European Journal of Molecular & Clinical Medicine

ISSN 2515-8260 Volume 07, Issue 09, 2020

DISTANCE VECTOR REPORT AUTHENTICATION ADJUSTABLE ROUTING PROTOCOL USING SECURE VERIFICATION-BASED DYNAMIC NODE SELECTION IN MOBILE AD-HOC NETWORK

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

Mobile Ad Hoc Network (MANET) is a wireless network without an access point or node physical infrastructure cooperation. Protection of data communication is because the nature of MANET is a major challenge.A particularly challenging problem is how to detect and maintain viable routing protocol possible attacks. In the mobile ad-hoc network, each node must be capable of routing data, self-organization, and taking care of the routing domain. The current implementation of laws and regulations has been a complex issue due to the lack of fast-moving and fixed infrastructure nodes. The existing system of malicious nodes in the ad-hoc network destroys the network performance of the original system. When a new node joins the network, the network does not have other nodes based on trust any major difficulties in the relationship between ad-hoc networks. Thus, the proposed system provides ad-hoc network routing security and authentication. In this proposed system, each node needs to introduce a Distance Vector Report Authentication Adjustable Routing Protocol (DVRAARP) and Secure Verification-Based Dynamic Node Selection (SVBDNS) algorithm. DVRAARP provides solutions to the greater threat of mobile ad-hoc network attacks. Enhanced SVBDNS requires its next hop to send confirmation emails to the originating node by maintaining the DVRAARP table. After receiving the route reply and confirmation routing path, the data was forward to the destination with encrypted using anRSA (Rivest, Shamir, Adleman) proxy with

ISSN 2515-8260 Volume 07, Issue 09, 2020

re-encryption. An SVBDNS algorithm is improved and extended by adding more realistic strategies such as varying node position, movement, speed, and data verification. Also, to identify the malicious nodes, it has been observed that this method will lead to the proposed system fewer savings and less breakage of communication.

Keywords: Distance Vector Report Authentication Adjustable Routing Protocol (DVRAARP), identify the malicious nodes, RSA (Rivest, Shamir, Adleman) proxy with re-encryption, Routing Security and Authentication, Secure Verification-Based Dynamic Node Selection (SVBDNS).

1. Introduction

MANET mobile user to communicate with relatively limited bandwidth in the autonomous radio link set. Since the nodes are mobile, the topology of the network fast, unpredictable changes over time. The network is distributed, and all network activity, including message, must be sent by the node itself found topology; routing function has been built into the mobile node. These different wireless ad hoc network applications, small to static networks, are limited to large-scale and highly dynamic mobile networks.

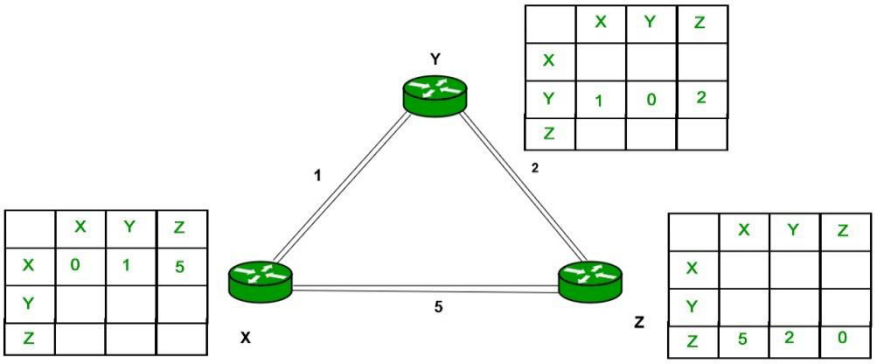

Figure 1 MANET routing analysis

It creates more than link-state flow because of changes in the number of hops that must be propagated to all the routers and each router for processing. Hops updates occur periodically, even if there is no change in the network topology, and therefore a waste of bandwidth broadcast still occurs as shown in figure 1.Network protocols are a complex issue for the design of these networks. In any case, the MANET application requires an efficient algorithm to determine the distributed network organization, scheduling and routing links. In mobile ad hoc networks (MANET), to use various applications that require greater security. This article aims to raise anonymity, security, authentication, authorization, and enforcement to meet the performance very safe and efficient routing method, the previous article in ad hoc networks. It meets greater flexibility, etc., to make such confidentiality, traceability, ad hoc performance environment safer

and more practical, and other requirements. The route is an important function of a network of mobile ad hoc networks.

Therefore, the enemy can attack network operations, and the routing protocol can easily collapse. These protocols' (RIP (Routing Information Protocol),IGRP (Interior Gateway Protocol)) security is analyzed by formal or informal methods that have never been applied to such protocols. Route discovery includes routes discovered between nodes and data packets, including forwarding of data packets superior to previously discovered routes.

Mobile ad-hoc network has the unique advantages of traditional networks in terms of encryption and encryption: (A) it can be easily installed and removed; (B) the solution is not suitable for the limitations of options such as geographical location, financial vulnerability as it is provided in a stable infrastructure set and low-cost area; (C), which can be set up in disasters (e.g., rescue missions). Identification is required for a node to exchange security information and avoid security threats.

2. Related Work

Heuristics identify the disk block accessed by the application startup process to access it and update the file system. The pointer moves from the HDD(hard disk drive) to an SSD (Solid State Drive).Since it runs as a background process, the overhead of moving blocks is negligible. It also an SSD strategy for the first edge block and the Shortest Sequence and Long Seek First (SSLSF) to make good use of the long initial limited space. A small collection of blocks assigned to the device driver is preferentially transferred to the SSD, especially if these blocks can cause long-term pursuit times on the HDD. This creates a lot of HDD space to reduce seek time at a small SSD cost [1].

Optimal IB (intermediate band) filling is a function of the IB region's constant amplitude and width with an absorption coefficient. The spatial variation of the sub-bandgap occurrence rate is not negligible. A new definition of optimal filling has been proposed for an account [2] to take this spatial change.

Also, regardless of node privacy, these methods rely on central control programs and third-party monitoring called DAPV (Diagnosing Anomalies Provenance and Verification) methods. A single or coordinated malicious node can be found in the entire network system, paralysis and abnormal nodes. DAPV phase can be detected in the routing [3] Release direct and indirect attacks.

Based on distributed dynamic addressing scheme low overhead identity in secure mobile ad hoc network nodes authorized management IP address settings. The new node receives an IP address from the existing neighbors. In the network [4], each terminal is assigned several new nodes, and a group can create a unique IP address from its IP address.

High-Frequency radar is an effective means of maritime supervision of the State. However, the difference causes deformation of the cable and receivers in the beam pattern of the antenna element in the phase response, resulting in loss of resolution direction. Estimating the

echo received by the phase Direction-Of-Arrival (DOA) sequence of the source measured in the primary ocean direction is proposed. The unique configuration of each signal decomposition is used to form a cost function. Minimizing a cost function, the angle of arrival, and phase error by combining an iterative process [5] Estimation.

Extensive research should determine the root cause of the loss to find the true malicious tip. If there is no such analysis, any security solution's effectiveness will punish the risk of innocent terminals, and the real malicious nodes will remain unknown. Therefore, this method is necessary to correctly identify the cause of bandage loss and [6] is the response verb.

MANET's flexibility and agility, so that they gained popularity in the use of a wide range. Network security protocol to protect protected application data for routing and development. However, this is only a security circuit or communication and can not be used simultaneously. Secure communications routing and security protocols must be implemented to provide comprehensive security. Wired telecommunications security protocols and WiFi network development were initially used [7] Manet only when placing high loads on network resources.

To increase the deliberate attack, MANET, the network of things in the robustness of the main nodes on the Internet, must be protected after the preliminary ruling. Keys that are usually focused on a single topology snapshot within a static or dynamic network of correlations with topology snapshots that can accommodate IoT networks that are not effective Dynamic Critical Node Identification (DCNI) Topology Used to Identify Nodes in MANET [8].

Also, vehicles must be protected to prevent criminals from using them to capture true identities further. To ensure that vehicle privacy is not leaked, effectively assisting vehicle communication, a 5G / B5G Vehicle Ad-Hawk Smart Trans Network to assist anonymous stabilization and key negotiations. It hingeson the confidence level of information to simulate human Evolutionary Self-Cooperative Trust (ESCT) projects' cognitive processes and prevent all kinds of interference routing attacks. In this method, the mobile node exchanging reliable information is received and analyzed [9] for the reliable determination of their knowledge [8].

Mobile payment systems in disaster areas offer the possibility of electronic transactions for people to buy goods and recycle food, clothing and medicines. On the other hand, to trade in the disaster area, current payment systems require communication infrastructure that can be destroyed in the disaster area in the event of a disaster such as a large-scale earthquake or flood (for example, wired network or cellular network cannot depend on) [10].

There is a unique dependency on collaboration between mobile ad hoc network participants to achieve fixed functionality. However, they are vulnerable to malicious attacks and refusal to cooperate. Therefore, it can see that the urgent need for security issues has been resolved. Many reliability’s have been considered in the last few years. The key to designing a reliable quantitative method is that these measures. This study proposes a lightweight subjective reasoning trust framework divided into a novel abstract trust and reliability evaluation and prediction [11].

In a typical radar system, the same hypothesis testing problem is to monitor the scene repeatedly periodically. This creates a basic balance between integration time and scanning speed. In particular, to increase the detection rate, the faulty alarm rate is defined as the average detection per unit time.Under constraints, the unit [12] defines the average false alarm time.

Multipoint Relay (MPR) indicators used in the new link quality evaluation function calculated by multiple routes. It uses the MPR selection mechanism to navigate topographical information flood nodes' selection using energy and ancillary quality. Read the energy and QoS parameters to benefit between QoS and energy-sensitive transaction closure. EXata-based simulations evaluate Multipath Energy And Quality Of Service (Qos)-Aware Optimized Link State Routing Protocol Version 2 (MEQSA-OLSRv2) Performance and its effectiveness are compared to traditional routing protocols [13].

To increase network capacity, information of the target neighbor multicast protocols proposed adjustment data and considerations taken to minimize the appropriate host repeater and barrier total transmission time of the total time blocks are to be transferred [14].Now, high energy and low mobility hosts are identified as cluster heads (cluster heads). Routing protocols are now proposing routing energy savings by controlling host power levels. Cooperative caching P2P connection has been proposed structured data based mobile P2P network. In this scheme, the cluster and the long run, mobile nodes are connected to the peer's neighbors to clean up the shared cache and propagate metadata to achieve highly efficient data retrieval performance [15].

This multicast routing protocol is proposed for encoding wireless at hook networks. A tree for each multicast that meets a certain percentage of demand, the tree's network usage network, installer use, and diversity may be lost. Guaranteed bandwidth for the series The proposed protocol can reduce consumption over the full bandwidth. Using network coding, the scheduling algorithm does not generate redundant packets, and the data packets are never assigned to the multicast tree [16].

Network coding is a proven technique for improving the performance of wireless networks. Quality of Service(QoS) bandwidth required to know the coding of consumption forces, to design a successful navigation Carolina network coding protocol. Also, it is necessary to increase the coding opportunity to increase network capacity. However, the host and the host can be challenged to determine whether encoding is determined in the mobile ad hoc network (MANET) [17] encoding the host bandwidth consumption.

Therefore, fairness and dual busy tones solve hidden and exposed terminals that need to improve throughput performance for multiple access protocols. Therefore, this article is to achieve an improved quality of service MANET Dual Busy Tone Multiple Access Protocol (DBTMAP) through service excellence to improve network capacity. The proposed method is the Retransmit Double Busy Tone Multiple Access (RDBTMA) protocol [18] using the improved dual-base tone multiple access protocols.

The Internet of Drones (IoD) is a hierarchical network control design designed primarily to integrate drone control and access with Internet transmission and provide navigation services

from a so-called node location.The IoD variety of drone applications include package delivery, traffic monitoring, search and rescue provision of general services, and more [19].

Wi-Fi has a very bright future for networking and communications, which is the researchers are very interested in. By increasing the user's goal using a wireless ad hoc network, they will also become a wireless ad hoc network with improved performance and diverse needs. Routing protocols can help better use resources for the application required QoS and load balancing communicate effectively and improve the network [20] performance.

A chaotic logistics mapping here uses the OFDM (Orthogonal Frequency Division Multiplexing) symbol for frequency and time domain congestion. Before transmitting the signal through the optical fiber, the message is calculated separately in the optical line terminal and the optical network unit to verify the actual data is reset to digestion and digested OFTM signal [21].

3. Implementation of the proposed system

DVRAARP can enable solitary MANET routing in its core function. According to the applicability of specific network scenarios, each auxiliary function is given additional functions. For example, each node provides a connection between MANET and other routing areas. It can reach directly with its transmission to consider MANET and define all other nodes as its communication neighbors. Assuming that each node knows the location of its location and its neighbors.The SVBDNSto verification of node location is an important issue in mobile networks, and it becomes especially challenging in the presence of adversary targeting damage systems. To DVRAARP,find neighbor nodes and verify them.

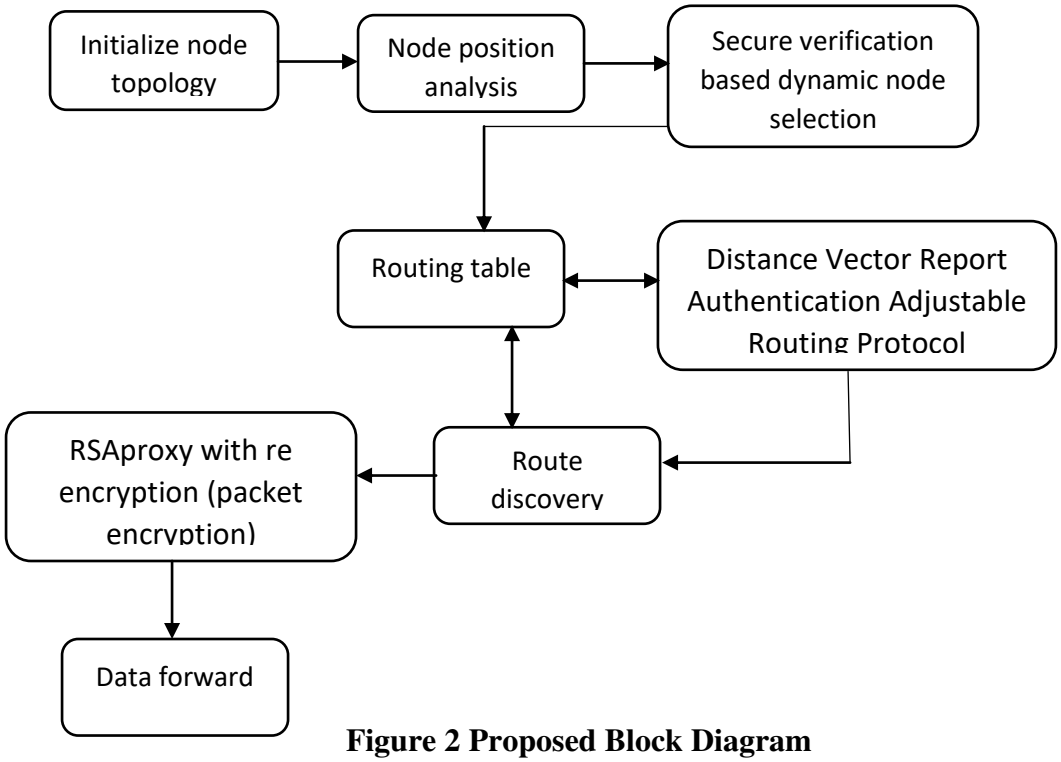

Figure 2 Proposed Block Diagram

ISSN 2515-8260 Volume 07, Issue 09, 2020

It is now necessary to remove the malicious node, which has a path to isolate the malicious node. This information will be broadcast to all neighbors who will be removed from each interconnection. In the same way, if the other nodes also decide to cancel the connection from the node. After removal, the analysis guidelines providing node remains at high spatial accuracy. In the proposed system, the message is signed by routing maintained by the node on the route when DVRAARP.In the RSA (Rivest, Shamir, Adleman), proxy with the re-encryption scheme on the agent and the route/destination node to verify each node's authenticity. Then in the case, to authenticate the source node to the destination node manner. And malicious nodes such as isolation may not participate in the network activities. Further communication, a malicious node neighbor node, not including the routing process, will not accept a request message from a malicious node. Because data verification is the task of proving that a that RSA (Rivest, Shamir, Adleman) proxy with re-encryption operates correctly concerning a formal property of data packets encryption and decryption key be to generated and then verify the data communication.

3.1 Analysis of Node Moving Transmission Range

When the route discovery process begins, the source node knows the existing route to the destination level analysis shown in figure 3. Due to the dynamic nature of all the mobile nodes.Suppose the maximum data in every node can transmit or receive radius simultaneouslyM_RBut not be used simultaneously.

Also, the process is initiated for the energy of each node. Node is defined by the mean of the N values of the neighbors.Then $N= \lambda\pi M_{R^2}$Characterizes a network connection. In the nodes of the network and are evenly distributed, and the density λ toxic process.

Figure 3 Node moving transmission range analysis

Edge depends on two major features:

Position of Nodes: It is calculated and controlled by changing the transmission radiusM_R topology is very difficult.

Communication Range: To use the communication range of the behind the formula:

$$E= \{(u, v)\ \varepsilon V^2 | u\neq v \text{ distance } (u,v) \leftarrow \text{range} \quad (1)$$

Wherein the maximum communication range ofM_R.

Neighbor set N (U) vertex u is:

$$N(u) = \{ v \mid (u, v)\ \varepsilon \text{ Edge}\} (2)$$

Range distribution function r(u) which is made available to label a vertex V and E is changed from 0 to r range denoted asG(V, Er)

$$\text{Edge contained by range (Er)} = \{(u, v)\ \varepsilon\ V^2 \mid u\neq v \text{ distance } (u,v) \leftarrow r(u) \quad (3)$$

In this circumstance, the radius is contingent on the effectiveness of the appropriate propagation model.

3.2 Secure Verification-Based Dynamic Node Selection

Instead of measuring the distance information between nodes, communication network transmission techniques using the proposed calculates, the unknown node's position coordinates. Problems proposed use purposes MANET node location is reduced to accurately position and position deviation between the actual and calculated for each node of the unknown nodes. The evaluation criteria include SVBDNS precise positioning, an unknown number of nodes positioned adjacent nodes, and a requests communication node radius. The DVRAARP in each node maintains a distance table.

Step1: Initialize the number of nodes

Step2: identify the source and destination node id. An available distance of node n_i and required the minimum distance of node m_i

Step3: Critical sensing point of then_i. If source node denote as s_n and the nearest neighbor node denote n_n

$$n_i < m_i \quad (4)$$

Step4: Calculates the distance to each neighbor node from an unknown node.

Step5: To calculate each neighbor node average distance

$$\text{Distance } d_i = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \quad (5)$$

Where $x_1, y_1, x_2, y_2$the position is coordinates of two neighbor nodes the number of sequences 1 and 2.

Step6: Each neighbor node calculates the average of all the unknown nodes, and each unknown hop distance reaches the first node receives informationa_i:

$$a_i = \frac{\sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}}{h_i} (6)$$

Where h_i the hops from the neighbor node.

Step7: Checking the communication node id

$$if\ hop > h_i \quad (7)$$

Update the detection of packets.

Else discard the detection packet. R

End if

Repeating the proceeding steps until all communication between nodes is covered.

The communication path between the two nodes in the routing table is to maintain the distance. Estimated distance is the distance covered by each hop.

3.3 Distance vector report authentication adjustable routing protocol (DVRAARP)

The protocol presented here uses the concept of water immersion for the serial number modification of RREQ. When an intermediate node receives the RREQ packet, the routing tables are modified with the latest information and broadcasts the RREQ packet to its neighbor. Reject data packet copied node. The serial number will then be rebroadcast on the routing table to copy

the process and RREQ packet status. The verification protocol RREQ replay sequence number equal to the stored current node in the RREQ same sequence number. If the serial numbers are different, this would be considered an unusual activity.

Algorithm

Step1: initialize the source node, destination node and total neighbor nodes in MANET.

Step2: Assume the categories of nodes. Node type= normal nodeN_n, misbehavior nodeM_n, suspicious nodeS_n and data path d_p

Step3: To check theN_n,M_n,S_n.

Step4: Broadcasting the RREQ check categorization number is not equal to the stored same RREQ in the current node sequence.

Step5: If the data packet does not equal the sequence numberd_p

d_p = true;

Step6: Send the data packets RREQ;

else

d_p = false;

Step7: Now, check its behavior, which Node_ type =N_n.

Track node attack

Then the node checks its capacity

Calculate Complete Data Rate (CDR)

If Complete Data Rate =max

Send the RREQ

End if

Step8:RSA (Rivest, Shamir, Adleman) proxy with re-encryption to use

Step9: In the unidirectional schemes, the proxy re-encryption cannot compute the data sent from node b to give the data sent from a to b.

The scheme to collect the source node and destination node id.

Step10: Input data i_d and split the data into several data packets d_p

For each $d_p$where p=1 to n do

End for

Step 11: Encrypt the packets using the public key p_k send and the server to given the private key p_t.

Step 12: The private key to generate after the original message to receive the destination node.

If a malicious packet's arrival time is longer than the original packet, it will detect anomalous activity and node type and update accordingly. Also, determine the nature of the suspicious node capacity and node by calculating the confidence values. If the result is satisfactory in terms of performance and the node's trust value, the corresponding node becomes a suspicious, malicious node. The capacity of the node depends on the percentage of data packets raised by the node.

4. RESULTS AND DISCUSSION

Distance Vector Report Authentication Adjustable Routing Protocol (DVRAARP) based routing based on data network security and the inspection's efficiency has been performed. There is a connection between the network and associated with the MANET significant pollutants.

Table 1 Proposed Simulation Parameters Details

SimulationParameters	Simulation Value
Proposed Simulator	NS2 (Network Simulator version-2)
Proposed Simulation Time	30 sec
Proposed Traffic Type	CBR (Constant Bit Rate)
Proposed Node Speed	20 m/s
Proposed Progression data size	180Mb
Data Packet size	512kb
Total packet	380

Portability practice has proved that other areas from the central area can take advantage of a Tool Command Language (TCL) content licensing purposes.This section designates the evaluation of existing Dynamic Critical Node Identification (DCNI), Multipath Energy and Quality of Service (QoS)-Aware Optimized Link State Routing Protocol Version 2 (MEQSA-OLSRv2), DAPV (Diagnosing Anomalies Provenance and Verification) and the proposed Distance Vector Report Authentication Adjustable Routing Protocol (DVRAARP).

This section compares the various parameter: i) Analysis of Packet Delivery Ratio, Throughput Performance Level, Route Availability Analysis, Analysis of Communication security level before malicious node enter, Analysis of Communication security level after malicious node enter.

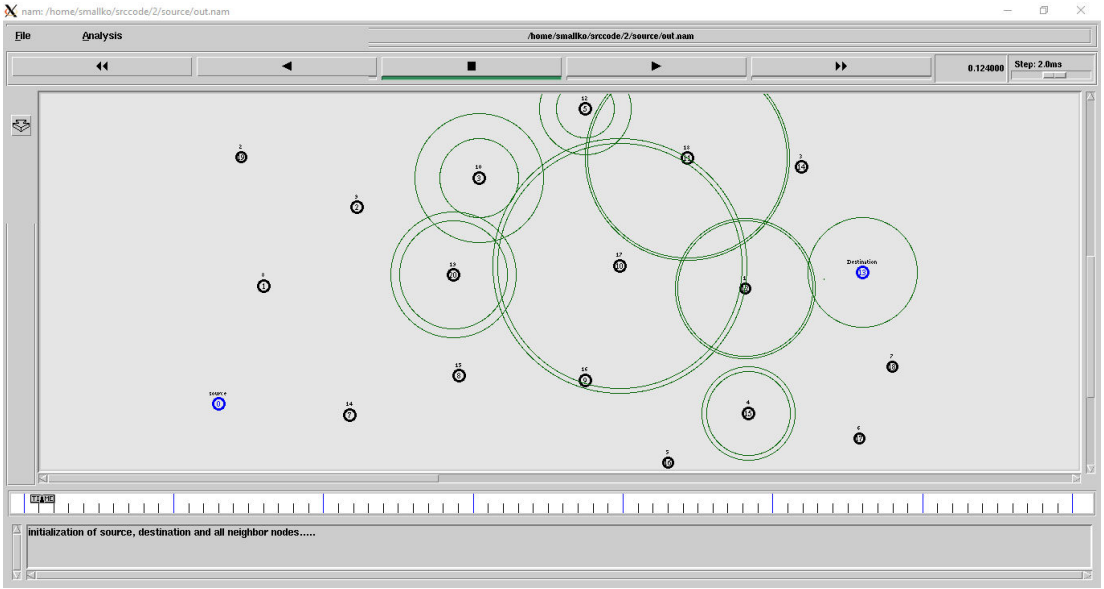

Figure 4 Node Initialization

Figure 4 shows the initialization of the source node, destination node and all neighbor nodes.

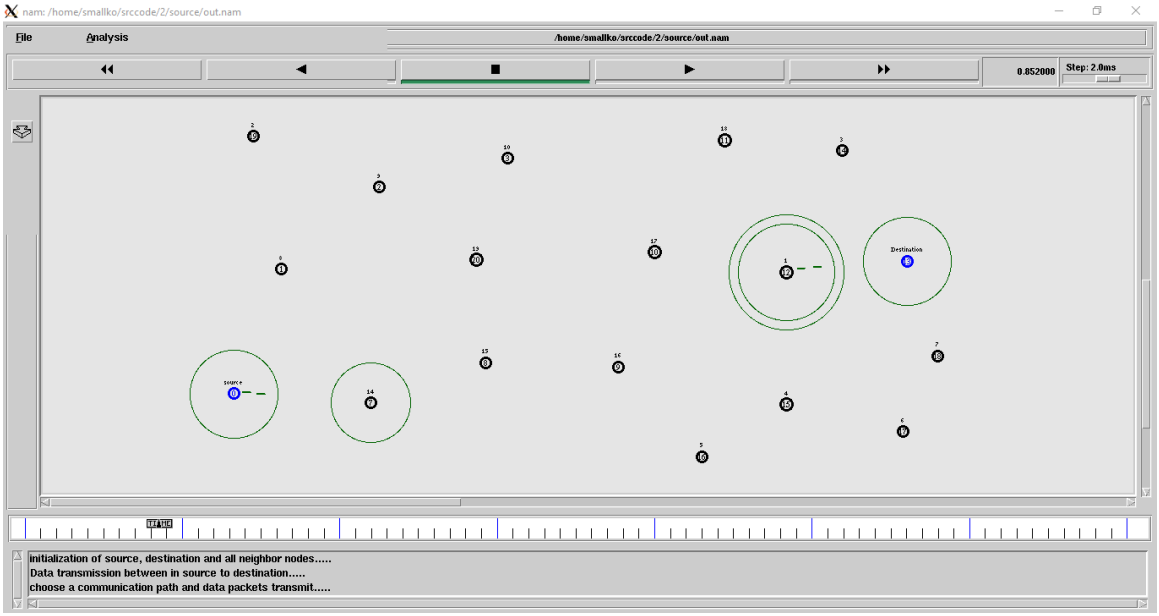

Figure 5 data packets to transfer between the source node and destination node

Figure 5 describes the transfer of data packets between the source node and the destination node. Before transmission, the DVRAARP protocol maintains the routing table and selects the communication path.

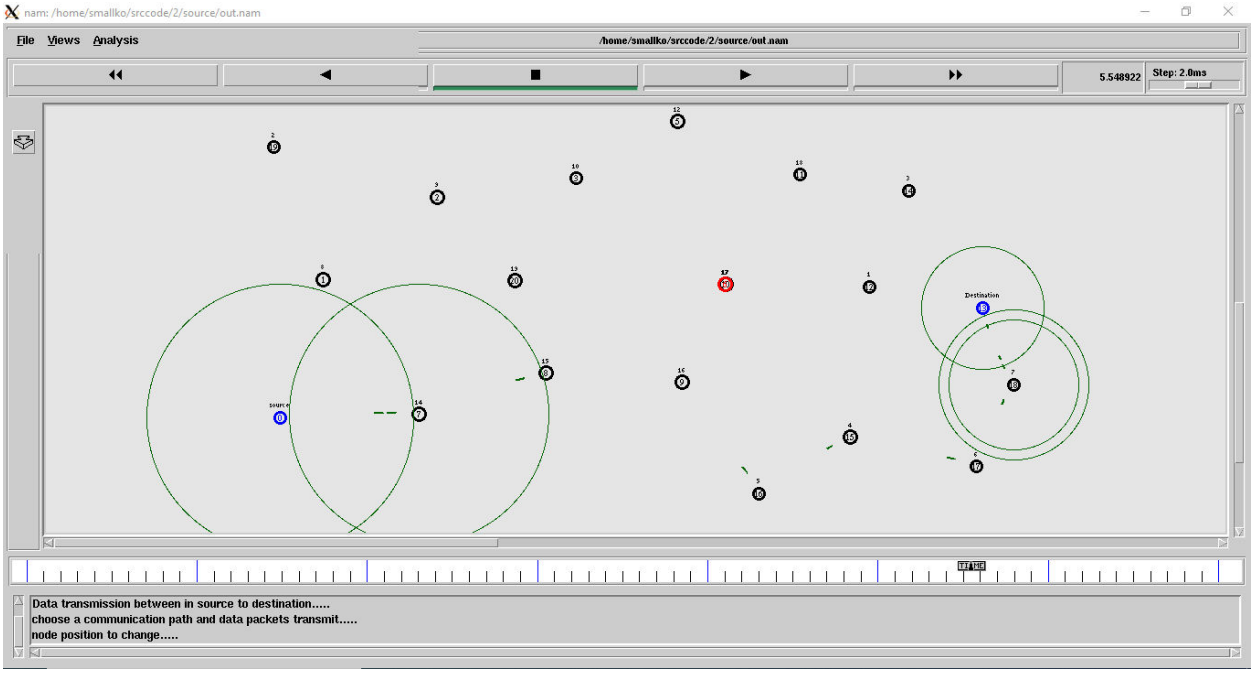

Figure 6 analysis of node position to change

Figure 6 describes the node position to change. The node number 6 and their id number 13 to change the position.

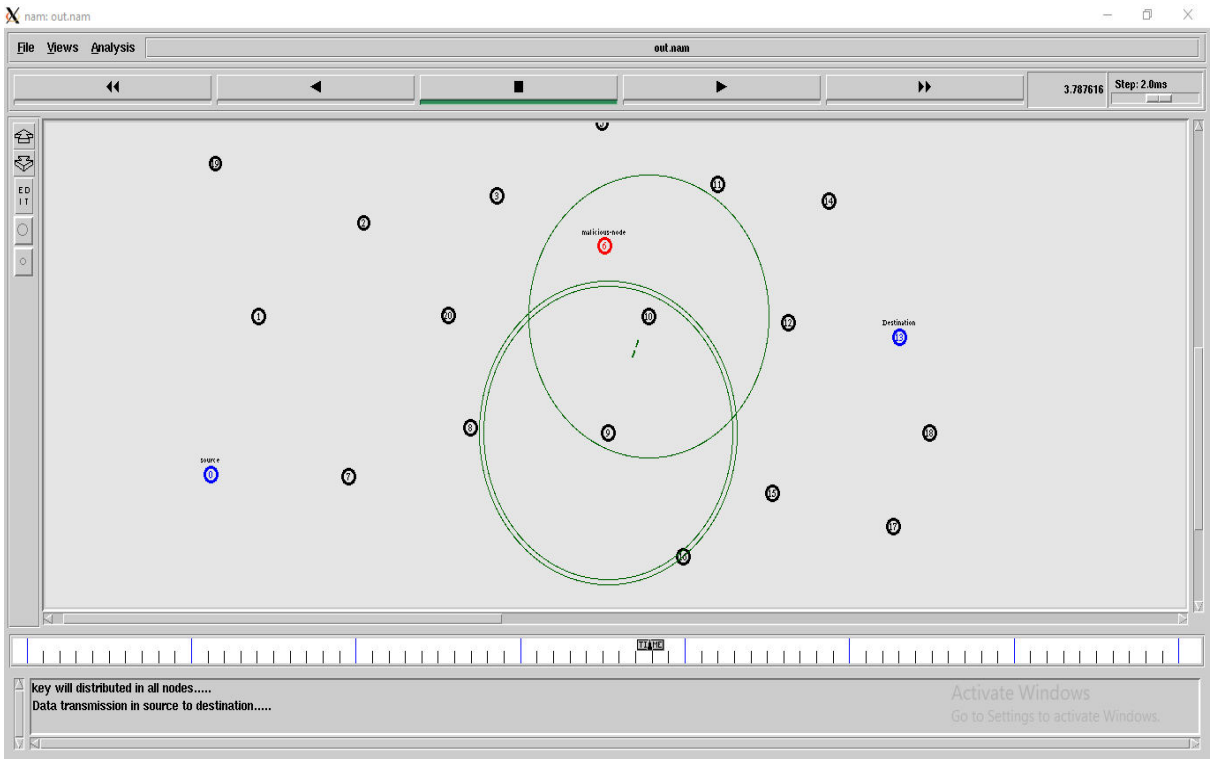

Figure 7identify the malicious of node

Figure 7 describes the identify the malicious node. The DVRAARP protocol to detect the malicious node does not allow to enter the source to the destination path. Because the DVRAARP protocol maintains the routing table and then the SA (Rivest, Shamir, Adleman) proxy re-encryption is used to encrypt the packets' data.

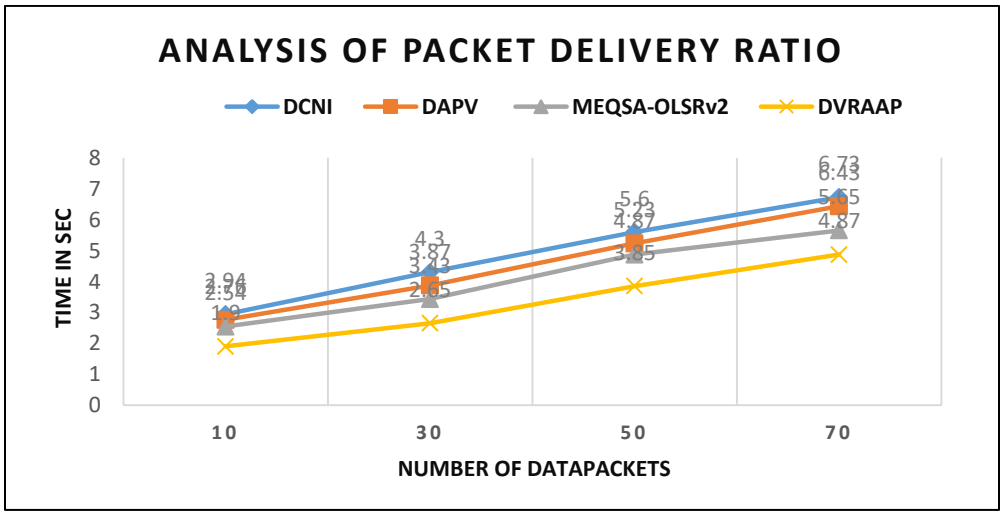

Figure 8Performance Analysis of Packet Delivery Ratio

Packet Delivery Ratio(PDR) to assess the quality of the network. It is defined as the ratio between the destination's packets and the source's packet data. It can use the awk script, which produces a trace file, and the results obtained.

PDR = Received packets/ Generated packets * 100 --- (8)

The proposed DVRAARP protocol and existing method DCNI, MEQSA-OLSRv2, DAPVcomparison of packet delivery ratio is shown in figure8. The analysis result proposed DVRAARP 9.4 in a sec of lower time-based packet delivery provide compare to the existing method DCNI has 6.73 sec, DAPV with 6.43 sec, and MEQSA-OLSRv2 has provided a 5.65 sec.

Table 2 analysis of throughput level

Simulation Time in s	DCNI in bps	DAPV in bps	MEQSA-OLSRv2 in bps	DVRAARP in bps
10	172	194	216	264
20	246	264	288	372
30	316	348	384	428
40	504	518	528	562
50	546	558	576	624

Table 2 indicates the throughput values received throughout the simulation analysis for DCNI, DAPV, MEQSA-OLSRv2, and DVRAARP mechanisms.

Successfully spreading the process and sending data packets of as many as 200 data packets to the Internet. Throughput is obtained using equation 9.

$$Throughput = \frac{Packets\ Received\ (n) * Packet\ size}{200} \quad \text{--- (9)}$$

Where

n = number of nodes

ISSN 2515-8260 Volume 07, Issue 09, 2020

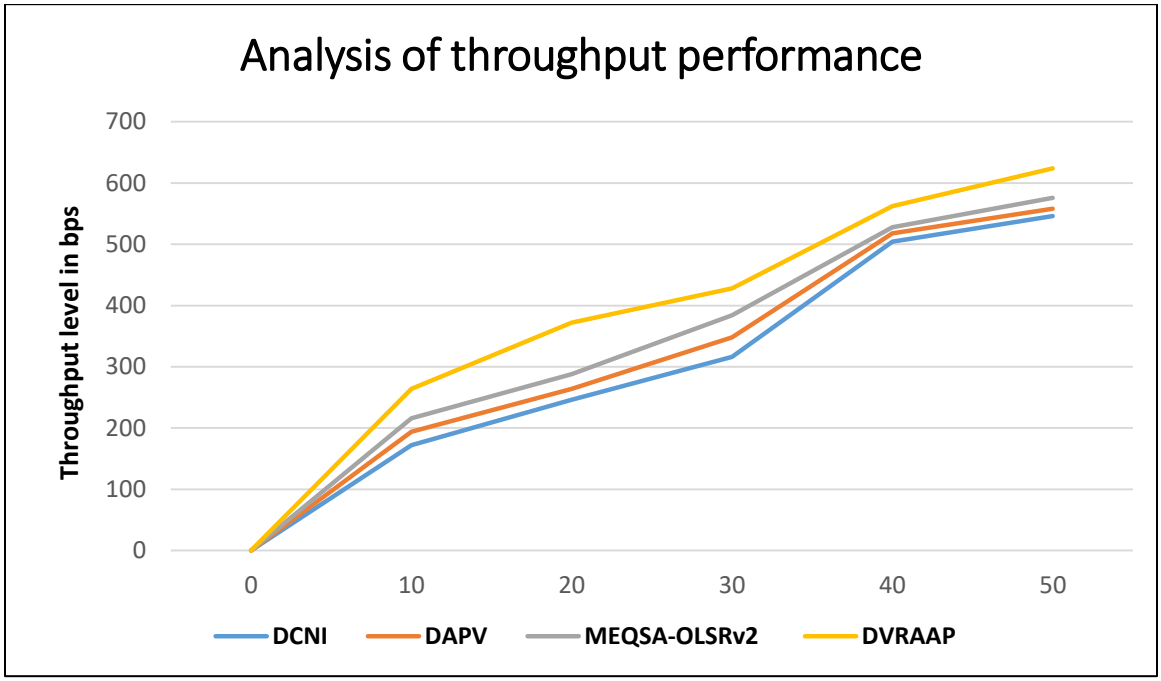

Figure 9Throughput Performance Level

It can be successfully received from the number of data packets in Figure 9. Every 200 data packets are observed for DVRAARP is higher than compared 624 in bps to that of the existing algorithms DCNI in 546 in bps, Fuzzy Logic 558 in bps, ARSH-FATI 576 in bps.

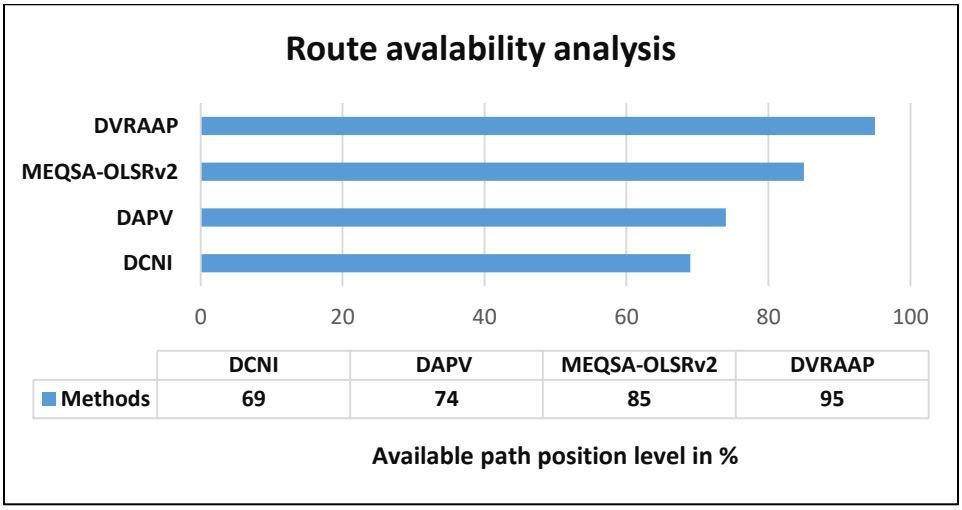

Figure 10 Route Availability Analysis

In path analysis, the total number of nodes is calculated by dividing the total number of connections by the number of available paths. An important advantage of using multipath transmission is the inherent path diversity (i.e., the loss process is expected to operate independently for different paths).Multitasking routing is an effective method to achieve this goal, as shown by network data shared via multiple paths to reduce network congestion.

ISSN 2515-8260 Volume 07, Issue 09, 2020

Comparison of the proposal shown in figure 10 with existing methods. The existing methods DCNI in 69%, DAPV in 74%,MEQSA-OLSRv2 in 85% and the proposed method DVRAARP with 95%.

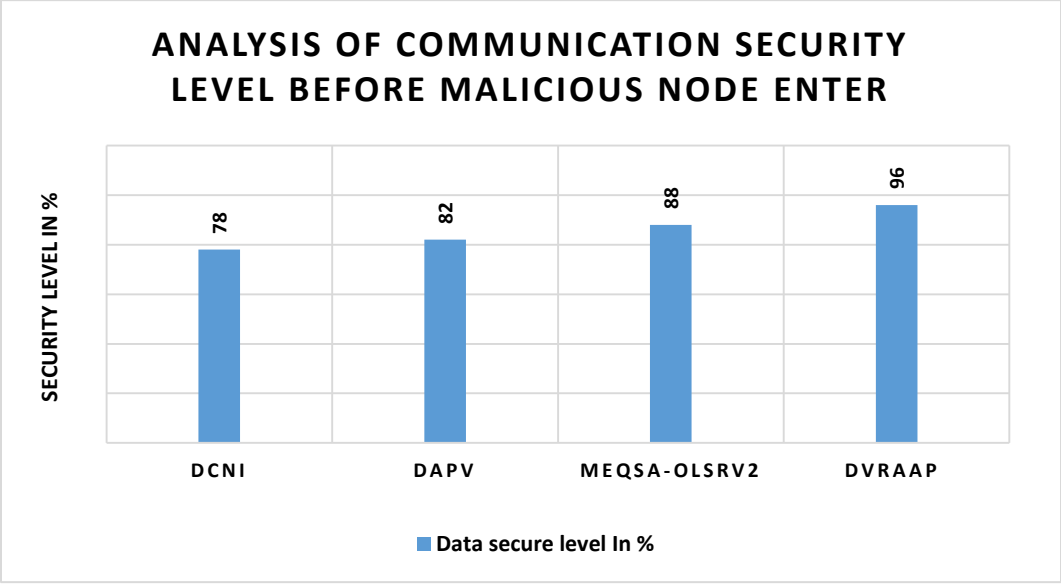

Figure 11Analysis of Communication security level before a malicious node enter

The above figure 11 describes the analysis of communication security level before a malicious node attack. The existing DCNI data secure communication level in 78%, DPAV data secure level in 82%, MEQSA-OLSRv2 data secure communication level in 88%, and the proposed DVRAARP data secure communication level in 96%.

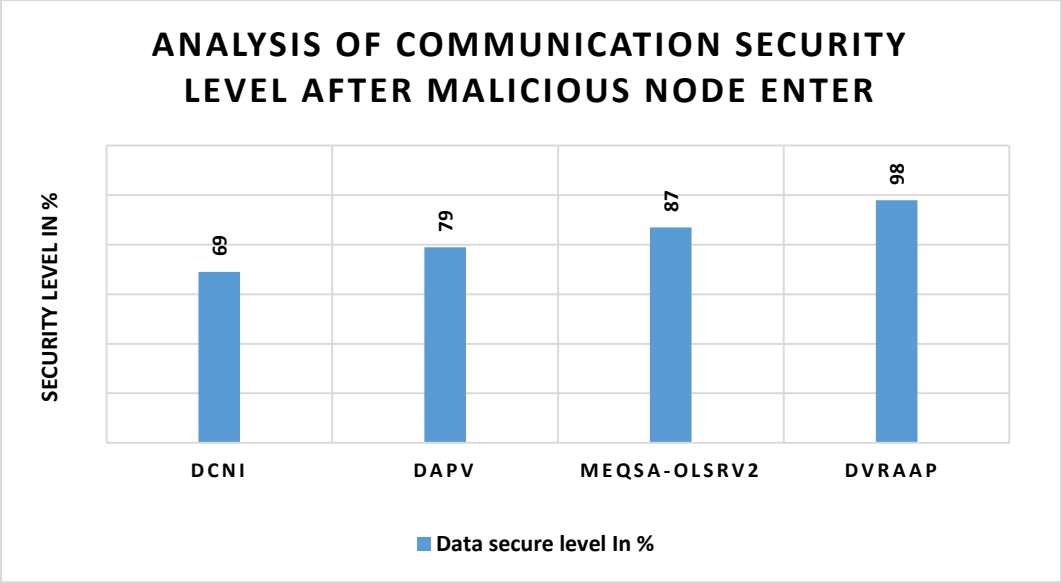

Figure 12Analysis of Communication security level before a malicious node enter

The above figure 12 describes the analysis of communication security level afterthe malicious node enter. The existing DCNI data secure communication level in 69%, DPAV data

secure level in 79%, MEQSA-OLSRv2 data secure communication level in 87%, and the proposed DVRAARP data secure communication level in 98%.

5. Conclusion

SVBDNS is presented here; the probability density function is used to find the location in the network nodes. Further, the node starts moving from the initial node position at a constant speed and track its position next node. The next level of each node is stored, and if the distance is greater than the sending node, it will be greater than the coverage of the network and therefore reduced.Allocation position and range of the communication range, the neighbor set, the node provides an effective solution for mobility for parameters. Initially, the proposed SVBDNS used to provide authenticated data between nodes between the source and destination. But this kind of algorithm is called a scene where the node has less movement, which is an effective solution for unsuitable ad-hoc routing protocols. The DVRAARP protocol has also been incorporated into this illustrative method to secure data transmission in a dynamic environment. The proposed DVRAARP to shows the analysis of packet delivery ratio is 9.4 sec. The throughput level is 624 bps; route availability analysis is 95%, analysis of communication security level before malicious node enter is 96%, and analysis of communication security level before malicious node enter is 98%.

References

1. Gao, Honghao; Liu, Can; Li, Youhuizi; Yang, Xiaoxian (2020). V2VR: Reliable Hybrid-Network-Oriented V2V Data Transmission and Routing Considering RSUs and Connectivity Probability. IEEE Transactions on Intelligent Transportation Systems, (), 1–14. doi:10.1109/TITS.2020.2983835.
2. Jain, Monika; Sharma, Nikhil; Gupta, Akash; Rawal, Divyang; Garg, Parul (2020). Performance Analysis of NOMA Assisted Mobile Ad hoc Networks for Sustainable Future Radio Access. IEEE Transactions on Sustainable Computing, (), 1–1. doi:10.1109/TSUSC.2020.2987427.
3. Li, Teng; Ma, Jianfeng; Pei, Qingqi; Song, Houbing; Shen, Yulong; Sun, Cong (2019). DAPV: Diagnosing Anomalies in MANETs Routing with Provenance and Verification. IEEE Access, (), 1–1. doi:10.1109/ACCESS.2019.2903150.
4. Ghosh, Uttam; Datta, Raja (2015). A Secure Addressing Scheme for Large Scale Managed MANETs. IEEE Transactions on Network and Service Management, (), 1–1. doi:10.1109/TNSM.2015.2452292.
5. Liu, Gao; Dong, Huidong; Yan, Zheng; Zhou, Xiaokang; Shimizu, Shohei (2020). B4SDC: A Blockchain System for Security Data Collection in MANETs. IEEE Transactions on Big Data, (), 1–1. doi:10.1109/TBDATA.2020.2981438.

6. Khan, Muhammad Saleem; Midi, Daniele; Khan, Majid Iqbal; Bertino, Elisa (2017). Fine-Grained Analysis of Packet Loss in MANETs. IEEE Access, (), 1–1. doi:10.1109/ACCESS.2017.2694467.
7. Hurley-Smith, Darren; Wetherall, Jodie; Adekunle, Andrew (2017). SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks. IEEE Transactions on Mobile Computing, (), 1–1. doi:10.1109/tmc.2017.2649527.
8. Zhang, Jing; Cui, Jie; Zhong, Hong; Bolodurina, Irina; Liu, Lu (2020). Intelligent Drone-assisted Anonymous Authentication and Key Agreement for 5G/B5G Vehicular Ad-hoc Networks. IEEE Transactions on Network Science and Engineering, (), 1–1. doi:10.1109/TNSE.2020.3029784.
9. Cai, Ruo Jun; Li, Xue Jun; Chong, Peter Han Joo Han Joo (2018). An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs. IEEE Transactions on Mobile Computing, (), 1–1. doi:10.1109/TMC.2018.2828814.
10. Ojetunde, Babatunde; Shibata, Naoki; Gao, Juntao (2017). Secure Payment System Utilizing MANET for Disaster Areas. IEEE Transactions on Systems, Man, and Cybernetics: Systems, (), 1–13. doi:10.1109/TSMC.2017.2752203.
11. Xia, Hui; Cheng, Xiangguo; Zheng, Yuhui; Liu, Anfeng (2018). A Novel Light-weight Subjective Trust Inference Framework in MANETs. IEEE Transactions on Sustainable Computing, (), 1–1. doi:10.1109/TSUSC.2018.2817219.
12. Chen, Zheng; Zhou, Wenli; Wu, Shuo; Cheng, Li (2020). An Adaptive on-Demand Multipath Routing Protocol With QoS Support for High-Speed MANET. IEEE Access, 8(), 44760–44773. doi:10.1109/ACCESS.2020.2978582.
13. Jabbar, Waheb A.; Saad, Wasan Kadhim; Ismail, Mahamod (2018). MEQSA-OLSRv2: A Multicriteria-based Hybrid Multipath Protocol for Energy-Efficient and QoS-Aware Data Routing in MANET-WSN Convergence Scenarios of IoT. IEEE Access, (), 1–1. doi:10.1109/ACCESS.2018.2882853.
14. Chen, Yu-Hsun; Hu, Chia-Cheng; Wu, Eric Hsiao-Kuang; Chuang, Shu-Min; Chen, Gen-Huey (2017). A delay-sensitive Multicast Protocol for Network Capacity Enhancement in Multirate MANETs. IEEE Systems Journal, (), 1–12. doi:10.1109/JSYST.2017.2677952.
15. Hu, Chia-Cheng (2020). P2P Data Dissemination for Real-Time Streaming Using Load-Balanced Clustering Infrastructure in MANETs With Large-Scale Stable Hosts. IEEE Systems Journal, (), 1–12. doi:10.1109/JSYST.2020.2992774.
16. Chen, Yu-Hsun; Wu, Eric Hsiao-Kuang; Chen, Gen-Huey (2015). Bandwidth-Satisfied Multicast by Multiple Trees and Network Coding in Lossy MANETs. IEEE Systems Journal, (), 1–12. doi:10.1109/jsyst.2015.2406756.
17. Chen, Yu-Hsun; Wu, Hsiaokuang; Lin, Chun-Han; Chen, Gen-Huey (2017). Bandwidth-Satisfied and Coding-Aware Multicast Protocol in MANETs. IEEE Transactions on Mobile Computing, (), 1–1. doi:10.1109/TMC.2017.2778262.

18. Sivaram, M.; Porkodi, V.; Mohammed, Amin Salih; Manikandan, V.; Yuvaraj, N. (2019). Retransmission DBTMA Protocol with Fast Retransmission Strategy to Improve the Performance of MANETs. IEEE Access, (), 1–1. doi:10.1109/ACCESS.2019.2918723.
19. Rahman, Taj; Ullah, Inam; Rehman, Ateeq Ur; Naqvi, Rizwan Ali (2020). Clustering Schemes in MANETs: Performance Evaluation, Open Challenges, and Proposed Solutions. IEEE Access, (), 1–1. doi:10.1109/ACCESS.2020.2970481.
20. Pathak, Gaurav; Kumar, Krishan (2017). Traffic aware load balancing in AOMDV for mobile Ad-hoc networks. Journal of Communications and Information Networks, (), –. doi:10.1007/s41650-017-0012-z.
21. Gill, Harsimranjit Singh; Gill, Sandeep Singh; Bhatia, Kamaljit Singh (2017). A Novel Chaos-Based Encryption Approach for Future-Generation Passive Optical Networks Using SHA-2. Journal of Optical Communications and Networking, 9(12), 1184–. doi:10.1364/JOCN.9.001184.
22. Zhang, Peng; Lin, Chuang; Jiang, Yixin; Fan, Yanfei; Shen, Xuemin (2014). A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks. IEEE Transactions on Parallel and Distributed Systems, 25(9), 2211–2221. doi:10.1109/TPDS.2013.161.