Computers, Materials & Continua
DOI:10.32604/cmc.2022.019221
Article

Tech Science Press

An Optimized Fuzzy Based Ant Colony Algorithm for 5G-MANET

R. Nithya[1], K. Amudha[2,*], A. Syed Musthafa[3], Dilip Kumar Sharma[4], Edwin Hernan Ramirez-Asis[5], Priya Velayutham[6], V. Subramaniyaswamy[7] and Sudhakar Sengan[8]

[1]Department of Computer Science and Engineering, Vivekananda College of Engineering for Women, Tiruchengode, 637205, Tamil Nadu, India
[2]Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Thottiam, 621215, Tamil Nadu, India
[3]Department of Information Technology, M. Kumarasamy College of Engineering, Karur, 639113, Tamil Nadu, India
[4]Department of Mathematics, Jaypee University of Engineering and Technology, Guna, 473226, M.P., India
[5]Business and Tourism Faculty, Universidad Nacional Santiago Antunez De Mayolo, Huaraz, Peru
[6]Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, 637018, Tamil Nadu, India
[7]School of Computing, SASTRA Deemed University, Thanjavur, 613401, Tamil Nadu, India
[8]Department of Computer Science and Engineering, PSN College of Engineering and Technology, Tirunelveli, 627152, Tamil Nadu, India
[*]Corresponding Author: K. Amudha. Email: ambakika123@gmail.com
Received: 06 April 2021; Accepted: 25 May 2021

Abstract: The 5G demonstrations in a business has a significant role in today's fast-moving technology. Manet in 5G, drives a wireless system intended at an enormously high data rate, lower energy, low latency, and cost. For this reason, routing protocols of MANET have the possibility of being fundamentally flexible, high performance, and energy-efficient. The 5G communication aims to afford higher data rates and significantly low Over-The-Air latency. Motivated through supplementary ACO routing processes, a security-aware, fuzzy improved ant colony routing optimization protocol is proposed in MANETs. The goal is to develop a MANET routing protocol that could provide a stable packet transmission ratio, less overhead connectivity, and low end-to-end latency in shared standard scenarios and attack states. MANET demonstrates effective results with hybrid architecture and proved to be effective than other *state-of-the-art* routing protocols of MANETs, like AODV, its routing organization implemented through Optimized Fuzzy based ACO Algorithm for 5G. Millimeter-wavelengths are required to perform a significant role in 5G. This research proposed to test the efficiency of MANET consisting of only *mm*Wave User Equipment. MANET reduced packet transmission loss of UEs with *mm*Wave, meaning well-transmitted SNR leads directly to a better packet delivery ratio. To verify results, simulation using the NS-3 simulator *mm*Wave module is used.

Keywords: 5G; attacks; D2D communications; MANET; *mm*Wave; security

1 Introduction

As technology advances, smartphones, iPad, and added advanced portable devices are widely accepted in the average lifespan. Smart devices like mobile offer user's various kinds of facilities that made life more comfortable, easy, and entertaining. Such portable devices have historically been associated with infrastructure-based networks like cellular networks, Wi-Fi, hot spots, and cable nets. Simultaneously, this kind of method can also form a Mobile Ad hoc NETwork (MANET) [1] that does not need any infrastructure. The MANETs are generally composed of wireless portable devices that can link and dispense the network free. Because of deficiency in an organization, a MANET would be set up at lower costs than required by deploying the wired network. Unlike portable devices that may link directly with each other through Wi-Fi or Bluetooth, the existence of supplementary specifications for routers, cables, or other forms of infrastructure-based equipment is not compulsory. They were studied over many years, and networks are developed uniquely through [2] mobile UE so that they are active in exchanging data in a wireless environment. MANET would be used in several applications, including disastrous areas, tactical edge operations, and crowded environments such as stadiums and educational campuses, where many users are willing to exchange data directly with everyone or use routers from other devices.

The 5th Generation (5G) in wireless communication [3] intends to offer great data rates with much reduced Over-The-Air (OTA) latency. The Millimetre-Wave (*mm*Wave) wavelength plays a key role in 5G standards. This has the benefits of primarily presented bandwidth and reduced latency. Simultaneously, Millimetre-Wave (*mm*Wave) wavelength also has certain drawbacks due to the restricted propagation spectrum [4] and the need to relay small beams to reach longer distances. This research is proposed to test the MANET's efficiency of *mm*Wave User Equipment without eNodeB (or gNodeB as recently suggested by 3GPP) [5]. For viability and reliability of *mmWave* MANET systems, the transmission ratio of data transferred among any two mobile nodes is essential in the network. This complex network topology (because of the complexity and lack of infrastructure) is inappropriate for regular end-to-end routing algorithms [6], which is why many MANETs routing protocols have been introduced for monitoring the data transmission from one node to other nodes in MANET using multi-hop nodes. MANET [7] currently has routing protocols that typically depend on wireless signals transmitted in the sub-6 GHz band. The claim is that wireless signals are no longer valid in the directional antennas and beamforming of the mmWave. To investigate such a lacking, *mm*Wave systems use various methods to search the whole environment around them, such as Random Beam Forming (RBF), beam sweeping, etc. and deliver small directional beams [8] the predictable destination nodes for minimizing loss of propagation route.

The Ant Colony Optimization (ACO) method is motivated through biology and incorporated with the method [9] used by ants to find effective routes by detecting deposited pheromones simultaneously. ACO perfectly suits networks in the environment and provides a collective framework for NP-hard optimization problems [10]. Because of the dynamic environment of ACO's networking, it continuously gets adapted to real-time network changes. Additionally, artificial ants can simultaneously catch multiple results to the problem under consideration. ACO-based models are therefore capable of finding optimum paths efficiently, which leads to being realistic in network communication routing. MANET applications [11] raise the attackers' stimulus to manipulate or interrupt them. For complex MANET systems, threats that seek to intrude the network or find private information in the network are always likely to be present. For example, in VANET situations, malicious vehicles will relay false road safety signals that could cause traffic jams or

even crashes [12]. Human life can be vulnerable in such circumstances if the network does not function correctly because of assaults. Also, some MANET nodes may be self-interested in the routing process for protecting the battery power or store data [13].

Consequently, routing protocol architecture plays an essential role in maintaining MANET confidentiality [14]. This study purports to develop an active routing protocol in MANETs that would not provide a high Packet Delivery Ratio (PDR) [15], minimize the overhead, and reduce end-to-end latency. Nevertheless, it can also be resilient contrary to malicious users and malfunctioning devices in the MANET.

The first approach depends on a specific context in the implemented nodes and offers instructions to define the optimal option as a feature of the device parameters. A Digitally Enabled Phase Shifter Network (DPSN)-depends on a hybrid precoding scheme of *mm*Wave Massive MIMO, which leverages the low-rank property of *mm*Wave Massive MIMO channel matrix and incurs necessary cost and flexibility of transceiver in a marginal loss of control [16]. This issue is common in scheduling and controlling congestion in *mm*Wave multi-hop networks utilizing the Network Utility Maximization (NUM) method. Intrusion is developed on an exact model with two models: real intrusion, along with a graph-based Signal to Intrusion plus Noise Ratio measurement subjected to complex relation operation and position [17], in addition to these upper and lower limits derived by worst-case intrusion and Interference-Free (IF) estimate.

Models and studies have multiple implications [18]: 1) for detailed parameter settings, *mm*Wave systems are more significantly noise-limited than sub-6 GHz; 2) initial exposure is far more complicated in *mm*Wave; 3) self-backhauling is more feasible than sub-6 GHz systems, which allow ultra-dense implementations more viable. . However, it contributes to progressively intrusion-limited behavior; and 4) under direct comparison with sub-6-GHz wireless networks, operators may support each other by exchanging their spectrum licenses if the free conflict comes from this. In conclusion, the studies describe many significant extensions leading to the baseline model, several of which open the door for future research avenues [19].

2 Related Works

The range of disjoint paths in D2D networks becomes more complicated since the disjointed nodes affect their transmission ranges. When two routes could not disjoint the broadcast-range-overlap, the same eavesdropper will intercept communication in either direction. A privacy-aware 2-factor authentication protocol [20,21] based on ECC is suggested for WSNs. This latest protocol fulfills numerous security procedures required for implementations in real-life environments while retaining practical effectiveness. They presented that the newest protocol achieves the Burrows–Abadi–Needham basis of shared authentication.

Regarding system usability, the design architecture also helps data processing and management [22]. They often compare the edge and core computing regarding the hypervisor form, virtualization, stability, and heterogeneity of the node by directing the complexity of nodes at the edge or center of 5G and self-important security issues and possible methods of attacks on the shared data in the 5G network between various devices.

A modern, secure, Time-Key-based, Single Sign-On (TK-SSO) key management protocol aims [23] at mobile devices by applying ECC. Thus, this helps one to obtain desired security properties, besides significantly lesser computation and connectivity. TK-SSO also allows device consumer and application revocations. They proved TK-SSO's security in a commonly agreed intruder real-or-random model. Also, TK-SSO uses Automated Validation of Internet Security

Protocols and Applications (AVISPA) and Burrows-Abadi-Needham logic (BAN) method to validate the TK-SSO withstand several known attacks.

For Femtocell Users (FUs) [24], they suggested a combined channel distribution and energy-aware algorithm using cerebral non-orthogonal multiple Access Radio. The aim is to optimize the FU's volume of secure QoS policy. Cognitive Radio Non-Orthogonal Multiple Access (CR-NOMA) is used by the Femto Base Station (FBS) to maintain QoS for FUs.

The motivation for recent cellular mmWave technologies, intruder detection methods, and equipment give a range of test findings demonstrating 28–38 GHz frequencies [25] by utilizing steerable directional antennas in the BS and portable devices. The author [26] recommended a probabilistic model for characterizing the beam distribution and the possibility of convergence in automotive *mm*Wave networks. The aim is to demonstrate several dynamic and well-formed trade-offs that need to be addressed while improving vehicle scenario resolutions depending on *mm*Wave networks. The traditional problem is dealing with the network's mobility and managing protocols in single and multi-hop infrastructure. This network mobility should give global connectivity to the user without interrupting ongoing processes. Solving this primary issue needs to go for a better delivery ratio through mmWave networks in 5G.

2.1 Relevant Methods

For many years, MANET has demanded the focus of many research studies. Several routing protocols for MANET have been recommended, and the ones discussed in this work were ubiquitous. It is also important in this network to ensure connection setup and network stability and provide appropriate data transmission protocols. The design of routes for achieving Ergodic Rate Density (ERD) in every routing path has been verified [27]. However, ERD is also considered as an upper bound, which achieved specific sub-optimal and other real-world protocols.

An energy-efficient routing protocol integrates an ACO algorithm into it, naming it as ant-swarm inspired Energy-Efficient Ad Hoc On-Demand Routing protocol CO-EEAODR. This weighs the remaining energy level and path length before choosing the most energy-efficient route. Because of the energy efficiency goals within this procedure, the first criteria load is set at 0.71. In comparison, pheromone-value changes in every node focused on the remaining energy level. An ant chooses to move a node by advanced energy relatively lesser than the shortest routing path.

Eavesdropping includes an attacker's successful attention to data exchange that can take various forms based upon the nature of an intruder's data and capacities. The author states that the relay node is viewed as an eavesdropper [28] in a relay scenario, in addition to 5G Device-to-Device (D2D) communication contact in which data is protected even if it is necessary for transmission [29].

Multipath routing is an important and challenging issue in wireless networks [30]. They assume that the route discovery requirements differ between wired and wireless networks due to common unauthorized access and probability. Not only do nodes utilize bandwidth with their connections, but they also interact with nodes nearby [31].

Interflow intrusion happens when two sections of the same flow try to utilize the same channel simultaneously [32]. It is difficult to detect and measure intrusion while counting the output of paths since the connection uses both the routes and the network link can exert intrusion on its neighborhood using the relationship. This provides a survey about the MANET integrated with 5G. That provides more views of about 20 proposals towards discovery-based mobility

management solutions. In that, optimized link-state routing and BATMAN protocol [33] provides the best outcome towards the integrated network.

2.2 Summarization of Our Proposed Work

1) For each case, we list various well-known and newly recommended channel models and equivalent path propagation loss, and expected energy is established.

2) They analyze the impact of several *mm*Wave channel models (for different circumstances) tested in recent years on the output of specific well-known MANET routing protocols through the literature (delivery speed, error rate, energy efficiency, etc.,)

3) The analysis shows that using *mm*Wave frequency bands (e.g., 28 GHz) for MANET standard routing protocols will.

4) The architecture and study of 5G *mm*Wave beamformed cell exploration for remote networks has been stated in part.

5) The data transmission multi-hop routing in 5G *mm*Wave V2X networks has been partially released.

This emerges from observations, and its feasibility relies on the application of Fuzzy logic, and ACO seems to improve MANET health. Nonetheless, it is essential to select suitable parameters [34] involved in the fuzzy framework. The option may be profoundly affected by the protocol's design goals and even linked to the designer's viewpoints. For, e.g., a practice typically permits the rule base used for a complicated structure to affect performance results. More attention is mandatory in this field, addressing or examining such accessible issues. Authentication backgrounds are an essential function that is used to reduce wireless networks' security. Such a framework was executed by 80% of trust-based models in this segment.

As can be shown, the transmission ratio and also the number of packets transmitted in the simulator during network research are much higher and more reliable for the rural and industrial *mm*Wave networks than standard Wi-Fi networks. This indicates the immense capacity that *mm*Wave has for short-range communications as predictable in the Ultra-Dense Networks (UDN). There are various research investigations ongoing to discover the drawbacks and characteristics of mmWave in the MANET domain that must be performed in this area. In addition to the transmission rate and the lack of propagation, the impact of Broad bandwidth (which *mm*Wave offers as a feature) on energy-driven device's longevity and network capacity (especially in the catastrophic regions) is also significant [35] to be studied. The final step in this analysis of *mm*Wave in MANET impacts the packet distribution ratio of the transmission range. It is said that increased energy minimizes route loss due to intrusion for transmitting wireless networks. Still, less energy is more than enough for *mm*Wave's directional beams to perform the same.

We specified the issues of optimizing a feasible data rate for *mm*Wave HetNets, seeing both uplink and downlink connection, and connectivity link transmissions. We also suggested a resource allocation algorithm and hybrid scheduling, consisting of the maximal independent set scheduling algorithm, equal, fair slot allocation algorithm, and even the water-filling space allocation algorithm to effectively address the maximization problem [36]. In addition to this, a hybrid routing algorithm using the path discovery algorithm is discovered; further, this algorithm increases the data rate obtained via the process of shared scheduling and allocation of resources with predefined static routes [37].

It is exposed that, both with and without a dynamic routing algorithm, the suggested combined scheduling and resource allocation algorithm outperforms the benchmark schemes concerning feasible data rate and reaches theoretical equilibrium so far from lower latency [38]. Also, the proposed algorithms enable versatile uplink, and downlink slot allocation to be modified, endorses half-duplex and full-duplex modes by significant performance improvements. Specifically, the proposed protocols can achieve different efficiency criteria with point-to-multipoint communications and point-to-point communications through specific importance on data transmission in the vehicle group examined by 5G standardization organizations and testing activities [39].

3 System Model of OFACA-5G in MANET

Motivated through additional ACO routing processes, a-security-aware, fuzzy enriched ant colony routing optimization protocol is proposed in MANETs. The goal is for an expanding MANET routing protocol that could provide a guaranteed packet transmission ratio, less overhead connectivity, and low end-to-end latency in shared standard scenarios and attack states. As a routing protocol for MANETs, an Optimized Fuzzy-based Ant Colony Algorithm for 5G (OFACA-5G) must, therefore, guarantee both efficiency and security because ANT proves effective outcomes with hybrid architecture and verified to be supplementarily effective than the additional state-of-the-art routing protocols of MANETs, like AODV, its routing organization implemented through OFACA-5G.

3.1 Route Setup in OFACA-5G

To relate the ACO system to routing in MANETs, it is essential for viewing the network as a graph. Ants only move beside edges of the table, reflecting contact relations between active nodes in the network. Node **S** emits sensitive FANTs to find a route [37]. The likelihood of a reactive Path starting node *'i'* for pick node *'j'* is the next-hop stated in Eq. (1).

$$P_{ij}^{d}(t) = \left[\tau_{ij}^{d}(t).R_{ij}(t)]^{\alpha} / \sum_{l \in N_i^d} .R_{il}(t) \right]^{\alpha}, \quad \forall j \in N_i^d. \tag{1}$$

3.2 Reactive Route Setup in OFACA-5G

The sensitive Forward ANT (FANT) is one or the other unicast or transmitted at every intermediate node, as exposed in Fig. 1, such that the present node has routing discovery details for the destination node. Whereas intermediate nodes first forward duplicate only, every obtained ant to limit overhead is incurred by transmitting ants. Reactive hop FANT moves to the destination node, or it reaches ANT at maximum travel hop count. According to this, the FANT selects one of its neighboring nodes for each move.

It transforms into a Backward ANT (BANT), and afterward, the ant reaches the destination node and returns to the source node almost in the same path. The BANT changes the count for every intermediate node by applying the last hop's count, and it reflects the cost of packet distribution on starting node 'i' to node d beside the path. The sum of behaviour is kept informed to the transmission link since it depends on the active route in this link and the rate of desertion of the behaviour as presented in Eq. (2). An ant treats the efficiency of the path as quantity inversely comparative to the routing cost.

$$\tau_{ij}^{new} = \rho.\tau_{ij}^{old} + (1-\rho).\frac{1}{C_{id}} \tag{2}$$

r_{ij}^{old} is the previous reasonable behavior percentage of node 'i' link and is modified standard behavior percentage with the node *'i'* connection, and *'j'* is the rate of evaporation of pheromones. In the tests, p set to 0.7, which is identical to ANT. Meanwhile, the cumulative cost is incurred for directing a packet node *'i'* to node *'d'* beside this path; thus, node A → B are adjacent to two nodes in this particular route), whereas the rate of directing a data packet from nodes A → B → D is well-defined.

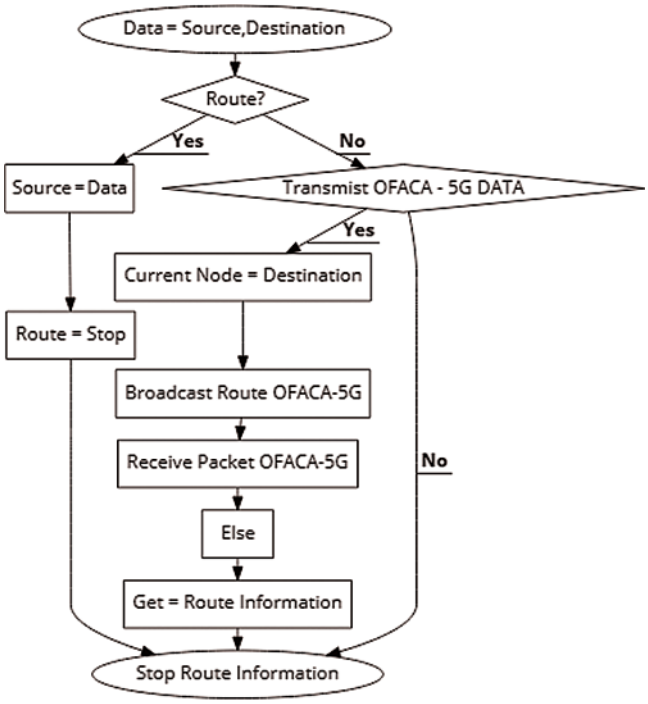

Figure 1: The flow of route set-up process

3.3 Route Maintenance in OFACA-5G

A proactive route discovery method consisting of dynamic behavior and distribution ant sampling is proposed in OFACA-5G to improve routing performance.

Proactive Ant Sampling

Core nodes sent out constructive forward ants periodically in the dynamic ant sampling cycle to collect routing details for ongoing data sessions. In this test, positive forward ants are focused during each second data session [38]. The Proactive forward ant's source likelihood rule is well-defined in Eq. (3) to decide their next step.

$$P_{ij}^{d}(t) = \max\left[\frac{\tau_{ij}^{d}, \omega_{il}^{d}(t).R_{ij}(t))^{\alpha}}{\sum_{l\in N_t^d}(\max[\tau_{il(t).}^{d}\omega_{il}^{d}(t)}\right].R_{ij}(t)^{\alpha}.\forall j \in N_i^d \tag{3}$$

This rule is similar to that defined in Eq. (1). The α in Eq. (3) is set to 3 in the tests. Once forward ant becomes proactive, ant enters their target node to transform forward ant into passive backward ant with similar reactive backward ant's behavior. On the way back to its source node, forwards ANT changes common—behavior values.

3.4 Data Transmission in OFACA-5G

Hop-by-hop, the data packets are forwarded to the target node after path initialization. Each hop then creates the routing choice to send data packets to the following path. Another thing is that routing decisions find regular behavior. In OFACA-5G, nodes forward data packets—random distribution depending upon varieties in standard behavior percentage stored for the proposed destination node in the—behavior table.

3.5 Malicious Behavior in OFACA-5G

This section describes the suspicious behavior detection method in addition to its primary routing method and describes the MANET's intrusion detection.

4 Fuzzy Logic Dependent Misbehavior Detection Model in MANETs

In this research, the initial set of studies was focused on MANETs. These tests' objective is to secure the network from Sybil attacks and the black hole. There are much more data around those two attacks. The described intrusion detection system is described in this section. The new packet transmission and the forward rate were provided as input values to the intrusion detection system, whereas reliability is the outcome.

4.1 Fuzzy Input

Suppose a node transfers the packet in advance through another node; the transmitting node must continue to listen on the wireless channel to verify whether the receiving node is currently forwarding the packet inside a sec. In this method, only the latest 30 packets are investigated for sniffing connection. The PDR packets sent through the node represents the forward hop. These levels are SMALL/MID/HIGH in the Fuzzy system. Fuzzy logic controls the routing policies and dynamically boost controls the routing policies. From this input value, the membership function is applied in Fig. 2. The Fuzzy framework's subsequent input is a new transmission labeled as the number of packets transferred for forwarding to the assumed node, irrespective of whether it was acknowledged. The process of obtaining—fresh inputs as of the selected input variables and measuring the degree of the data belong to every respective fuzzy set is called Fuzzification. As the packets are distributed from the last 30 s, this will control a maximum of 30 packets as defined in the forward data rate.

4.2 Fuzzy Output

The fuzzy logic element accomplishes fuzzy inference over two input values, and it creates reliability of the output value. The combined output of the fuzzy set is assumed as input in this step, and a single—new number produces output. This outcome value is either be "Highly Unreliable," "Unreliable," "Neutral," or "Reliable" in membership function—this output value is used to make decisions about the routing process.

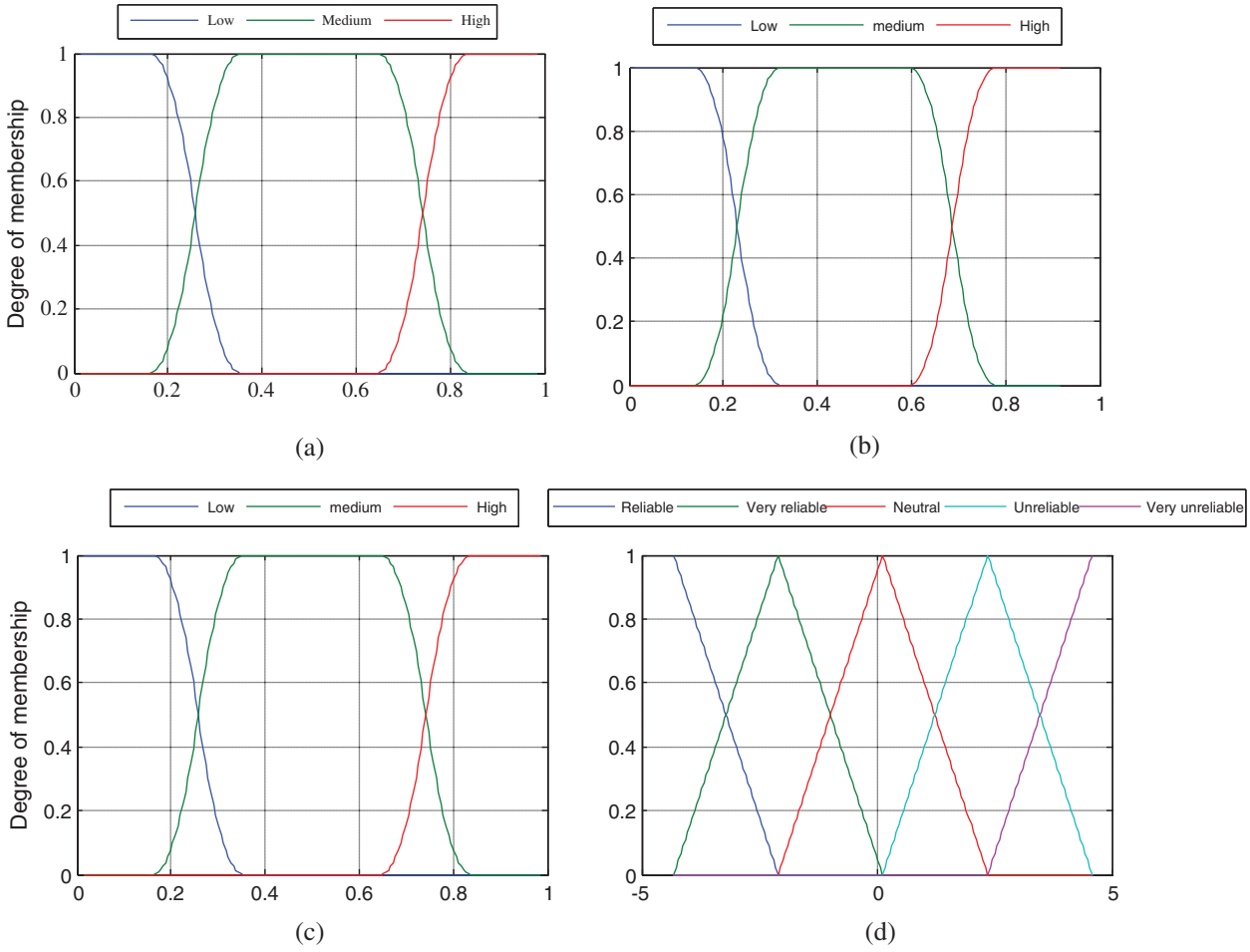

Figure 2: Experimental set-up of fuzzy based OFACA-5G in MANET

4.3 Fuzzy Rules

Rule 1: If the forward rate and current transmission are less, it is supposed that reliability is neutral, as minor is identified about node behavior. The node is classified as very weak if the latest communication is low [37].

Rule 2: If forward performance is average, then every recent value of the low, medium and high transmission leads to stable, neutral, and inaccurate reliability values.

Rule 3: Eventually, the node is accurate when the new transmission is low, and the forward rate is high. It is understood that the node is exact for new transmission values of low and high.

4.4 Fuzzy Inference System Rules

OFACA-5G improves ANT through a centralized suspicious activity detection system focused on a traffic monitoring system based on Fuzzy logic. Meanwhile, the network's traffic monitoring within the network has no additional control packets present in the routing protocol, unlike the intrusion detection system. In MANET tests, each node paths every neighboring node's

activities. It transfers the new parameters, namely the forward rate and the number of new packets forwarded, through its fuzzy inferential device. In this experiment, the reliable threshold value was originated at 0:12. Whereas all nodes with reliability rates lesser than the threshold are considered unreliable, they would not select proactive or reactive forward ants. In this event, a node has only behavior rates to unstable nodes. The node sent new and sensitive forward ants to determine new possible routes that may lead to additional overhead.5 Model of mmWave Routing Algorithm for MANET

Remote ad hoc networks made up of more UE are accomplished by directly sending and receiving through one another without network infrastructure. The network is accepted to have (n) UE at some moment. There will be a definite number of receivers and transmitters to share data packets through network service at particular times. The primary motive of this antenna is to gain directionality with performance, and reports various channel models.

5 MANET Routing

5.1 Differences from Traditional MANET Routing Algorithms

We analyzed specific channel models recommended through [9] 3GPP to affect efficiency through several renowned MANET routing protocols. To recognize improvement in performance among traditional Wi-Fi and *mm*Wave networks, we must first elucidate the following:

1) Wi-Fi devices broadcast wireless signals and cover more extensive distances in all ways. Thus, *mm*Wave devices transmit only narrow beams through specific directions and include smaller ranges.

2) The Friis equation defines route Loss of Wi-Fi signal propagation.

If we use similar path loss of *mm*Wave UE and proceeds, T_x gain reflections

Where n represents the Path Loss Exponent (PLE), and a single model parameter, with 10 *n* performance path loss in *dB* in relations with times of spaces starting at 1 *m*, whereas d is separate space between receiver and transmitter nodes, SF is a standard deviation that defines wide signal variations over mean path loss with space, and loss of Free Space Path Loss (FSPL) (f, 1, m) signifies free path loss *i*. The FSPL might also be designated as: such that *c* is the speed of light.

While this is valid only for omnidirectional antennas, Fig. 3 shows that the use of beam-forming and directional antennas has a much-reduced path loss than comparable short-distance Wi-Fi devices. Thus, these proofs suggest the UE in MANET, which uses Wi-Fi frequencies, to transfer messages to root nodes that signify more loss in propagation. Compared, the UE with *mm*Wave tends to transmit signals to closer nodes and narrow beams of significant directional gains that mean lesser distribution loss. The reduced transmission loss of UEs with *mm*Wave means a well-communicated SNR that leads directly to a better packet delivery ratio.

5.2 Multipath Routing and Security

D2D network security requires other sensitive data and the sharing of keys. As soon as transmitting data through a single path, the attacker has to target only one node through the path. Having several disjoint routes to transfer data means an intruder needs to focus on the number of nodes. Multipath routing protocols may depend upon the theory of max-flow/min-cut. The maximum number of disjoint paths among source **S** and destination **D** is proportional to min-cut among **S** and **D**.

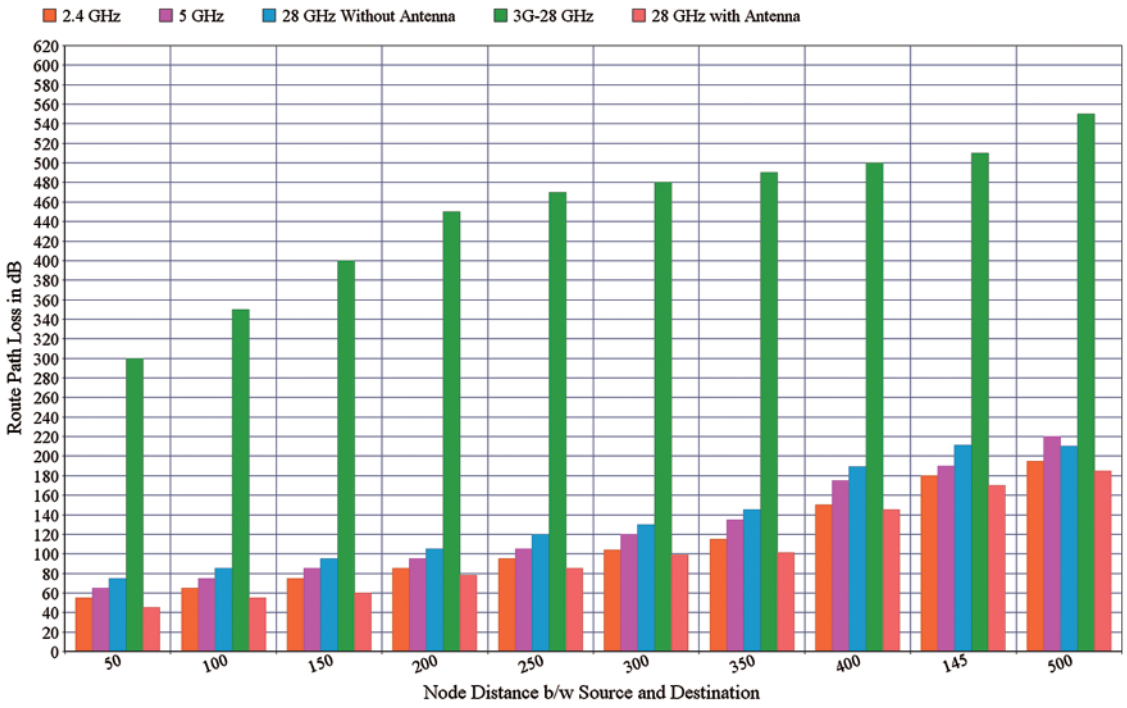

Figure 3: Route path loss *vs.* route models *vs.* route distance

5.2.1 Methodology City Section Mobility Model

They implement node mobility by using the City Section Mobility Framework. Many multi-path routing approaches are proposed in the sense of cognitive radio and wireless sensor networks. Multipath routing and cryptographic methods don't exclude each other. Throughout combination, they can be used to provide greater security.

5.2.2 Transmission Radius and Eavesdropping Rate

In our simulation, the nodes can link a communication range with other nodes. They separate two nodes, the root node where the message is created and the destination node where the message is ended. During the simulation, we mark all relay nodes as eavesdropping nodes.

5.2.3 Transmission Radius and Eavesdropping Rate

For selecting a path from multipath, we proposed a well-known Path selection algorithm. Our simulations equate towards results when using multipath routing, but there is no account of security features of selecting -intruders-aware routes in the following algorithm.

5.2.4 Algorithm 1: Optimized Multi-Path Selection Algorithm

Step 1 Input: Link graph G (V, E)

Step 2 Output: The optimal path ψ

Step 3 Initialization: $V_t = \{\}, V_n = \{\}, V_C = \{s\}, w(v) = \infty, \forall_v \in V/s$

Step 4 Start

Step 5 While $V_t \neq V$ do

Step 6 For Each $v \in V_c$, do

Step 7 Each $u \in V/V_t$ that is neighbor of v *Do*

Step 8 If w (u) $= \infty$ OR w(u) = min {W_{v-u}, W(v)} then

$w(u) = \min\{w_{v-u}, w(v)\}$

$P(u) = P(u)\, U\, \{v\}$

$V_n = V_n U \{u\}$

Step 9 Else If w(u) < min {min w_{v-u}, w(v)} Then

Empty P(u)

$P(u) = \{u\}; V_n = V_n U \{u\}$

Else, Continue

Step 10 End

Empty $V_c \rightarrow V_c = V_n$

Empty V_n

Step 11 End

Return

The optimal path $\psi : s \rightarrow \ldots \rightarrow P(P(d)) \rightarrow P(d) \rightarrow d$

Step 12 End

6 Result and Discussions

Tab. 1 displays the eavesdropping levels for every method in an overly dangerous world. Each transmission node is a -malicious eavesdropper, with varying radii and node size. The Multipath Route algorithm has less eavesdropping rate in every case, though there is no situation where eavesdropping is removed entirely. This algorithm results in a 28% eavesdropping rate in many networks with an effective transmission radius, affecting an 11% rate with a smaller range. It is known that except in two instances, the incidence of eavesdropping decreases as the distance rises.

Table 1: Table caption

Algorithm type	Routing distance		
	700 m	1200 m	1700 m
I	0.41	0.34	0.19
II	0.36	0.54	0.42
III	0.59	0.61	0.45

6.1 MANET Scenarios

To investigate the activity of OFACA-5G in particular, multiple tests are conducted based on different scenarios. The maximal node speed and amount of CBR sessions vary for black hole attack scenarios in the experiments. In the Sybil attack situations, the number of Sybil nodes occurs over the network, and the number of Sybil identities per Sybil node will differ. Tab. 2 outlines different investigative series conducted in MANET scenarios.

Table 2: Experiments of OFACA-5G

Series	Attacks	
	Black hole	Sybil
I	Varying node speed 10–50 m/s	Varying sybil nodes 1–10
II	Varying CBR 10–50	Varying sybil identities 1–10

6.2 Performance Evaluation Metrics

The routing algorithms through sub-6GHz and *mm*Wave algorithms are labeled below:

1) Number of Packets Diffused (NPD)

2) Packet Delivery Ratio (PDR)

3) Average Delivery Ratio (ADR)

6.3 Performance Evaluation

The purpose of this research is to examine the viability of routing protocols in *mm*Wave MANETs and then equate their efficiency for different network settings with the standard routing protocols in MANET. The newly developed module for *mm*Wave in (NS-3) is primarily used for simulation specified in Tab. 3. The module offers various *mm*Wave channel models extracted from multiple dimension campaigns recently undertaken through different eco-friendly conditions and unique places.

Table 3: Simulation scenario parameters

Content	Parameters
Simulator	NS-3
Simulation test period	500 s
Area	1600 × 1600
No. of nodes	100
Node speed	25 *m/s*
Model	Random way
Data rate	1.5–5 *Mbps*
Tx power	10–50 *dBm*
No. of Tx nodes	15
No. of Rx nodes	15

On another side, the packets are moved through similar routing protocols using *mm*Wave frequencies. Also, it is evident that when utilized with *mm*Wave, it provides excellent reliability and delivery ratio than sub-6GHz rates.

The final step in our *mm*Wave investigation in MANET impacts the distribution ratio of transmitting capacity. It is well understood that increased energy could minimize route loss due to attenuation and intruders for sending wireless networks. Still, less energy should be enough for *mm*Wave's directional beams to do the same. So, we analyzed the result of increasing UE's T_x capacity on data packet transmission rate for specific routing protocols in MANETs. The results uncovered in Fig. 4 are expected, which means that mmWave performs better than regular Wi-Fi frequency. According to the recent Federal Communication Commission (FCC), the maximum UE EIRP is 42 *dBm* (nearly 20 *watts*). We therefore, analyzed the effects of an aggregate of the EU's Tx capacity on data packet transmission rate for various routing protocols in ad-hoc *n* networks and outcomes referred.

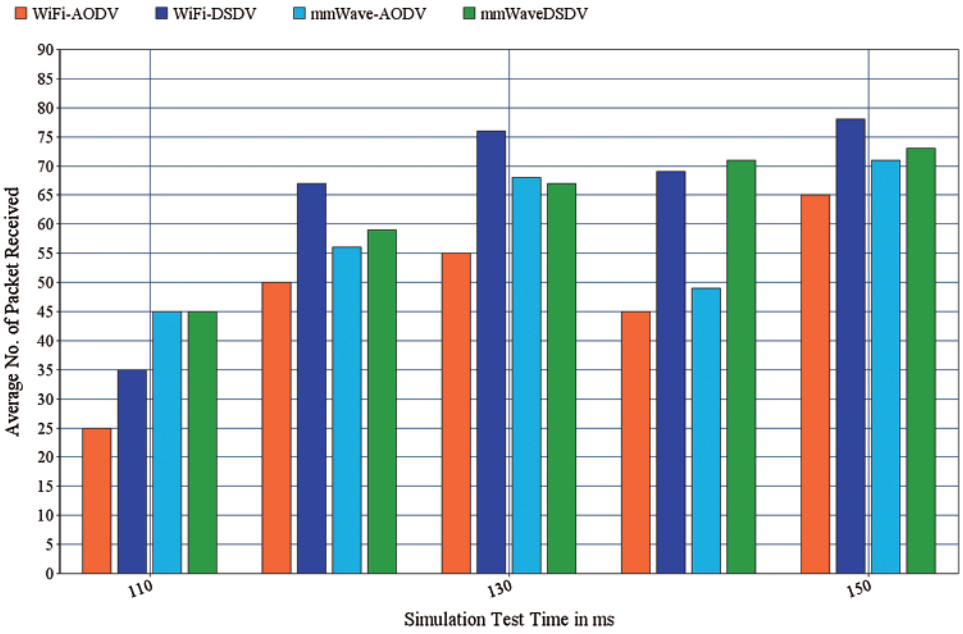

Figure 4: Average packet delivery of Wi-Fi *vs. mm*Wave

6.4 Presentation Beneath Black Hole Attacks

Creation with the simple scenario labeled in this section, the nodes' maximum speed ranges in 5 *ms* steps from 5–30 *ms*. Since the aim is to test OFACA-5G's output in both conventional and complex settings, OFACA-5G is pretending in three types of states: no black hole attacks, two continuous black hole nodes, and one ongoing black hole node. ANT is both selected in different scenarios for contrast. It triggers a lower PDR. Due to buffer time through intermediate nodes, the recovered data packets also cause a more significant delay.

Fig. 5 anticipated the OFACA-5 G and ANT PDR simulation outcomes when maximal node speed decreases. For the efficiency comparison, AODV without attacks is given as a secure attribute. This situation displays that ANT is the best PDR performance in states with no attacks;

OFACA-5G outperforms AODV. If there are any black hole nodes in the network, then ANT will fail more than the other two protocols, and OFACA-5G will turn out to be the best solution. Although a substantial decrease in output triggered through a black hole is referred to in all three protocols, the number of black hole nodes present in the network raises. ANT with an average PDR drop of 41:8% loses more, while OFACA-5G performs the best with a 7:0% drop. In comparison, when focusing on differing node sizes, OFACA-5G's PDR stays at the same standard, and above all other solutions are under consideration in all black hole attack scenarios.

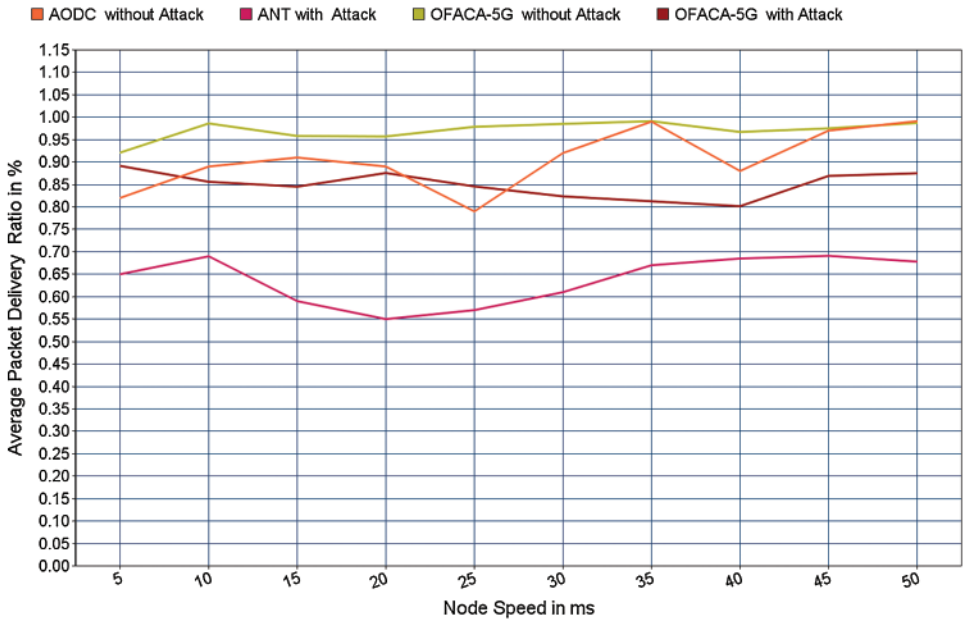

Figure 5: Average PDR with/without attack

Overall, OFACA-5G's PDR is resilient and more stable for attacks. It shows an average overhead of packets and bytes on behalf of all protocols nominated. Deviations are respectively: 8:4% and 7:6%. Relatively, AODV and ANT's latency can be assumed to continue at some point as node speed increases. It shows that the AODV routing approach is outperforming the ACO-based routing methods. However, ANT has a minor delay, especially under blackhole attacks; it is mostly an object of how the delay is measured in tests. The delay is started by dropped packets, which are not reproduced. Fig. 6 reveals which attacks of black hole ANT lose the most data packets. When several black hole nodes within the network grow, the protocol latency parameter decreases. One potential reason for this behaviour is which expired packets are not observed through delay measurement. It demonstrates that the Black Hole attacks in ANT-2BH and OFACA-5G-2BH are causing different packs to decrease. Hence, all protocols achieve better average latency. Looking at OFACA-5G's calculations as speed rises reveal that the latency increases slightly as pace increases. In all estimated situations, the latency of simple ANT is significantly higher than OFACA-5G.

It shows that more black hole nodes give the network more harmful effects. Unlike ANT, a second black hole node's impact is highly prominent; OFACA-5G's robustness just slightly decreases with two black hole nodes. ANT does not contain a precise defence method compared to black hole attacks, so lower power values than OFACA-5G are appropriate for it to have. When node speed is high, its solidity is no better than ANT's robustness, and in some situations, it is

even worse. OFACA-5G's robustness is not significantly affected by rising node speeds. The output of OFACA-5G's at a similar level with ANT is consistently overhead through both black hole nodes. From this point, OFACA-5G is the best solution for securing the network from attacks through the black hole.

Figure 6: Average signal strength

6.5 Performance Under Sybil Attacks

This segment describes OFACA-5G's success under Sybil assaults. Sybil nodes alter their uniqueness and do not have a destructive effect on routing efficiency. Thus, black hole intrusions [38] are involved in the operation. Sybil attack is applied in subsequent attacks through embedded black hole assaults unless it is not stated differently. In principle, this type of outbreak on Sybil is essentially a variation of black hole attacks. It can also provide further chances for malicious nodes to target the network. For instance, if the systematic nodes identify the first identity, the Sybil node will be unique to another new individuality in the network. The corresponding nodes must accept that identity as a new node.

The different experiments' simulation findings demonstrate that OFACA-5G fits well into specific MANET environments and permits effective routing high PDR and small or equivalent end-to-end latency and overhead. This study examined the effectiveness of some well-known routing protocols for *mmWave* frequency bands for MANETs [39]. This study demonstrated how *mm*Wave frequencies would improve the network capacity and transmission ratio. Many network parameters were modified, and the MANET with *mm*Wave is vulnerable to Wi-Fi equivalent in each situation.

Security is a dynamic review in 5G networks and exciting due to cellular and 5G networks' private attributes; these methods vary from security against similar attacks on cable and other networks. Due to this open design and system collaboration, eavesdropping is an ongoing problem. Jamming restricts device access to limited space on the network. The communication moves to

different channels, preferably because a jammer cannot track it. The first user simulation attack is a denial-of-service attack that is mainly vulnerable to 5G networks. It is observed that while increasing mobile device broadcast range improves potential eavesdropping and increases node density. It mitigates the issue by providing additional feasible routes.

7 Conclusion

In this proposed work, OFACA-5G introduced a MANETs routing protocol focusing on security-aware fuzzy logic and improved ant colony optimization with the hybrid routing solution by ANT. It uses a distributed fuzzy logic detection modelstructure to avoid suspicious or malicious nodes since the routing. The ACO algorithm and Fuzzy logic-based detection model are implemented. This detection model strongly analyses nodes' lack of network traffic information and has built-in strong fault tolerance to minimize false identification. The fuzzy reliability attribute is constantly modified, but regular nodes' false identification like malicious nodes reasonably need a chance to show trustworthiness through secure data packets forwarding. To validate outcomes, simulation using the NS-3 (Network Simulator), which provides simulation results towards discrete-event network and mmWave module, is deployed for virtual reality towards broadband, transport systems, etc.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Konak, G. E. Buchert and J. Juro, "A flocking-based approach to maintain connectivity in mobile wireless ad hoc networks," *Applied Soft Computing*, vol. 13, no. 2, pp. 1284–1291, 2013.

[2] B. Krishnamachari, S. B. Wicker and R. Bejar, "Phase transition phenomena in wireless ad hoc networks," in *IEEE Global Communications Conf.*, vol. 5, pp. 2921–2925, 2001.

[3] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng *et al.,* "Device-to-device communications underlaying cellular networks," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3541–3551, 2013.

[4] S. Sudhakar and S. Chenthur Pandian, "Investigation of attribute aided data aggregation over dynamic routing in wireless sensor," *Journal of Engineering Science and Technology*, vol. 10, no. 11, pp. 1465–1476, 2015.

[5] D. Martens, M. De Backer, R. Haesen, J. Vanthienen, M. Snoeck *et al.,* "Classification with ant colony optimization," *IEEE Transactions on Evolutionary Computation*, vol. 11, no. 5, pp. 651–665, 2007.

[6] G. Nardini, G. Stea and A. Virdis, "A fast and reliable broadcast service for LTE-advanced exploiting multihop device-to-device transmissions," *Future Internet*, vol. 9, no. 4, pp. 89, 2017.

[7] H. Hamann and T. Schmickl, "Modelling the swarm: Analysing biological and engineered swarm systems," *Mathematical and Computer Modelling of Dynamical Systems*, vol. 18, no. 1, pp. 1–12, 2012.

[8] H. Zhang, N. Liu, X. Chu, K. Long, A. H. Aghvami *et al.,* "Network slicing based 5G and future mobile networks: Mobility resource management and challenges," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 138–145, 2017.

[9] S. Sudhakar and S. Chenthur Pandian, "Authorized node detection and accuracy in position-based information for MANET," *European Journal of Scientific Research*, vol. 70, no. 2, pp. 253–265, 2012.

[10] H. Zhang, A. Bochem, X. Sun and D. Hogrefe, "A security aware fuzzy enhanced ant colony optimization routing in mobile ad hoc networks," in *14th Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Limassol, Cyprus, pp. 1–6, 2018.

[11] J. Harri, C. Bonnet and F. Filali, "Kinetic mobility management applied to vehicular ad hoc network protocols," *Computer Communications*, vol. 31, no. 12, pp. 2907–2924, 2008.

[12] J. Li, X. Li, Y. Gao, Y. Gao and R. Zhang, "Dynamic cloudlet-assisted energy-saving routing mechanism for mobile ad Hoc networks," *IEEE Access*, vol. 5, pp. 20908–20920, 2017.

[13] J. Liu, N. Kato, J. Ma and N. Kadowaki, "Device-to-device communication in LTE-advanced networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 1923–1940, 2015.

[14] N. Keerthana, V. Viji and S. Sudhakar, "A novel method for multi-dimensional cluster to identify the malicious users on online social networks," *Journal of Engineering Science and Technology*, vol. 15, no. 6, pp. 4107–4122, 2020.

[15] J. P. Barbin, M. Taghipoor and V. Hosseini, "A novel algorithm for manets using ant colony," *International Journal of Computer Science Issues*, vol. 9, no. 1, pp. 109–113, 2012.

[16] S. Sudhakar and S. Chenthur Pandian, "A trust and co-operative nodes with affects of malicious attacks and measure the performance degradation on geographic aided routing in mobile ad hoc network," *Life Science Journal*, vol. 10, no. 4s, pp. 158–163, 2013.

[17] S. Krishna, "Path reliability of multipath routing in MANET," *International Journal of Science and Research*, vol. 2, no. 6, pp. 137–139, 2013.

[18] S. Sudhakar and S. Chenthur Pandian, "Secure packet encryption and key exchange system in mobile ad hoc network," *Journal of Computer Science*, vol. 8, no. 6, pp. 908–912, 2012.

[19] L. Kumar, "Performance evaluation of ACO based on-demand routing algorithm for mobile ad hoc networks," *International Journal of Engineering Science Technology*, vol. 3, no. 3, pp. 1809–1815, 2011.

[20] L. Dash and M. Khuntia, "Energy-efficient techniques for 5G mobile networks in WSN: A survey," in *Int. Conf. on Computer Science, Engineering and Application*, Gunupur, India, pp. 1–5, 2020.

[21] M. H. Eiza, T. Owens and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETs," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 32–45, 2016.

[22] M. Hussaini, S. A. Nor and A. Ahmad, "Optimal broadcast strategy-based producer mobility support scheme for named data networking," *International Journal of Interactive Mobile Technologies*, vol. 13, no. 4, pp. 4–19, 2019.

[23] S. Sudhakar and S. Chenthur Pandian, "Trustworthy position based routing to mitigate against the malicious attacks to signifies secured data packet using geographic routing protocol in MANET," *WSEAS Transactions on Communications*, vol. 12, no. 11, pp. 584– 603, 2013.

[24] M. Hussaini, S. A. Nor, H. Bello-Salau, H. J. Hadi, A. A. Gumel *et al.,* "Mobility support challenges for the integration of 5G and IoT in named data networking," in *2nd Int. Conf. of the IEEE Nigeria Computer Chapter (NigeriaComputConf)*, Zaria, Nigeria, pp. 1–7, 2019.

[25] M. Mauve, J. Widmer and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE Network*, vol. 15, no. 6, pp. 30–39, 2001.

[26] S. Sudhakar and S. Chenthur Pandian, "An efficient agent-based intrusion detection system for detecting malicious nodes in MANET routing," *International Review on Computers and Software*, vol. 7, no. 6, pp. 3037–3304, 2012.

[27] S. Pankaj, "Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next-generation communication network," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 8, pp. 47–53, 2013.

[28] R. E. Ahmed, "A novel multi-hop routing protocol for D2D communications in 5G," in *IEEE 11th Annual Computing and Communication Workshop and Conf.*, NV, USA, pp. 627–630, 2021.

[29] K. Ganesh Kumar and S. Sudhakar, "Improved network traffic by attacking denial of service to protect resource using Z-Test based 4-Tier geomark traceback (Z4TGT)," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3541–3575, 2020.

[30] R. Olfati-Saber, "Flocking for multi-agent dynamic systems: Algorithms and theory," *IEEE Transactions on Automatic Control*, vol. 51, no. 3, pp. 401–420, 2006.

[31] S. A. Abd, S. S. Manjunath and S. Abdulhayan, "Direct device-to-device communication in 5G networks," in *Int. Conf. on Computation System and Information Technology for Sustainable Solutions*, Bengaluru, India, pp. 216–219, 2016.

[32] S. J. Mirabedini and M. Teshnehlab, "FuzzyAntNet: A novel multi-agent routing algorithm for communications networks," *GESJ: Computer Science and Telecommunications*, vol. 12, no. 1, pp. 45–49, 2007.

[33] S. Misra, S. K. Dhurandher, M. S. Obaidat, P. Gupta, K. Verma *et al.,* "An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks," *Journal of Systems and Software*, vol. 83, no. 11, pp. 2188–2199, 2010.

[34] S. Sethi and S. K. Udgata, "The efficient ant routing protocol for MANET," *International Journal on Computer Science and Engineering*, vol. 2, no. 7, pp. 2414–2420, 2010.

[35] X. Zhu, P. Li, Y. Fang and Y. Wang, "Throughput and delay in cooperative wireless networks with partial infrastructure," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4620–4627, 2009.

[36] Z. Ali and W. Shahzad, "Analysis of routing protocols in AD HOC and sensor wireless networks based on swarm intelligence," *International Journal of Network and Communications*, vol. 3, no. 1, pp. 1–11, 2013.

[37] A. U. Priyadarshni and S. Sudhakar, "Cluster based certificate revocation by cluster head in mobile ad-hoc network," *International Journal of Applied Engineering Research*, vol. 10, no. 20, pp. 16014–16018, 2015.

[38] S. Sudhakar and S. Chenthur Pandian, "Hybrid cluster-based geographical routing protocol to mitigate malicious nodes in mobile ad hoc network," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 21, no. 4, pp. 224–236, 2016.

[39] M. A. mojamed, "Integrating IP mobility management protocols and MANET: A survey," *Future Internet MDPI*, vol. 12, no. 150, pp. 1–22, 2020.