ISSN: 2278-4632
Vol-11 Issue-01 2021

PERFORMANCE OF NEIGHBOR TRUST TRANSMISSION ROUTING PROTOCOL WITH HASH-BASED DATA ENCRYPTION STANDARD ALGORITHM FOR SECURE COMMUNICATION IN MANET

G.BALAMURUGAN

Full-Time Research Scholar, PG and Research Department of Computer Science Bharathiar University Arts and Science College, Modakkurichi, Erode District, Tamilnadu

Dr.P.VIJAYAKUMAR M.Sc., M.Phil., Ph.D

Assistant Professor and Head, PG and Research Department of Computer Science Bharathiar University Arts and Science College, Modakkurichi, Erode Dt Tamilnadu

Abstract

A Mobile Ad-hoc Network (MANET) is an autonomous group of mobile nodes that can continue the communication while moving from any fixed location with no permanent infrastructure to another location. Routing protocol security plays an important role in the MANET. Secure routing and data transmission have been the important factors in MANET because it is more vulnerable due to its structural characteristics. The existing algorithm Dynamic Cloudlet-assisted Routing Mechanism (DCRM) algorithm has data transfer is less security process, routing is still vulnerable and the probability of malicious nodes and traffic occurrence is very high. To resolve this problem, the proposed Neighbor Trust Transmission Routing Protocol (NTTRP) is used to avoid traffic and malicious nodes for secure routing from source to destination. During the routing phase, NTTRP can detect direct and indirect attacks, analyse the node traffic, and select the neighbour node, perform malicious node detection. There are two cases in the proposed NTTRP algorithm namely the effectiveness of both traffic and malicious node detection in MANET. The source node sends the data to destination when traffic or attack occurs. The proposed algorithm selects and alters net neighbour node or another path to reduce traffic, avoid malicious nodes. The Hash-based Data Encryption Standard (HDES) algorithm encrypts the data by generating a private key from source to destination for secure communication to the destination node using the private key for decrypting the data. Simulation results confirm that the proposed method NTTRPand HDES algorithm shows good performance with regard to security constraints compliance. Compared to existing algorithms, source node to destination node communication is better with the proposed method.

Keywords:MANET, Neighbour Trust Transmission Routing Protocol (NTTRP) algorithm, Avoid traffic and attack, Hash-based Data Encryption Standard (HDES), Encryption, data transfer, malicious node.

ISSN: 2278-4632
Vol-11 Issue-01 2021

1. Introduction

The MANET is a set of successively smaller infrastructure and mobile devices network that configures itself without any centralized control. In these networks, each node cooperates with other nodes and can serve as a host or router. As the MANET's main target is to route, the distributed nodes can send quick and accurate data to secure routing devices to establish the correct and valid path. Intruder and passive attacks try to eavesdrop on communications, make various changes in an active network and over a MANET, damage data and networks commonly. In a typical case, the data transfer coordinates violate the network through a direct or indirect attack to a source node to destination node to deceive the route. In a direct attack, the attacker can tamper with the discarded data packet, making a network paralysed with a black hole of attacks and a wormhole attack. Concerning the indirect attack, the attacker is to give effect for intentional data transfer, without disrupting the network debugging system, to change its log. For example, to detect a network failure, peer review and network auditing are dependent on the log nodes. These offend the ability to detect such malicious parties and attacking node by node. The various network management tasks need to identify misbehaving nodes to perform accountability network by implementing the trust management policies distributed system.

It was found that the abnormal node was attacked directly or indirectly to explain that this attack was caused by the network. An automated warranty system that monitors and monitors the failure of a MANET to detect the cause of a failed mobile ad, in order not to disclose the privacy of the terminal. In these methods, the node that detects it is affected by anyone who first tested it. Based on the origin of the phenomena observed by this method of causation, the chains of these events find a set of phenomena called phenomena. If it receives an error on the request log entry's target node, it is possible to trace the request log back to the previous-hop node. It can also find the records or other false of the log. The MANET of abnormal events such as lack of log entries on the particular node, the destination node is possible to perform the generation of the error log entries. A valid starting point is not tracked in the background; however, none of these methods report the lack of good events.

2. Related work

Anonymous communication is important because of the hostile environment to deploy several MANET applications. The network's primary requirement is to provide a non-specific and non-linkable functionality for the mobile node and the traffic [1]. Although a secure routing protocol in many anonymities have been proposed, the requirements cannot be completely satisfied. Existing

ISSN: 2278-4632
Vol-11 Issue-01 2021

protocols rejected routing packets or service broadcasting false that is protected by a pseudonym, and the node is vulnerable to attack from even identity. The existing routing protocol, to Authenticated Anonymous Secure Routing (AASR), and resistance to attack [2].

Mobility of nodes and resource constraints are the important factors affecting the performance of MANET. As it is very difficult to design services, mobile nodes will affect the stability of the link. A crowded node's resource constraints occur through the Quality of Service (QoS) in MANET routing protocol. Particularly in moving a fast node, the frequent link interruptions would adversely affect the QoS performance. Therefore, to support QoS, a MANET routing protocol must be designed to adapt network topology changes [3].

MANET network infrastructure has independent access to the centre of the model. MANET is a wide, fast and flexible network model which is used under certain circumstances. However, the topology and the potential security have led to rapid and open channel changes [4]. Active routing Authentication Scheme (AAS) is used to characterize the active substance-based routing protocol. It systematically selects the route of transfer attacks and fraud attacks, which have proven effective. So with regard to the Byzantine attack and the MANET mixing of malicious nodes to Burrows–Abadi–Needham (BAN) are the rule set.

The fixed opportunistic data transfer have been made on behalf of the wireless network and has attracted wide attention in the research community of the multi-hop wireless network [5].

First, there are a wide range of opportunities for data transfer. The reason it is not used on MANET is the lack of effective active routing methods. It has the rooting properties of the Lightweight Active Source Source Routing (PSR) protocol with powerful source. First, there are a wide range of opportunities for data transfer. The reason it is not used on MANET is the lack of effective active routing methods. It has the rooting properties of the Proactive Source Routing (PSR) protocol with powerful source.

Ad hoc on-Demand Distance Vector (AODV) is the routing protocol that is widely used in MANET, called Secure AODV routing protocol for solving the defects and the original problem of the related security vulnerabilities AODV protocol detects the block hole attacks and the repair of the black hole attacks. Specifically, the AODV protocol can prevent malicious nodes from running black hole attacks during the routing process [6]. However, two nodes cannot endure together in the coordinated black hole attacks. Therefore, it overrides the security vulnerabilities of the security AODV protocol related to the original AODV protocol in secure MANET routing protocol, and it contains AODV current methods.

ISSN: 2278-4632
Vol-11 Issue-01 2021

Rapid energy depletion (due to the mobile node) and the interruption of frequent links (to cause limited battery capacity) are the two major problems affecting the MANET's flexibility. MANET's cooperative communication has become an attractive process because it can improve system capacity and energy efficiency. Despite at cooperative communication, coordination routing system design solution has (path detection, route response, path extensions including cooperative data transmission), the cooperative communication flow resistance and routing (energy consumption, energy collection capacity, link interruption possibility) [7].

To achieve a fixed function, it has its dependence on collaboration between participants in the MANET [8]. However, these are vulnerable to denial of malicious attacks and cooperation; therefore, users can ensure that the urgently required security problems have been resolved. In the past few years, many trusts have proposed that the design of reliable quantitative methods is the key to these measures. In the present method, reliability evaluation is divided into reliable prediction abstract and new lightweight subjective trust inference framework. Node reliability evaluation of the process is based on the historical behaviour of the node [9].

Distributed Hash Table (DHT) is arbitrary; it came out of a useful auxiliary design and self-organizing network specification. In existing methods, by designing an expandable routing protocol used in MANET, it will be realized by multiplying its advantages at the network layer. There is a need to consider two related issues: DHT-based routing protocols; if it is decided that they must be designed, problems and logical network discrepancies reduce the efficiency and flexibility of the DHT-based routing protocols [10]. To solve these problems, the DHT base account takes the nodes' physical internal Neighbor relationships and uses the logical space of three dimensions using a three-dimensional structure to explain the relation of the proposed routing protocol.

In some special cases, if the communication infrastructure is damaged, it will not exist. Mobile Smart Service (MSS) can be used for communication between people to build a MANET [11]. MSS helps to ensure quality, improve the QoS and Quality of Experience (QoE), and focuses on data transmission in the user's MANET. However, for the well-known problem of frequent disconnection or high transmission failure rate in the MANET. Content-Centric Mobile Ad-hoc Network (CCMAN) is a potential ancillary spread of multimedia content in the wireless network's future. The network cache reduces significant network traffic load which is one of the key technologies in CCMAN that can improve content search performance [12]. However, the challenge is in the CCMAN cache. All the Wireless nodes act as a router by limiting the cache size and the user

ISSN: 2278-4632
Vol-11 Issue-01 2021

can cache each wireless node's function. The caching strategy must improve the space efficiency performance and the cache of the CCMAN of Cache Space Efficient Caching (CSEC).

Network coding has been used for efficient broadcasting in wireless multi-hop networks to pass successfully. Two coding methods are suitable for mobile networks, Random Linear Network Coding (RLNC) and XOR-based coding. MANET has become a focus on the multi-broadcasting problem. Compared with the observation of packet loss based on the coding XOR, RLNC has made greater flexibility. It has developed an analytical model to prove our intuition. However, the model also has RLNC to bind to the probability that the approach is taken in the literature.

MANET is a mobile device, and re-establishing the re-routed cloud service lost the communication link between the clouds. It will consume more energy, and leave the MANET coverage. The 5G mobile communication technology for fog calculation is defined as a distributed processing architecture for billion computing devices connected to the internet [13]. In MANET, for fog and 5G computing, new and effective combinations of Dynamic Cloudlet-Assist Routing Mechanism (DCRM) have been existing to solve link failure's energy-saving problem.

In recent years, MANET technology's rapid development has been attributed to its low cost, simplicity, versatility for mobile devices. In Short natural disasters, this kind of communication network infrastructure provides a reliable network, thus, it can be used as a post-repair information system [14]. In this way, nodes in the network without centralized control at any time can move freely and do routing which is thought to be the most difficult problem. Some routing algorithms are reactivated based on the probability of coverage of such proximity, depending on the variables that must be set by the system administrator [15].

3. Proposed Methodology

MANET is the most important self-organization and multi-hop network of the infrastructure. The proposed Neighbour Trust Transmission Routing Protocol (NTTRP) algorithm is integrated with secure mechanism to deploy the difficulty of wireless ad hoc network routing protocols. Among the key challenges, providing secure routing communication (reliability) for network users is the key challenge.

ISSN: 2278-4632
Vol-11 Issue-01 2021

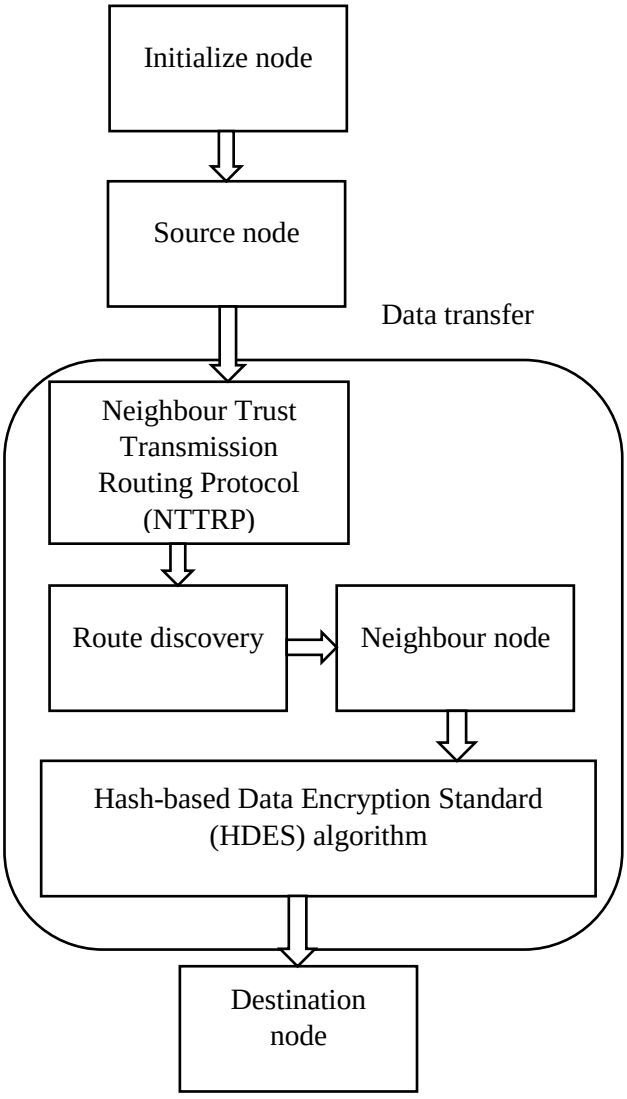

Figure 1: Proposed diagram

Figure 1 describes the process between source node and destination node during the data transfer in case of traffic or attack. The proposed algorithm selects neighbour node and another path to reduce traffic and avoid malicious nodes. The Hash-based Data Encryption Standard (HDES)

ISSN: 2278-4632
Vol-11 Issue-01 2021

algorithm used to encrypt the data source node generates the private key to the destination node for secure communication.

3.1 Identify the attack or traffic using Neighbour Trust Transmission Routing Protocol (NTTRP)

Data traffic attacks occur during the transfer of packets via their drop or delayed data packets of the node. The attack node will send all the data packets received in the buffer and maintain some random delay in the order of the received data packet. The proposed NTTRP routing is a way to exchange data from a node to another network node. Via multiple hops, due to the short distance ordinary node for routing, a communication data transceiver in the MANET is achieved. The data packet routing table stores the network protocols for each node which communicates with the NTTRP information transmitted between them. The proposed NTTRP algorithm is used for secured communication between source and destination node to avoid traffic and attack. Constant Bit Rate (CBR) is the transmission rate of the service CBR communication which has constant transmission speed and consumption of real-time traffic specified by the peak cell rate parameter. The proposed NTTRP algorithm selects the forward Neighbour node while traffic or malicious node occurs.

Algorithm Steps

Input: Source node S_n, Destination node D_n

Output: Route from S_n to D_n

Begin

Step 1: Initialize the number of nodes

Step 2: Identify $S_n$and $D_n$nodes id

Step 3: S_n data transfer

S_n-->PREQ

Step 4: For each (neighbour node n_n)

Step 5: Next hop<--n_n

Step 6: min route cost <--n_n

Step 7: End for each

Step 8: Transfer the data packets to next hop

ISSN: 2278-4632
Vol-11 Issue-01 2021

Stop

The above algorithm provides a source node to start the data transfer to the destination node to find the malicious attack using the proposed NTTRP by redirecting the path. Routing protocol is to collect specific information about the network and the router from the surrounding environment. This information is stored in the routing table of the router memory. The routing information in this table identifies the network from another computing which is the best path to run. Let us assume NN is the Neighbor node, the Source nodeS_n, the Destination node D_n

3.2 Route Discovery

Routing protocols has the responsibility of establishing and maintaining the paths between the source and destination. The two main categories of ad hoc routing protocol are phenotype and on-demand protocol. In the table-based protocol, each node maintains a routing table containing routes to all network nodes. To maintain the routing table to the packet, the transmission node must occur regularly with the route information. Route finding maintains a plurality of paths between the networks connected to the source and destination nodes. The proposed Neighbour Trust Transmission Routing Protocol (NTTRP) is used to retransmit the packet and select the forward Neighbour node when traffic or malicious node occurs.

Algorithm Steps

Step1: To initialize the nodes as v, distance as d

Step2: Initialize the node distance

Node distance [0]=0

$Initialize\ redundancy\ =\ 0;$

$Link\ v\ =\ 0;$

$for(int\ k\ =\ 0;\ k\ <\ n\ -\ 1;\ k++)\{$

$int\ j\ =\ 0;$

$while(v[j].node\_size()\ !=\ 0)\{$

$if(distance[\ v[j][0]\ ]\ +\ v[j][2]\ <\ dis[\ v[j][1]\ ])\{$

$dis[\ v[j][1]\ ]\ =\ dis[\ v[j][0]\ ]\ +\ v[j][2];$

$redundancy++;$

ISSN: 2278-4632
Vol-11 Issue-01 2021

}

$$k++;$$

}

The above algorithm steps select another path for multipath detection. Let us assume E refers to set of edges and d refers to distance.

3.3 Data encryption Hash-based Data Encryption Standard (HDES) algorithm

Data encryption, whether the data is in the node or in transportation, helps protect MANET data leakage information. The proposed Hash-based Data Encryption Standard (HDES) algorithm is also used to help protect data from malicious activities. Because of these protection, the sender node and receiver node will be able to communicate without fear of data leakage. The proposed algorithm has a private key that requires the source node and destination which have same keys access. The proposed hash based encryption gives input to a variable-length of data transmission of any fixed-size letters and numbers with the help of a mathematical function of the process. To avoid duplication of data, hash based encryption will be used to generate a random string stored in the database. Therefore, the proposed algorithm and the destination node must have the private key which can decrypt the message. It secures data transfer by using the HDES algorithm and encrypts the data generate key from source to the destination.

Step 1: Source node $S_n$sends data packets

Step 2: Generate the private keyP_k

P_k=key send random number of the encryption key

Step 3: For Secure data transfer using HDES algorithm

Step 4: Encrypt the message using $P_k$key

Step 5: Data convert to cipher text

Step 6: Destination nodeD_n receives the data

Step 7: Decrypt the key and message with the same private key P_k

KeyP_k authentication check

Step 8: Data converted as readable information data

ISSN: 2278-4632
Vol-11 Issue-01 2021

The above algorithm steps provide secure data transmission from the source node to the destination node using the HDES algorithm. The proposed HDES algorithm generates the private key for encrypting the data, and the same key is used to decrypt the data for the destination node.

4. Result and discussion

This section shows the simulation results to evaluate the performance comparison of the proposed algorithm Neighbor Trust Transmission Routing Protocol (NTTRP) algorithm, and the existing algorithms like Ad hoc On-demand Distance Vector (AODV) and Dynamic Cloudlet-assisted Routing Mechanism (DCRM) algorithm.

Table 1: Details of Simulation parameters

Parameters	Values
Simulator tool	NS2
Number of nodes	100
Simulation area	300m*300m
Traffic pattern	CBR
Data packet size	512KB

Table 1 defines the details of simulation parameters for implementation through the Network Simulator version 2.

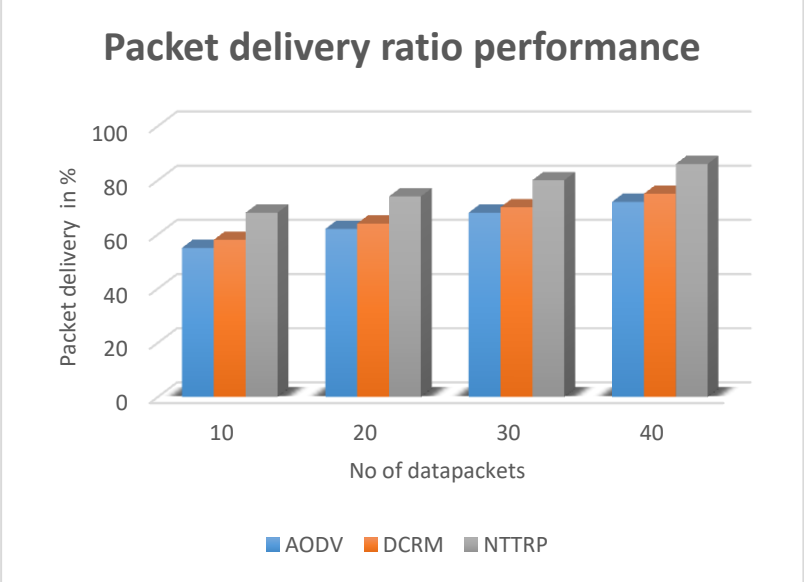

Figure 2: Examination of Packet delivery ratio performance

ISSN: 2278-4632
Vol-11 Issue-01 2021

Figure 2 defines examination of packet delivery ratio performance. The proposed algorithm Neighbor Trust Transmission Routing Protocol (NTTRP) algorithm achieves the performance of 86% against the existing algorithms Ad hoc On-demand Distance Vector (AODV) packet delivery ratio performance of 72% and Dynamic Cloudlet-assisted Routing Mechanism (DCRM) packet delivery ratio performance of 75%.

Table 2: Examination of Packet delivery ratio performance

No of data	AODV (%)	DCRM (%)	NTTRP (%)
10	55	58	68
20	62	64	74
30	68	70	80
40	72	75	86

Table 2 defines the examination of packet delivery ratio performance. The proposed algorithm provides the best results compared to existing methods.

Figure 3: Examination of Throughput performance

Figure 3 defines the examination of throughput performance as the number of data bytes received successfully. The suggested algorithm Neighbor Trust Transmission Routing Protocol (NTTRP) algorithm achieves 86% of result compared to existing algorithms Ad-Hoc On-demand Distance Vector (AODV) throughput performance of 72% and Dynamic Cloudlet-assisted Routing

ISSN: 2278-4632
Vol-11 Issue-01 2021

Mechanism (DCRM) throughput performance of 75%. Finally, throughput performance can be increased using the suggested algorithm Neighbor Trust Transmission Routing Protocol (NTTRP) algorithm in MANET.

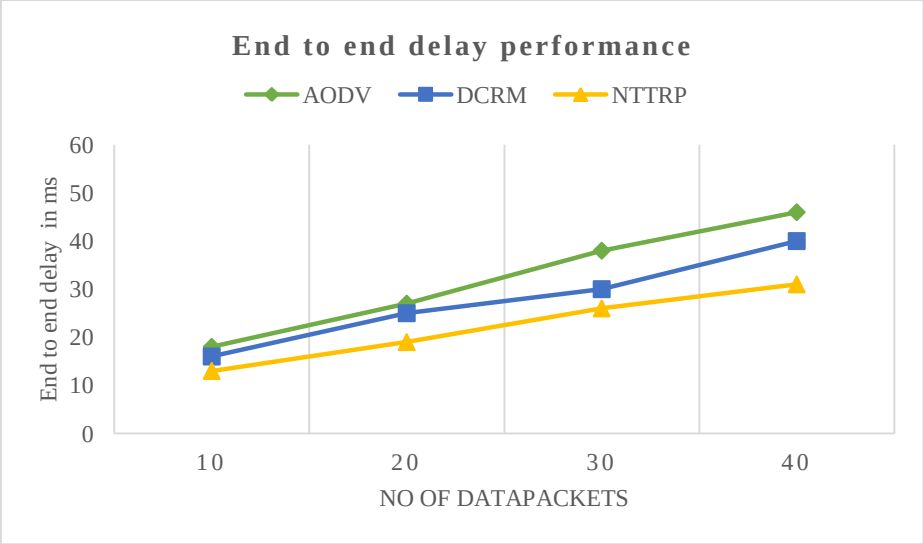

Figure 4: Examination of Delay to delay performance

Figure 4 identifies delay to delay performance to transfer the data packets from a source node to a destination node in time performance. The proposed algorithm Neighbor Trust Transmission Routing Protocol (NTTRP) algorithm reduces mobile delay in MANET and achieves the delayed performance of 31ms. In contrast, the existing algorithms Ad-hoc On-demand Distance Vector (AODV) achieves performance of 46ms. Dynamic Cloudlet-assisted Routing Mechanism (DCRM) achieves performance of 40ms.

5. Conclusion

MANET is used to communicate with each other by quickly configuring a centralized access point or centrally managed multihop network, and communicate with a collection of mobile nodes without any use of infrastructure. In MANET, and several routing protocols have been proposed which provide different performances. Finally, it is concluded that for secure communication in MANET, the proposed Neighbor Trust Transmission Routing Protocol (NTTRP) algorithm has been the best against the existing algorithms AODV and DCRM. HDES algorithm is used to secure data transmission to encrypt the data from source to destination with the same key. The proposed algorithm provides packet delivery ratio of 96%, throughput performance ratio of 92%, and the end to end delay performance of 28ms.

ISSN: 2278-4632
Vol-11 Issue-01 2021

References

1. W. Liu and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," in IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, Nov. 2014, doi: 10.1109/TVT.2014.2313180.
2. Z. Chen, W. Zhou, S. Wu and L. Cheng, "An Adaptive on-Demand Multipath Routing Protocol With QoS Support for High-Speed MANET," IEEE Access, vol. 8, pp. 44760-44773, 2020, doi: 10.1109/ACCESS.2020.2978582.
3. J. Tu, D. Tian and Y. Wang, "An Active-routing Authentication Scheme in MANET," in IEEE Access, doi: 10.1109/ACCESS.2021.3054891.
4. Z. Wang, Y. Chen and C. Li, "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 859-868, Feb. 2014, doi: 10.1109/TVT.2013.2279111.
5. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019, doi: 10.1109/ACCESS.2019.2928804.
6. J. Bai, Y. Sun, C. Phillips and Y. Cao, "Toward Constructive Relay-Based Cooperative Routing in MANETs," in IEEE Systems Journal, vol. 12, no. 2, pp. 1743-1754, June 2018, doi: 10.1109/JSYST.2017.2721543.
7. H. Xia, Z. Li, Y. Zheng, A. Liu, Y. Choi and H. Sekiya, "A Novel Light-Weight Subjective Trust Inference Framework in MANETs," in IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 236-248, 1 April-June 2020, doi: 10.1109/TSUSC.2018.2817219.
8. S. A. Abid, M. Othman, N. Shah, M. Ali and A. R. Khan, "3D-RP: A DHT-Based Routing Protocol for MANETs," in The Computer Journal, vol. 58, no. 2, pp. 258-279, Feb. 2015, doi: 10.1093/comjnl/bxu004.
9. T. Zhang, S. Zhao and B. Cheng, "Multipath Routing and MPTCP-Based Data Delivery Over Manets," in IEEE Access, vol. 8, pp. 32652-32673, 2020, doi: 10.1109/ACCESS.2020.2974191.
10. Dr.G.Kavitha2018,"Qos Improvement Based Security Enhancement For Link Activity Monitoring Service In Mobile Ad Hoc Network," in Cluster Computing-The Journal Of Networks Software Tools And Applications, Springer, Vol. 22, pp: 12863–12869, DOI: 10.1007/s10586-018-1786-y

ISSN: 2278-4632
Vol-11 Issue-01 2021

11. T. Zhang, X. Xu, Le Zhou, X. Jiang and J. Loo, "Cache Space Efficient Caching Scheme for Content-Centric Mobile Ad Hoc Networks," in IEEE Systems Journal, vol. 13, no. 1, pp. 530-541, March 2019, doi: 10.1109/JSYST.2018.2851394.
12. N. Papanikos and E. Papapetrou, "Deterministic Broadcasting and Random Linear Network Coding in Mobile Ad Hoc Networks," in IEEE/ACM Transactions on Networking, vol. 25, no. 3, pp. 1540-1554, June 2017, doi: 10.1109/TNET.2016.2641680.
13. J. Li, X. Li, Y. Gao, Y. Gao and R. Zhang, "Dynamic Cloudlet-Assisted Energy-Saving Routing Mechanism for Mobile Ad Hoc Networks," in IEEE Access, vol. 5, pp. 20908-20920, 2017, doi: 10.1109/ACCESS.2017.2759138.
14. J. A. Ruiz-De-Azúa, A. Camps and A. Calveras Augé, "Benefits of Using Mobile Ad-Hoc Network Protocols in Federated Satellite Systems for Polar Satellite Missions," in IEEE Access, vol. 6, pp. 56356-56367, 2018, doi: 10.1109/ACCESS.2018.2871516.
15. M. E. Ejmaa, S. Subramaniam, Z. A. Zukarnain and Z. M. Hanapi, "Neighbor-Based Dynamic Connectivity Factor Routing Protocol for Mobile Ad Hoc Network," in IEEE Access, vol. 4, pp. 8053-8064, 2016, doi: 10.1109/ACCESS.2016.2623238.