security Requirements Analysis for the IoT," in *2017 International Conference on Platform Technology and Service (PlatCon)*, 2017, pp. 1–6.
- [12] V. V. Mandhare and R. C. Thool, "Improving QoS of Mobile Ad-hoc Network Using Cache Update Scheme in Dynamic Source Routing Protocol," in *Procedia Computer Science*, 2016, vol. 79, pp. 692–699.
- [13] S. Informatic, J. Anantapur, and V. Ramana, "T O L E R A N T M O B I L E A D - H O C N E T W O R K S M . V e n k a t a R a m a n a 1 , D r . P V e n k a t a K r i s h n a 2," 2016, vol. X, pp. 25–29.
- [14] Samika Nikam "Delay Analysis Of Adhoc Network," 2016, vol. 8, no. 9, pp. 7–11.
- [15] M. Imran and M. A. Qadeer, "Evaluation Study of Performance Comparison of Topology Based Routing Protocol, AODV and DSDV in MANET," in *2016 International Conference on Micro-Electronics and*

- Telecommunication Engineering (ICMETE)*, 2016, pp. 207–211.
- [16] P. Dwivedi, “A Prototyped Ad Hoc Routing Protocol for Efficiency Enhancement for Routing in MANET,” 2016, vol. 133, no. 13, pp. 15–17.
- [17] B. K. Joshi, “Security Assessment of AODV Protocol under,” 2016, pp. 173–177.
- [18] S. N. Ferdous and M. S. Hossain, “Randomized energy-based AODV protocol for wireless ad-Hoc network,” in *2016 3rd International Conference on Electrical Engineering and Information and Communication Technology, iCEEiCT 2016*, 2017, pp. 1–5.
- [19] P. M. Jawandhiya and S. S. Asole, “Performance analysis of mobility models using routing protocols, traffic models and provides an outcome as to which routing protocol is better,” in *2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016*, 2017, pp. 0–4.
- [20] P. Das and D. D. Seth, “Performance analysis of routing protocols for adhoc network in a fading environment,” in *2016 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2016*, 2017, pp. 6–10.
- [21] A. K. Awadhiya, S. Mishra, and V. Sharma, “Link Lifetime Prediction in Mobile Adhoc Network: A Survey,” 2016, vol. 5, no. 7, pp. 736–740.
- [22] S. Hou, M. Wu, W. Liao, and D. Wang, “Performance comparison of AODV and DSR in MANET test-bed based on Internet of Things,” in *2015 IEEE 82nd Vehicular Technology Conference, VTC Fall 2015 - Proceedings*, 2016, pp. 3–7.
- [23] V. Bokhare and S. Suryavanshi, “A secure NCPR for reducing routing overhead in MANET,” in *2015 4th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2015*, 2015.
- [24] H.-M. Xin and K. Yang, “Routing {Protocols} {Analysis} for {Internet} of {Things},” in *2015 2nd {International} {Conference} on {Information} {Science} and {Control} {Engineering} ({ICISCE})*, 2015, no. i, pp. 447–450.
- [25] S. Goswami, C. Agrawal, and A. Jain, “Location based Energy Efficient Scheme for Maximizing Routing Capability of AODV Protocol in MANET,” in *International Journal of Wireless and Microwave Technologies*, 2015, vol. 5, no. 3, pp. 33–44.
- [26] L. Almazaydeh, E. Abdelfattah, M. A.- Bzoor, A. A.- Rahayfeh, and C. Science, “P Erformance E Valuation of R Outing,” 2010, vol. 2, no. 2, pp. 64–73.
- [27] S. H. Park, S. Cho, and J. R. Lee, “Energy-efficient probabilistic routing algorithm for internet of things,” *J. Appl. Math.*, vol. 2014, 2014.
- [28] G. R. Pathak, S. H. Patil, A. D. Rana, and Y. N. Suralkar, “Mathematical model for routing protocol performance in NS2: Comparing DSR, AODV and DSDV as example,” *Proc. - 2014 IEEE Glob. Conf. Wirel. Comput. Networking, GCWCN 2014*, pp. 184–188, 2015.
- [29] A. Macintosh, M. FeiSiyau, and M. Ghavami, “Simulation study on the impact of the transmission power on the performance of routing protocols under different Mobility Models,” *Innov. Comput. Technol. (INTECH), 2014 Fourth Int. Conf.*, pp. 185–190, 2014.
- [30] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT urban scenarios,” *IEEE Sens. J.*, vol. 13, no. 10, pp. 3558–3567, 2013.
- [31] Shivashankar, H. N. Suresh, G. Varaprasad, and G. Jayanthi, “Notice of Violation of IEEE Publication Principles Designing Energy Routing Protocol With Power Consumption Optimization in MANET,” *IEEE Trans. Emerg. Top. Comput.*, vol. 2, no. 2, pp. 192–197, 2014.
- [32] O. Of and R. Protocols, “Comparative Performance Analysis of.”
- [33] K. A. Ai-ghadanfary and D. M. B. Al-Somaidai, “Simulation of Some Routing Protocols in a Client Wireless Mesh Networkfor Multimedia Applications,” *First Int. Conf. Electr. Commun. Comput. Power Control Eng.*, 2013.
- [34] S. Liu, Y. Yang, and W. Wang, “Research of AODV Routing Protocol for Ad Hoc Networks1,” *AASRI Procedia*, vol. 5, pp. 21–31, 2013.
- [35] A. Chaturvedi, D. N. Goswami, and T. Sharma, “Energy Optimal Path Algorithm for routing in Static Adhoc Network using Greedy Approach (EOGR),” *Int. J. Comput. Appl.*, vol. 48, no. 24, pp. 23–28, 2012.
- [36] R. MadhanMohan and K. Selvakumar, “An Energy Efficient Routing in Mobile Adhoc Networks using Aggregate Interface Queue Length and Node Remaining Energy,” *Int. J. Comput. Appl.*, vol. 42, no. 19, pp. 8–12, 2012.
- [37] K. S. Rao, R. S. Kumar, P. Venkatesh, R. V. S. Naidu, and A. Ramesh, “Development of Energy Efficient and Reliable Congestion Control Protocol for Multicasting in Mobile Adhoc Networks compare with AODV Based on Receivers,” vol. 2, no. 2, pp. 631–634, 2012.
- [38] Y. Tian and R. Hou, “An improved AOMDV routing protocol for internet of things,” *2010 Int. Conf. Comput. Intell. Softw. Eng. CiSE 2010*, pp. 0–3, 2010.
- [39] D. Espes and C. Teyssié, “Approach for Reducing Control Packets in AODV-based MANETs,” 2007.

- [40] S.Hu, "Dynamic Monitoring Based On Wireless Sensor Networks of IoT," pp. 0–3, 2015.
- [41] S. Naski, "Performance of Ad Hoc Routing Protocols : Characteristics and Comparison," *Ad Hoc Networks*, 2005.
- [42] A. Tiwari and I. Kaur, "Performance Evaluation of Energy Efficient For MANET Using AODV Routing Protocol," *3rd IEEE Int. Conf. "Computational Intell. Commun. Technol. (IEEE-CICT 2017)*, pp. 1–5, 2017.
- [43] P. M. Jawandhiya and S. S. Asole, "Performance analysis of mobility models using routing protocols, traffic models and provides an outcome as to which routing protocol is better," in *2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016*, 2017, pp. 0–4.
- [44] H. R. Jain, "International Conference on Advances in Engineering and Technology Research (ICAETR), 2014," *Improv. Energy Effic. Secur. Multipath AODV Routing Protoc. MANET*, pp. 1–9, 2014.
- [45] E. S. Alwadiyeh and A. F. a Aburumman, "Interference-aware multipath routing protocols for mobile ad hoc networks," *38th Annu. IEEE Conf. Local Comput. Networks - Work.*, no. December, pp. 980–986, 2013.
- [46] A. Ambhaikar, H. R. Sharma, and V. K. Mohabey, "Improved AODV Protocol For Solving Link Failure In MANET," *Int. J. Sci. Eng. Res.*, vol. 3, no. 10, pp. 1–6, 2012.
- [47] Bikash Chandra Singh, Tapan Kumar Godder, S. Miah, and H. M. Abdul Awal, "Experimental Analysis of UDP Performance in Mobile Ad Hoc Networks with Different Routing Protocols and varying payload," *Int. J. Distrib. Parallel Syst.*, vol. 2, no. 6, pp. 107–113, 2011.
- [48] A. Suman, "A Behavioral Study of Wormhole Attack in Routing for MANET," vol. 26, no. 10, pp. 42–46, 2011.
- [49] M. Dasgupta, "Routing Misbehavior in Ad Hoc Network," *Int. J.*, vol. 1, no. 18, pp. 94–97, 2010.
- [50] M. Ramakrishnan and S. Shanmugavel, "Implementation Network," 2006.