Adaptive Traffic Routing Practice for Load Balance and Congestion Control in AdHoc Network in Cloud-MANET

Surjeet Dalal · Neeraj Dahiya · Bijeta Seth · Vivek Jaglan · Meenakshi Malik · Surbhi · Uma Rani · Dac-Nhuong Le · Yu-Chen Hu

Received: 15 July 2021/ Accepted: date

Abstract Cloud services can dramatically improve the computing proficiency of mobile devices. Mobile operators can count on the cloud to carry out thorough computing operations such as research, data mining and multimedia handling. Load balancing and network congestion are the difficult ad hoc net-
work tasks due to its un-predictable dynamic behavior and random topology alteration of such systems. The most important reason of data loss in wireless grids is flexibility, network congestion and channel errors. The majority of the accessible directing schemes deal with the energy efficiency, congestion and balancing overload outstandingly. Proficient routing protocol is proposed in this manuscript which will adaptively control the network congestion and achieve load balancing in Mobile Ad Hoc Networks (MANET). The proposed technique discovers multiple alternate paths between two nodes. The cost and stability of the link and traffic load is calculated depending on the available power of the participated nodes. If the traffic load on a specific link escalates beyond the threshold value, the traffic will be distributed to other alternate links. It is clear with the simulation outcomes that the projected approach enhances the network lifespan by integrating load balancing and congestion control with energy efficient algorithm. Thereby, it reduces the packet dropping probability and node to node delay in the network and improves the system lifetime.

**Keywords** Congestion control · load balance · MANET · adaptive traffic routing

1 Introduction

In the recent years, considerable development has taken place in wireless technologies to assist multimedia applications over adhoc networks. The wireless networks are useful in multimedia services and other data related services. Ad hoc wireless networks have less network setup. They do not have permanent topologies to wrap a wide area. The structure may alter in a dynamic and unpredictable manner at any time as the nodes might be on mobility. Devices in these networks are autonomous. These autonomous devices communicate with all using multiple hops connected by wireless links.

Smart devices have made our lives easier than before and have created a connection amid other smart devices through wireless networks. MANET is a self-organizing system of mobile nodes which lack federal control and is associated with wireless links. Because of its basic structure which is infrastructure less, the chance of attack on any of the nodes and thus the whole MANET system increases. Cloud offers services to MANET clients. A Cloud-MANET is a new notion that is distinct from the traditional broadcasting network because the nodes act as routers instead of serve ends.

The remainder of the paper is planned in the following manner. Overview of techniques and literature survey is discussed in Section 2. The proposed technique is discussed in Section 3. Section 4 discusses simulation and performance analysis. Section 5 mentions the conclusion of the paper.
2 Overview of CloudMANET

In the present era of computers, the MANET is playing a prominent part in the Internet of Things (IoT). Current cellular networks don’t enable intelligent devices to link without central infrastructure. This new combination allows for the development of intelligent device capabilities. An adhoc system can link smart devices in a decentralized manner. MANET automatically organizes and links to a distributed system. All MANET devices can travel from place to place in any route. They can make a system out of their neighbours’ and transfer information to another node. The IoT-Cloud-MANET framework for intelligent devices is made up of IoT, cloud computing and MANET. This system makes it possible to enter and provide cloud services to MANET clients via their intelligent devices in the IoT framework in which all the calculations, information management and asset allotment are borne away. Smart devices can travel between locations on the MANET network. This section provides an overview of employed techniques.

2.1 Ad Hoc Network

Fig. 1 represents the wireless ad-hoc network which has mobile nodes and is not facilitated with an external device or control means [1]. It may be determined that initial and destination nodes are allied through multi-hop communication and achieve congestion-less path to attain consistent communication. A decentralized infrastructure with cloud capabilities would no doubt alter the prospects for today’s IoT. In this way, improved communication and data exchange between intelligent devices is attained.

![Notion of ad hoc wireless network](image)

**Fig. 1** Notion of ad hoc wireless network

Wireless ad hoc networks offer many advantages, such as:
- Use to build extensive networks.
– Set up sophisticated protocols.
– Diminish the amount of (wireless) communication needed to complete distribution tasks.
– Implement complex power saving modes depending on your system.

However, several challenges exist in mobile environments. They can be categorized:

1. Limitations of the wireless web.
   – Thrashing of packets.
   – Variable capacity associations.
   – Recurrent log outs.
   – Restricted communication bandwidth.
   – The extent to which communications are broadcast.

2. Limitations associated with mobility.
   – Dynamic topologies and routes.
   – Need of awareness about the system.

3. Shortcomings of mobile computer
   – Small duration of the battery.
   – Limited capacities.

2.2 Cloud Mobile Ad Hoc Networks (MANET)

The introduction of various computer models such as grid computing, parallel computing and distributed computing in a single high computing framework pulled into cloud computing in the technical world. Communication between devices in a point-in-time setting should be distinctive [12] and new [33]. Intercommunication deprived of a centralized method is a very potent mechanism that guarantees reliable communication with clients [30]. Cloud computing is considered as popularized computing paradigms. Cloud Computing proposes three fundamental paradigms:

a. Infrastructure as a Service: these are the systems architects that need infrastructure capabilities.
b. Platform as a service: this is for designers who require platform to build different applications.
c. Software as a Service: it is aimed at the clients who require software for their day-to-day operations.

The Cloud-MANET structure is suitable for peripherals that are situated close by. The user can use this smart device to share videos, pictures, and other data with cloud servers while decreasing information.

The Cloud-MANET network gives users the luxury to connect anywhere and at any time. The combination of the Cloud and MANET offers entrance to the cloud inside the MANET network for intelligent devices. Clients are now seeking a single MANET network to access the network.
Algorithm 1. Phases of the Cloud-MANET framework.

BEGIN
Step 1: Set up a dedicated mobile network.
Step 2: Activate the range’s devoted network.
Step 3: Register client smart devices in MANET.
Step 4: Roll MANET units into the cloud.
Step 5: Employ the IoT-based Cloud-MANET model onto all smart devices and start communicating.
END

Communication amid the smart devices in the Cloud-MANET [5] framework as shown in Fig. 2 is an innovative notion that enables the discovery and connection of smart devices in close proximity with no central structure.

![Cloud-MANET integration scheme](image)

The connection amid smart devices in the cloud-MANET framework connects inside the range of WiFi wireless network is shown above [5]. In IoT Cloud MANET model as shown in Fig. 3 [7], at least one intelligent device must be allied to cellular or WiFi networks. All MANET intelligent equipment must be stored individually in the cloud.

A variety of MANETs can link to a single cloud and utilize cloud services in real time. To connect the MANET intelligent device to the cloud must be built [7] into mobile applications. This technique is deployed as an application and checked on the cloud-MANET of intelligent devices. The cloud services provide a significant approach to communication between many smart devices using routing protocols. The MANET Cloud Mobility Model is a model to link cloud and MANET. The working of MANET depends on the movement of its points and assets [8]. In the MANET Cloud mobility model as shown in Fig. 4, MANET’s devices can converse.
Devices in ad-hoc networks must check the existence of other devices and accomplish the required procedure to ease connections and the division of data and services. Though, with limited bandwidth and shared common channels across all nodes, congestion has developed into more stimulating in ad-hoc wireless networks. It is considered to be the primary factor responsible for performance and bandwidth degradation of the network, packet losses and depletion of time and energy.

The major reason for network congestion is the explosion in real-time multimedia data traffic that requires more bandwidth. The network congestion causes retransmission of information packets, packet losses and bandwidth degradation. It requires more energy and time for recovery from congestion. Finding a new path in congested networks is not only relevant, it could exacerbate the problem of congestion. Consequently, in order to improve network
performance, congestion control technology needs to be launched to efficiently use limited bandwidth and energy resources in MANETs.

The primary purpose of bottleneck control is to reduce buffer overflow and delay system congestion and therefore facilitate the network for better results. In wired networks, the transport layer is responsible for implementing a congestion control system and is designed independently of the functions of the other layers. There are two different categories of routing protocols depending on congestion: protocols adapted to congestion and protocols not adapted to congestion [1]. Various traffic-conscious routing protocols have been designed with factors such as reduction of delays, efficient use of bandwidth, reduction of overhead control costs in MANET in mind. These protocols utilize the shortest path routing procedure which has heavy loads on certain nodes and makes the path unstable. Therefore, instead of the shortest path routing schemas, multi-path routing techniques provide a good result. Some of the current congestion protocols [2, 3] do not adapt to congestion. In congestion aware algorithms, when the new itinerary is established congestion is considered and all the data packets travel along the same route until the route failure and mobility results in link breakage. Whereas, in the process of adaptation to congestion, the route is modified depending on the state of congestion of the network in an adaptive manner. The loss of packets in the MANET is primarily due to congestion [4] which results in a shortened lifespan and loss of network energy. This unwanted power loss can lead to other issues such as bandwidth degradation, increased delay and packet loss. Hence, it is essential to design an adaptive congestion routing algorithm that considers many routing paths and the traffic load of different network nodes. The proposed protocol will perform following tasks: identification of congestion status, remaining energy, and Alternate route discovery.

Certain traits of Cloud-MANET framework are mentioned underneath:

- The framework uses a decentralized infrastructure to communicate intelligent devices.
- It can be embedded in the wireless network zone.
- It is compatible with 5G (heterogeneous array).
- It offers reliable and secure communication.
- Connected smart devices seem to be nodes.
- Using this framework, intelligent tool recognition and communique can be performed in 2D and 3D planes.
- The framework operates dynamically for communications.

The Cloud-MANET framework makes it possible to access and provide cloud facilities to MANET operators via their smart devices. Intelligent devices can change from place to place. Different MANETs can link to a single cloud and utilize the cloud facility in real time. The connection of the MANET smartphone to the cloud needs integration with mobile applications. The communique method for connecting one smart device to a different device as part of the Cloud-MANET should be organized by the IP address [9].
2.3 Detecting, Controlling and Balancing Congestion in MANETs

Various algorithms and techniques for detecting, controlling and balancing congestion are available in MANETs. It is shown that little attention has been paid to congestion techniques. Riasudheen et al. [22] discussed the increase use of Device to Device (D2D) communication in 5G networks. Although, D2D has raised the quantity of clients and the info transmission rate amid cloud MANETs; yet it faces several limitations. The author proposed an Energy Efficient Cloud assisted Routing Mechanism (EECRM) for CA-MANETs. Sathyaraj et al. [23] mentioned the usage of IoT devices in MANET for the support of routing and evaluated trust of IoT devices. A Real-time Secure Route Analysis (RSRA) approach was discussed. Trustworthiness was calculated based on different parameters like location, mobility, speed, energy, neighbors etc. improved the quality of service of MANET. Vyasand Abimamnan [24] mentioned the existing usage of secured algorithmic approach in MANETs. The paper proposed a new combined approach named Alpha Numeric Reflex Routing algorithm. The analysis and discussion of the results obtained was done. Zhang et al. [29] explained Vehicular Ad-Hoc Network (VANET), a spatial MANET with two features like frequent network topology changes and unreliable communication link which arise due to vehicle mobility. The details of the motion characteristics of vehicles were discussed. A link relation duration model based on time duration was proposed and evaluated link reliability. Q-learning algorithm was used to adjust the routing path and reliable self-adaptive routing algorithm was proposed. NS2 simulator was used. Vinoth et al. [34] stated that the existing network approaches lack the balance amid energy and safety in adhoc network. The author focused on security and network traffic issues and proposed a technique called Security based Data Aware Routing Protocol (SDARP) for high data gathering and to attain metrics for security and energy. The protocol worked in two phases. Phase 1 monitored the behavior of cluster head and cluster members. The second phase enhanced the safety with data gathering algorithm.

Alam [30] integrated cloud and MANET to propose a technique whereby all the devices can interact with smart devices in the Cloud-MANET framework. The implementation of a middleware in cloud-MANET mobility model for communication on interact of smart cities was discussed. Srinivas [43] discussed the need of MANETs to be lightweight in a reliable environment due to the resource limitations of the nodes. The data traffic may be influenced by the attacks (inside or outside the network) and may result in denial of services. The author studied several security protocols in MANET and discussed the techniques to alleviate attacks. Jing Xu et al. [35] proposed the maximum likelihood-based estimation method to find the position of sensor nodes during mobility scenarios. The calculation was achieved through Received Signal Strength Indicator (RSSI) period. Quan et al. [36] presented a Neighbor Aided Compressive Sensing (NACS) scheme for collecting data in several mode of sensor network. In the monitoring phase, random readings
were taken. Simulation outcomes reveal that the NACS model can attain finer recovery results and receptions with fewer transmissions.

Chen et al. [4] developed a Congestion Aware Routing Protocol (CARM) for mobile ad hoc networks which introduced Weighted Channel Delay (WCD) to compute the link cost by utilizing transmission delay, queuing delay in order to pick out the path. CARM improves channel usage. Sharma et al. [6] suggested an adaptive congestive protocol based on the Ad-hoc On-Demand Distance Vector Routing (AODV) protocol. In this approach, each node sends information to its previous node about the occurrence of congestion according to the packets queued to the node in relation to the buffer size. An alternative route is discovered and used in case of congestion on a particular node. Hashim et al. [7] proposed the Congestion Aware Multipath Dynamic Source Routing (CAWMP-DSR) protocol. In this approach, several disjointed paths were created and the correlation factor between the paths is attained. The issue of end-to-end delay and overheads is improvised using the correlation factor metric.

Soundararajan and Bhuvaneswaran [8] suggested a novel Multipath-Load-Balancing and Rate-Based-Congestion-Control (MLBRBCC) algorithm. In this the percentage of channel use and traffic load are calculated at every intermediary node. Depending on this congestion status and rate control is computed and communicated to the sender in order to lessen end to end delay and enhance packet delivery ratio. Seth et al. [9], the authors presented a new load distribution model, Effective-delay-controlled-load-distribution model using available local information, thus minimizing the variation between end-to-end delays. Without any additional network resources, packet control time is minimized. Prabhavat et al. [10] author presented Load Balanced Congestion Adaptive (LBACA) routing mechanism. In this technique congestion status of the path is computed based on the traffic density of neighboring nodes. The load is scattered uniformly based on the traffic density.

Tabrizchi [38] stated that Cloud computing demand has increased tremendously. However, the allied security and privacy challenges need to be addressed. The author presented several security issues, threats, requirements, and vulnerabilities with their solutions. The issues faced by cloud entities like service provider, data owner and client were discussed. Ghafir [39] mentioned the usage of technology deployed in critical infrastructure which is used in our daily life. The effect of globalization and further challenges raised by it were discussed. The paper discussed threat of social engineering mainly the attacks caused by it. The prevailing safety awareness programs were discussed. The role of critical elements of infrastructure and the threat caused by operators was mentioned. The design and implementation of the projected security awareness training program was discussed. The software testing and evaluation of the methodology used to train operators of critical infrastructure was explained. Tan [40] mentioned that cloud computing paradigm is mainly used for single type of application which requires individual quality of service. For more than one application to operate smoothly, resource multiplexing is mandatory for heterogeneous workloads to guarantee proper resource utilization. The idle
resource segments reserved by workloads are given to other workloads. Resource preemption and resource stealing methods are used. An adaptive combined resource provisioning technique was presented which merged resource multiplexing and elastic resource provisioning schemes to attain better experimental results.

Jeong [41] proposed a blockchain-based cloud consumer information supervision system using stochastic weights to corroborate that the data of clients getting cloud services has not altered. The planned scheme used color key scheme for user attribute information to effectively process user information in different cloud milieus. Concept of authentication keys for real time cloud services was used. The given scheme was said to reduce the time of blockchain generation on average by linking user information to the probability value of user information. Efficiency in managing blockchain-based user information over overlay networks was improved with minimum overhead. Chen [42] proposed a secure three-factor-based authentication with key agreement protocol. The analysis done showed that proposed protocol managed to overcome denial of service attack and replay attack. The security of the protocol was evaluated using Burrows-Abadi-Needham (BAN) logic and was said to attain better security and performance for e-Health clouds [43-45].

3 The Proposed Adaptive Traffic Routing Technology

The IoT-MANET frame is an incorporated routing model. The working of MANET depends on the agility of its nodes and links, and resources [4]. In the cloud, cloud providers maintain facilities that support agility, proficiency, and scalability [1]. In the Cloud-MANET, all MANET smart devices need to be saved independently into the cloud. The projected model will be deployed offline. When MANET is enabled, cloud services execute in real time and offer services to MANET smart devices [35]. Smart devices send an appeal to log into the cloud. The cloud offers the best connectivity to the smart device.

3.1 Overview

The sender sends the packets to the receiver using intermediary relay nodes. On receiving the packet, intermediary node remaining energy status, queue length, and congestion status are computed of each node. The remaining energy according to the present traffic load on the individual node is calculated. The current energy and congestion information is disseminating in the network. The sender controls data packet flow to avoid congestion.

3.2 Congestion Level Detection and Control Mechanism

The proposed approach considers the congestion aware data delivery scheme and remaining energy available so that the neighboring nodes in the network
recognize the congestion level and lifetime of a node. At an intermediary node the congestion level and remaining energy is computed and that information is sent to the originating node so that based on the calculated information appropriate action can be taken.

3.2.1 Congestion Level Detection

The congestion level detection technique uses queue occupancy to detect the congestion status of a node. \( Q_{\text{min}} \) and \( Q_{\text{max}} \) represent the minimum and maximum queue length of a node respectively. \( \alpha \) and \( \beta \) are the control variables and their values range between 0 and 1.

\[
Q_{\text{min}} = \alpha \times Q_{\text{size}} \tag{1}
\]

\[
Q_{\text{max}} = \beta \times Q_{\text{size}} \tag{2}
\]

In case if the queue-length of a node is lesser than \( Q_{\text{min}} \) then the node is lightly loaded and if queue-length is more than \( Q_{\text{max}} \), then the node is heavily load or overcrowded. Its queue length is in between \( Q_{\text{min}} \) and \( Q_{\text{max}} \) then the node is in safe position. Average queue length of each node can be calculated with exponentially weighted moving average after some interval as follows:

\[
Q_{\text{avg}} = (1 - \gamma) \times Q_{\text{avg}} + Q_{\text{current}} \times \gamma \tag{3}
\]

where \( \gamma \) is the weight factor and \( Q_{\text{current}} \) is current queue length at a particular node. If \( Q_{\text{avg}} \) is greater than \( Q_{\text{threshold}} \) then node is congested and alert message is sent to the source node so that alternative route can be chosen. The congestion level can be detected by using Algorithm 2.

**Algorithm 2.** Congestion Level Detection.

Congestion Level Detection Method \((Q_{\text{min}}, Q_{\text{max}}, Q_{\text{avg}}, Q_{\text{threshold}}, Q_{\text{Length}})\).

**BEGIN**

If \((Q_{\text{avg}} < Q_{\text{min}})\)
- No congestion and normal operation continued;
If \((Q_{\text{avg}} \geq Q_{\text{min}} \text{ and } Q_{\text{avg}} \leq Q_{\text{threshold}})\)
- Node is moderately loaded;
If \((Q_{\text{avg}} \geq Q_{\text{threshold}} \text{ and } Q_{\text{avg}} \leq Q_{\text{max}})\)
- Node is heavily loaded and alert message sent to the sender;
If \((Q_{\text{avg}} > Q_{\text{max}})\)
- Node is congested and cannot further relay the data packets, select alternative path;

**END**

3.2.2 Remaining Energy Calculation

Lifetime of a node [13] is evaluated as per the given equation:

\[
N_{\text{LT}} = \frac{\text{Battery capacity of anode}}{\text{Drain Rate}} \tag{4}
\]
Drain rate [13] can be calculated as the rate of energy consumption as

\[ DR = \sum e_{ij}^t \sum q_{ij} + \sum e_{ji}^r \sum q_{ji} \]  

(5)

in which, \( e_{ij}^t \) is the transmission energy mandatory for transmission of a packet from node \( i \) to node \( j \), \( e_{ji}^r \) is the reception energy essential to receive a packet from node \( i \) to node \( j \) and \( q_{ji} \) is the rate of flow of data.

Remaining Energy (RE) can be calculated as:

\[ RE = E_{initial} - E_{consumed} \]  

(6)

where \( E_{initial} \) is the initial energy available and \( E_{consumed} \) is energy consumed in transmission and reception of packets. If \( RE < \text{threshold energy} \), then node is selected in the routing process. Based on available remaining energy the node’s lifetime can be calculated. An algorithm for load distribution using different path selected based on residual energy is given in Algorithm 3.

Algorithm 3: Load Distribution using Alternative Path Selection based on Residual Energy, RE.

\begin{algorithm}
BEGIN
Call Algorithm 1 for congestion detection;
If (congestion is found) then
Send message to the source node;
Compute remaining energy of the nodes;
If (\( RE > \text{threshold energy} \)) then
Node selected as relay node for load distribution;
Endif
Based on the remaining energy alternative path will be selected.
END
\end{algorithm}

A flowchart for the proposed load balancing algorithm is shown in Fig. 5. Depending on the comparison between the queue length generated and the energy level, the operation is performed. In case of a match, a normal operation is performed. Otherwise, an alert message is sent to the sender and other path is being selected.

4 Performance Evaluation

In this part, the suggested algorithm is assessed and compared the consequences with the Load Balanced Congestion Adaptive Routing (LBCAR) [14], and Multipath Load Balancing technique for Congestion Control (MLBCC) [15] proficiencies. In this part, the proposed algorithm is evaluated and the results are contrast to the LBCAR [14] and MLBCC [15] techniques. The simulations were executed with the Matlab software. Simulation metrics are presented in Table 1. The parameters included number of nodes, mobility model,
transmission range, packet dimension, simulation time, and network area and traffic type.

Table 1 Parameter settings for simulations

| Parameters          | Values                        |
|---------------------|-------------------------------|
| Number of Nodes     | 100                           |
| Mobility model      | Arbitrary waypoint model      |
| Transmission range  | 150m                          |
| Packet dimension    | 512 bytes                     |
| Simulation time     | 500 sec                       |
| Network Area        | 1500m x 1500m                 |
| Traffic Type        | Constant Bit Rate             |

The metrics for analyzing and evaluating the performance of the projected and prevailing load balancing procedures are:

- **Packet Delivery Report**: The packet delivery report (PDR) indicates the quality of the selected pathway for data transmission. It may be computed using the following equation:

  \[
  \text{Packet Delivery Ratio} = \frac{\text{Packet Received}}{\text{Packets Sent}} \times 100
  \]  

- **Average End-to-End Time**: It is defined as the average time a data packet takes to get from the source to the destination. A greater delay indicates
that the access path has become congested. This can be calculated by:

\[
\text{Average end-to-end delay} = \sum \frac{\text{Time of packet reception - Time of packet sent}}{\text{Total packets}}
\]

(8)

- **Throughput**: This is termed as the ratio of the number of data packets successfully received during transmission on the total amount of packets sent. This can be calculated by:

\[
\text{Throughput} = \frac{\text{Number of packet received}}{\text{Delay}}
\]

(9)

The simulation results were presented in Figures 6 to 8 for a package delivery report, end-to-end delay and flow. The PDR should be high to have an effective transmission. In Fig. 6, the PDR is indicated according to the different data rate. As data transmission rates rise, packet delivery rates begin to decline due to network congestion. In this scenario, the proposed method has a greater packet delivery ratio than the MLBCC and LBCAR algorithms. In Fig. 7, end-to-end time in relation to the different nodes in the system is illustrated. As network nodes increase, end-to-end delay also increases due to limited linkage capacity and bandwidth availability. Link breakages occur due to increase the number of customers and traffic load causes to discover fresh routes, swap control messages to set new path, thereby increasing the terminal to end delay.

![Fig. 6 Packet delivery ratio versus data rate](image)

The throughput performance comparison of different algorithms has been shown in Fig. 8. The throughput escalates with the rise of traffic data load; however, it starts declining at 300 where the network load is congested and saturation condition reaches. So, further traffic load will result in performance deterioration and makes the network congested. It is shown in Fig. 8 that the proposed algorithm yield to high performance in comparison with the other techniques as we have considered residual energy along with the congestion control scheme which leads to stable paths for data transmission.
5 Conclusion

To efficiently balance the extra load in MANET’s a multiple path congestion control algorithm has been suggested in this report. This research strengthens the part of a Cloud-MANET system for communicating between the Internet and smart devices. The research has led to the development of a novel IoT framework. In this algorithm multiple routes have been identified and congestion status of each node using congestion detection algorithm has been computed. Depending on the state of congestion and the residual energy of the node, the stable path will be selected, thus improving the lifespan of the network. The traffic flow is distributed on alternative paths and thus improved the network performance. The proposed techniques can be adopted in multiple path on routing protocols. The simulation results show that the proposed scheme outperformed the existing MLBCC and LBCAR algorithms in terms of achieved throughput, end-to-end delay, and packet delivery ratio. It efficiently balances the network traffic load and increases the service life of the network.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.
Conflict of interest

The authors declare that they have no conflict of interest.

Author contributions

All the authors have substantial contributions to the conception and design of the work.

References

1. A.D. Tran and H. Raghavendra, “Congestion adaptive routing in mobile ad hoc networks,” IEEE Transactions on Parallel and Distributed Systems, 17(11), pp. 1294-1304, 2006.
2. S.J. Lee and M. Gerla, “Dynamic load-aware routing in ad hoc networks,” in Proceedings of IEEE International Conference on Communications, pp. 3206-3210, June 2001.
3. Y. Lu, W. Wang, Y. Zhong, and B. Bhargava, “Study of distance vector routing protocols for mobile ad hoc networks,” in Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 187-194, Mar. 2003.
4. X. Chen, H.M. Jones, and A.D.S. Jayalath, “Congestion-aware routing protocol for mobile ad hoc networks,” in Proceedings of IEEE Conference of Vehicular Technology, pp. 21-25, 2007.
5. W. Wu, Z. Zhang, X. Sha, X., and C. He, “Auto rate MAC protocol based on congestion detection for wireless ad hoc networks,” Information Technology Journal, 8(8), pp. 1205-1212, 2009.
6. S. Sharma, R.C. Jain, and S.S. Bhadauria, “Simulation study of congestion adaptive routing algorithm for mobile ad hoc network,” Trends in Applied Sciences Research, vol. 1, pp. 368-378, 2006.
7. R. Hashim, Q. Nasir, and S. Harous, “Congestion aware multipath dynamic source routing protocol (CAWMP-DSR) for mobile ad-hoc network,” in Proceedings of the 5th International Conference on Advances in Mobile Computing and Multimedia (MoMM ’07), Jakarta, Indonesia, December 2007.
8. S. Soundararajan and R.S. Bhuvaneswaran, “Multipath load balancing & rate based congestion control for mobile ad hoc networks (MANET),” in Proceedings of 2012 Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Bangkok, Thailand, May 2012.
9. B. Seth, S. Dalal, V. Jaglan, D.N. Le, S. Mohan and G. Srivastava, “Integrating encryption techniques for secure data storage in the cloud,” Transactions on Emerging Telecommunications Technologies, e4108, 2020.
10. S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, “Effective delay-controlled load distribution over multipath networks,” IEEE Transactions on Parallel and Distributed Systems, 22(10), pp. 1730-1741, 2011.
11. L. Shrivastava, S.S. Bhadoria, and G.S. Tomar, “A load balancing approach for congestion adaptively in MANET,” in Proceedings of the International Conference on Computational Intelligence and Communication Networks (CICN’11), pp. 32-36, October 2011.
12. T.G. Basavaraju, S.K. Sarkar, C. Puttalamadappa, and M.A. Gautham, “ECARP: an efficient congestion adaptive routing protocol for mobile Ad hoc networks,” in Proceedings of the 6th International Conference on ITS Telecommunications Proceedings (ITST ’06), pp. 715-718, Chengdu, China, June 2006.
13. M.S. Ali, B.G.Ashahraibi and A.Vallavaraj, “Congestion adaptive multipath routing for load balancing in mobile ad hoc networks,” in Proceedings of IEEE International Conference on Innovations in Information Technology (IIT), pp. 305-309, 2012.
14. D.A. Tran and H. Raghavendra, “Congestion adaptive routing in mobile ad hoc networks,” IEEE Transactions on Parallel and Distributed Systems, 17(11), pp. 1294-1305, 2006.
15. J.Y. Kim, G.S. Tomar, L. Shrivastava, S. Bhadaura, and W.H. Lee, “Load balanced congestion adaptive routing for mobile ad hoc networks,” International Journal of Distributed Sensor Networks, 10(7), pp. 1-10, 2014.
16. C.E. Perkins and P. Bhagwat, “Routing over multi-hop wireless network of mobile computers,” In: Imielinski T., Korth H.F. (eds) Mobile Computing, The Kluwer International Series in Engineering and Computer Science, vol. 353, pp. 183-205, Springer, Boston, MA, 1994.
17. S.V. Mallapur, S.R. Patil, J.V. Agarkhed, “Load balancing technique for congestion control multipath routing protocol in MANETs,” Wireless Personal Communications, 92(2), pp. 749-770, 2016.
18. D. N. Le, B. Seth and S. Dalal, “A hybrid approach of secret sharing with fragmentation and encryption in cloud environment for securing outsourced medical database: a revolutionary approach,” Journal of Cyber Security and Mobility, 7(4), pp. 379-408, 2018.
19. V.K. Sharma, M. Kumar, “Adaptive energy efficient load distribution using fuzzy approach,” Ad Hoc & Sensor Wireless Networks, 39, pp. 123-166, 2017.
20. L. Chen and W. B. Heimzelman, “Qos-aware routing based on bandwidth estimation for mobile ad hoc networks,” IEEE Journal on Selected Areas in Communications, 23(3), pp. 561-572, 2005.
21. C.K. Toh, A.N. Le, and Y.Z. Cho, “Load balanced routing protocols for ad hoc mobile wireless networks,” IEEE Communications Magazine, 47(8), pp. 78-84, 2009.
22. H. Riasudheen, K. Selvamani, Saswati Mukherjee, I.R. Divyasree, “An efficient energy-aware routing scheme for cloud-assisted MANETs in 5G,” Ad Hoc Networks, 97, 102021, 2020.
23. P. Sathyaraj, D. Rukmani Devi, “Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method,” Journal of Ambient Intelligence and Humanized Computing, 2020. https://doi.org/10.1007/s12652-020-02358-4
24. A. Vyas, S. Ahimman, “Implementing security features in MANET routing protocols,” International Journal of Computer Network and Information Security, 10(8), pp. 51-57, 2018.
25. R. Singh, P. Singh, M. Duhan, “An effective implementation of security based algorithmic approach in mobile adhoc networks,” Human-Centric Computing, 4, article no. 7, 2014.
26. W.C. Chen, H.T. Liaw, “A study of high secure and efficient MANET routing scheme,” Journal of Sensors, 2015, article no. 365863, 2015.
27. R. Dilli, P.C.S. Reddy, “Implementation of security features in MANETs using SHA-3 standard algorithm,” 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), pp. 455-458, 2016.
28. R.K. Singh, P. Nand, “Literature review of routing attacks in MANET,” 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 525-530, 2016.
29. D. Zhang, T. Zhang, X. Liu, “Novel self-adaptive routing service algorithm for application in VANET,” Applied Intelligence, 49, pp. 1866-1879, 2019.
30. T. Alam, “Middleware implementation in Cloud-MANET mobility model for internet of smart devices,” International Journal of Computer Science and Network Security, 17(5), pp. 86-94, 2017.
31. A. Sharma, A. Bansal, V. Rishiwal, “SBADR: Stable and bandwidth aware dynamic routing protocol for mobile ad hoc networks,” International Journal of Pervasive Computing and Communications, 16(3), pp. 205-221, 2020.
32. D. Kanellopoulos, V. K. Sharma, “Survey on power-aware optimization solutions for MANETs,” Electronics, 9, article no. 1129, 2020.
33. D. N. Kanellopoulos, “Recent progress on QoS scheduling for mobile ad hoc networks,” Journal of Organizational and End User Computing, 31(3), pp. 37-66, 2019.
34. K. VinothKumar, T. Jayasankar, V. Eswaramoorthy, V. Niveditha, “SDARP: Security based data aware routing protocol for ad hoc sensor networks,” International Journal of Intelligent Networks, 1, pp. 36-42, 2020.
35. J. Xu, J. He, Y. Zhang, F. Xu, F. Cai, “An L2-distance-based maximum likelihood estimation method for sensor localization in wireless sensor networks,” International Journal of Distributed Sensor Networks, pp.1-8, 2016.

36. L. Quan, S. Xiao, X. Xue, C. Lu, “Neighbor-aided spatial-temporal compressive data gathering in wireless sensor networks,” IEEE Communications Letters, 20(3), pp. 578-581, 2016.

37. S. Kalime, Dr. K. Sagar, “A review: Secure routing protocols for mobile adhoc networks (MANETs),” Journal of Critical Reviews, 7(19), pp. 8385-8393, 2020.

38. Tabrizchi, H., Kuchaki Rafsanjani, M., “A survey on security challenges in cloud computing: issues, threats, and solutions,” J Supercomput, 76, 9493-9512, https://doi.org/10.1007/s11227-020-03213-1, 2020.

39. Ghafir, I., Jibran, S., Mohammad, H., Hanan, F., Vaclav, P., Sardar, J., Sohail, J., Thar, B., “Security threats to critical infrastructure: the human factor”, J Supercomput, 74(10), pp. 4986-5002, 2018.

40. Tan, Y., Wu, F., Wu, Q., Liao, X., JTJOS, “Resource stealing: a resource multiplexing method for mix workloads in cloud system”, J Supercomput, 75(1), pp.33-49, 2019.

41. Jeong, Y.S., Ahn, B.T. An efficient management scheme of blockchain-based cloud user information using probabilistic weighting. J Supercomput, 77, pp. 3339-3358, https://doi.org/10.1007/s11227-020-03396-7, 2021.

42. Chen, Y., Chen, J. A secure three-factor-based authentication with key agreement protocol for e-Health clouds. J Supercomput, 77, pp. 3359-3380, https://doi.org/10.1007/s11227-020-03395-8, 2021.

43. Kalime, Srinivas & Sagar, K., “A review: secure routing protocols for mobile adhoc networks (MANETs)”, Journal of Critical Reviews, 7, pp. 8385-8393, 2021.

44. Le, D. N., Bhatt, C. M., & Madhukar, M. (Eds.). (2019). Security Designs for the Cloud, IoT, and Social Networking. John Wiley & Sons, Incorporated.

45. Khalaf, O. I., Ajesh, F., Hanaid, A. A., Nguyen, G. N., & Le, D. N. (2020). Efficient Dual-Cooperative Bait Detection Scheme for Collaborative Attackers on Mobile Ad-hoc Networks. IEEE Access.