

Clustering And Security Management For Manet Using Artificial Bee Colony Optimization And Rsa Cryptography

B.Somasekhar¹, Srinivas Sabbavarapu², B. Chandra Kiran Patrudu³, Silpa Kesav Velagaleti⁴, Chukka Anoosha⁵, V. Vijaya Kumar Raju⁶

^{1,2,3,5,6} Dept. of ECE, ANITS (A), Visakhapatnam,

⁴Dept. of ECE, CVR College of Engineering(A), Hyderabad.

ABSTRACT

A mobile ad hoc network (MANET) is a collection of wireless mobile devices that form a temporary network without the aid of an infrastructure. This type of network is not only built dynamically, but it also adjusts to constantly changing network settings. Despite the dynamicity, MANET provide additional obstacles for improving network efficiency in large scale networks with large number of nodes. The Cluster Heads (CHs) are nodes that are in charge of cluster formation, network topology management and allocating resources to all nodes in their clusters. Owing to dynamic mobile node nature, the CH configuration is varying constantly. Hence, reducing the number of CH and providing efficient routing in MANET is essential. In that aspect, a clustering based routing protocol called Artificial Bee Colony (ABC) optimization algorithm is introduced to route the mobile nodes in MANET. The nodes in MANET communicate with one another freely and dynamically. However, there is a chance of initiating routing assaults by malicious node to disrupt routing processes. Hence, a safe routing technique called Rivest-Shamir-Adleman encryption (RSA) cryptography is developed to prevent insider attack in network. The proposed ABC algorithm is compared with various other protocols to assess different parameters. Also, the performance metrics of RSA cryptography is analyzed.

Key Words: MANET, Cluster head, Routing, Artificial bee colony, RSA cryptography.

I. INTRODUCTION

A MANET is self-configuring dynamic network made up of wireless mobile nodes that operate independently of any infrastructure. The nodes in MANET communicate with one another freely and dynamically. Battery life, processing speed, connectivity and storage capabilities are all constrained on these nodes. The lack of a central base station in MANET introduces a slew of additional issues and challenges. The energy efficiency is a key need of a MANET that enhances its lifetime [1, 2]. The collection of nodes inside a CH's transmission range is known as its neighborhood. The Cluster Heads (CHs) are nodes that are in charge of cluster formation, network topology management and allocating resources to all nodes in their clusters. Owing to dynamic mobile node nature, the CH configuration is varying constantly. As a result, nodes in MANET are clustered to increase efficiency of the network [3, 4].

MANET provide additional obstacles for improving network efficiency in large scale networks with large number of nodes. The clustering in MANET aims to identify node groups in such a way that the identified groups are exclusive and each instance in the network belongs to just one of them. Also, the communication connection breakdown is common in MANET due to its unique features, which increases routing cost and diminishes network longevity. To overcome all these issues, efficient routing and clustering technique in MANET is necessary. Hence, various optimization algorithms are introduced to minimize the CH issues and provide efficient routing in MANET [5]. A Particle Swarm Optimization (PSO) algorithm is utilized to tackle the mobility and energy efficiency challenges. For selecting nodes to act as CHs for extended periods of time, the election of cluster heads considers remaining energy, degree of connectedness and mobility. However, the node mobility in MANET is not effectively managed [6, 7]. Also, the integration of PSO algorithm with an adaptive K-nearest neighbor algorithm suffers from

energy issues and packet loss. Likewise, the PSO algorithm integrated with Genetic Algorithm (GA) needs to manage energy in mobile nodes to enhance the network lifetime [8, 9]. Hence, GA is introduced to solve the optimization issues in MANET. During routing, it becomes a candidate for determining the best route. Even if data packets are lost at random, these protocols provide an optimization process to select the most efficient paths [10, 11]. However, the technique ignored the random loss that typically happens in wireless communications in networks. Also, when the propagation delay increases, the congestion window steadily enlarge. As the time delay increases, the amount of data transmitted and the throughput eventually decrease [12, 13]. The Grey Wolf Optimizer (GWO) is a generic multi-purpose optimization method that is used to choose the best path. Grey wolf nature forces a faster convergence, resulting in the optimal amount of clusters [14]. However, the accuracy, convergence rate and searching ability of GWO is found to be low [15]. Since, the ACO algorithm reduces the packet delay with low consumption of energy it is widely utilized in MANET. It considers the ability of basic ants to collaborate to solve complicated challenges [16]. Despite the fact that, the ACO algorithm has positive feedback accounting for quick identification of optimal solutions, theoretical analysis is challenging [17, 18]. In addition, MANET is vulnerable to major security risks that are difficult to combat. Because of the open medium and lack of a defined line of defense, security is a critical concern with MANET [19]. When using mobile ad hoc networks in sensitive or hostile areas, security services are required. As a result, a safe routing protocol for MANET with a significant variety of security services at the network layer is essential [20, 21]. By utilizing group key management of asymmetric key cryptography, a safe and energy-efficient routing system is developed. The whole network security is not threatened when nodes other than the proposed keys are hacked. However, malicious activity has made the estimated destination nodes less dependable [22]. An innovative safe authentication technique for MANET communication is developed in which, a symmetric key cryptography is utilized for data encryption. But, the key transportation is a difficulty in symmetric cryptosystems [23]. To manage the security and energy of MANET effectively, a security based data aware routing protocol is developed. Monitoring the cluster members and encrypting and decrypting the model using data gathering algorithm are the 2 stages of the model. However, the energy consumption of the model is not achieved as expected [24]. Hence, trust enhanced cluster based multipath routing algorithm is introduced, which utilizes PSO to form cluster or cluster head. However, routing assaults occurs by the misbehavior of malicious node in the network [25].

In this study, the ABC optimization algorithm is utilized to route the mobile nodes in MANET. Also, a security protocol called RSA cryptography is introduced to overcome the attacks of caused by the misbehavior nodes in network. Finally, the ABC optimization algorithm is compared with other existing protocols in terms of energy consumption, routing average delay, overhead, life time and throughput. Finally, the performance metrics of RSA cryptography is analyzed.

II. BACKGROUND AND MOTIVATION

A Mobile Ad Hoc Network (MANET) is a self-configuring dynamic wireless network composed of mobile nodes that communicate without relying on any centralized infrastructure. The nodes in a MANET operate both as hosts and routers, forwarding packets to neighboring nodes through multi-hop communication. Due to limited battery power, processing capability, storage resources and dynamic topology, maintaining efficient routing and network management becomes a challenging task in MANET environments [26], [27].

Clustering is widely used in MANETs to improve scalability, routing efficiency and network stability. In clustering, the network is divided into groups of nodes known as clusters, where a Cluster Head (CH) is responsible for managing intra-cluster communication, routing coordination and resource allocation among member nodes. Proper cluster formation reduces routing overhead, improves bandwidth utilization and enhances the lifetime of the network [28], [29]. However, due to the dynamic mobility of nodes, cluster heads frequently change, which may degrade network performance and increase routing delay.

To address these challenges, various optimization-based routing approaches have been proposed in recent years. Swarm intelligence algorithms such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), Ant Colony Optimization (ACO) and Grey Wolf Optimization (GWO) have been applied to identify optimal cluster heads and routing paths in MANETs [30]–[31]. PSO-based clustering approaches consider parameters such as residual energy, node mobility and connectivity degree for cluster head election, but they often suffer from slow convergence and instability under high mobility conditions [32]. Hybrid PSO–GA approaches attempt to improve routing efficiency; however, they still face challenges in balancing energy consumption and packet loss during dynamic topology changes [33].

Similarly, Grey Wolf Optimizer (GWO) and Ant Colony Optimization (ACO) algorithms have been employed to improve route discovery and packet forwarding in MANET environments [34], [35]. Although these algorithms demonstrate promising optimization capability, they often experience issues such as premature convergence, increased computational complexity and unstable routing paths under large-scale network scenarios [36].

Recently, Artificial Bee Colony (ABC) optimization has gained significant attention in wireless networking due to its efficient exploration and exploitation mechanisms. The ABC algorithm models the foraging behavior of honeybee swarms to search for optimal solutions in a distributed manner. Compared with other swarm algorithms, ABC provides faster convergence, better global search capability and improved adaptability to dynamic network environments [37], [38]. Therefore, ABC-based routing algorithms are increasingly explored for cluster head selection and route optimization in MANETs.

Despite the advantages of clustering and swarm-based routing, security remains a critical challenge in MANETs. Due to the open wireless medium, decentralized architecture and dynamic topology, MANETs are highly vulnerable to various attacks such as blackhole attacks, wormhole attacks, routing misbehavior and insider attacks [39]. Malicious nodes can disrupt routing processes, degrade network performance and compromise data confidentiality.

To address these issues, secure routing mechanisms based on cryptographic techniques have been proposed. Public key cryptography plays an important role in ensuring authentication, confidentiality and secure key management in wireless networks [40]. Among various asymmetric encryption schemes, the Rivest–Shamir–Adleman (RSA) algorithm is widely used due to its strong security properties and robustness against cryptographic attacks [41]. RSA enables secure communication between nodes by encrypting transmitted data and preventing unauthorized access during routing.

Recent studies have explored the integration of optimization-based routing with cryptographic security mechanisms to improve both network efficiency and protection against malicious attacks in MANET environments [42]–[44]. However, achieving an effective balance between routing efficiency, energy consumption and network security remains a significant research challenge.

Therefore, this study proposes an Artificial Bee Colony (ABC) optimization-based clustering and routing framework integrated with RSA cryptography to enhance both

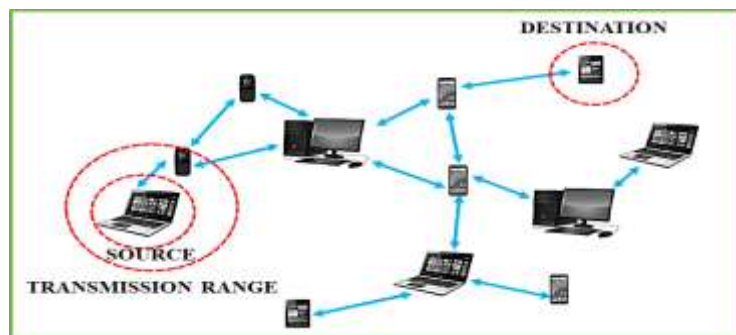
network performance and communication security in MANETs. The ABC algorithm is used to identify optimal routing paths and cluster structures, while RSA encryption is employed to protect data transmission from malicious nodes and insider attacks. The proposed method is evaluated using simulation experiments and compared with existing routing protocols in terms of energy consumption, routing overhead, delay, throughput and network lifetime.

III. PROPOSED METHODOLOGY

A) MANET

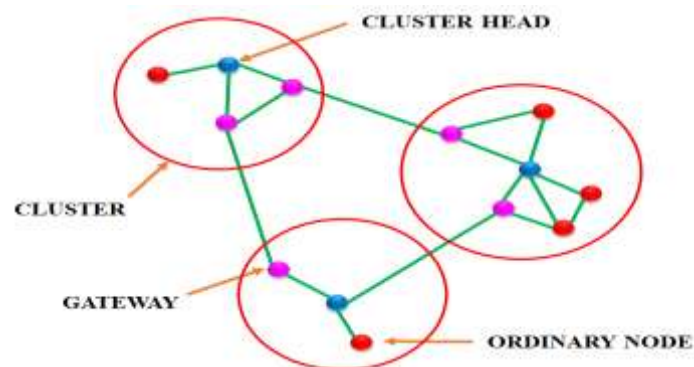
A Mobile Ad-Hoc Network (MANET) is a sort of ad-hoc network that connects a group of mobile nodes. Radio waves allow the mobile nodes to communicate with one another through wireless network. The topology of the network is continually changing due to the randomized mobility of mobile nodes. The storage capacity, battery and processing speed of nodes in the network are all restricted. When the nodes are in a short range they connect directly otherwise, they require the assistance of an intermediary node to route their packets. These networks are completely distributed and they operate without the need for any infrastructure. The architecture of MANET is represented in Fig.1.

Fig.1: MANET Architecture



The nodes in MANET collaborate and interact with one another, with each node acting as a relay as required to accomplish certain services. When a node attempts to communicate data to another node that is beyond the range of communication, the packets has to be routed through 1 or more intermediary nodes. Each mobile node in a MANET is an autonomous node that act as both a router and a host. Since nodes are free to migrate at any moment and at different speeds, the network architecture is altered at any time. The clustering of mobile nodes by MANET is represented in Fig.2.

Fig.2: Clustering in MANET



The MANET nodes construct their own network by dynamically developing routing among themselves as they go around. Any entity with the necessary technology and resources access the wireless communication channel. As a result, channel access cannot be controlled. The communication connection breakdown is common in MANET due to its unique features, which increases routing cost and diminishes network longevity. In addition to this, the network topology in MANET becomes very dynamic as a result of the increased mobility, resulting in network congestion. Hence, ABC optimization is utilized for attaining effective optimization in MANET.

B) ABC Optimization

The ABC algorithm is a relatively recent swarm intelligence algorithm that simulates honey bee swarm foraging behaviour. The colony of artificial bee has 3 types of individuals: onlookers, employed and scouting bees. The employed bees take use of certain food sources and provide valuable data to onlooker bees. The onlooker bees gather data about food sources and based on the quality of that information, it select a food source to utilize. The employed bee that has lost its food supply becomes a scout and begins looking for a new food source. The pseudocode of original ABC algorithm is given below,

ABC Algorithm

Input : Initial population of food sources X_i ($i = 1, 2, \dots, SN$), Maximum number of iterations (MaxIter)	
Output: Best solution Xbest	
1. Initialize the population of food sources X_i randomly 2. Evaluate the nectar amount (fitness) $f(X_i)$ for each food source 3. Assign employed bees to the initialized food sources 4. Iteration = 0 5. while (Iteration < MaxIter) do 6. /* Employed Bee Phase */ 7. for each employed bee i do 8. Generate a new food source V_i in the neighborhood of X_i using Eq. (8) 9. Evaluate fitness $f(V_i)$ 10. if $f(V_i) > f(X_i)$ then 11. $X_i = V_i$ 12. end if 13. end for 14. Compute the selection probability P_i for each food source 15. /* Onlooker Bee Phase */ 16. for each onlooker bee do 17. Select a food source X_i based on probability P_i 18. Generate a new solution V_i in the neighborhood using Eq. (8) 19. Evaluate fitness $f(V_i)$ 20. if $f(V_i) > f(X_i)$ then 21. $X_i = V_i$ 22. end if 23. end for 24. /* Scout Bee Phase */	

25. if any food source exceeds the abandonment limit then
26. Replace it with a randomly generated food source
27. end if

28. Memorize the best solution Xbest obtained so far
29. Iteration = Iteration + 1
30. end while

31. Return the best solution Xbest

The algorithm provides a set of food sources in the initialization phase that is related to the search space solutions. Within the range of the variables' boundaries, food sources are generated randomly.

$$x_{i,j} = x_j^{\min} + \text{rand}(0, 1) (x_j^{\max} - x_j^{\min})$$

(1)

Here, $i = 1, 2, \dots, SN$ and $j = 1, 2, \dots, D$. The number of food source is given by SN and it is half the colony's size. The problem's dimension is denoted by D, which represents the number of parameters to be optimized. The jth parameter's upper and lower bounds are denoted by $x_j^{\max}$ and $x_j^{\min}$ respectively. In this phase, counters that register the number of trials completed by each bee are reset to zero.

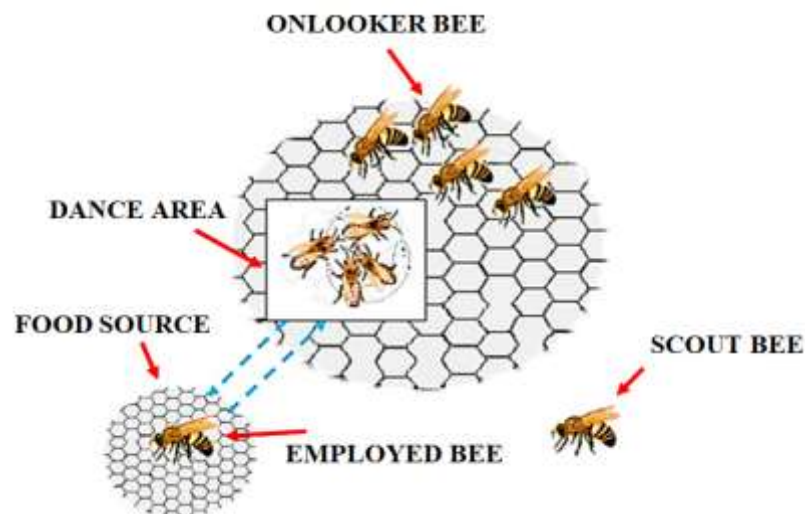
Each employed bee is transported to the food source stored in its memory and discovers a nearby food source during the employed bees phase. According to (2), the nearby food supply is obtained as follows:

$$V_{i,j} = x_{i,j} + \varphi (x_{i,j} - x_{k,j})$$

(2)

Here, k is a randomly chosen food supply that is distinct from its neighbour i and j is a dimension that was chosen randomly. φ is an evenly distributed random number in [1, 1] range. Also, changing 1 dimension on x determines the new food source v. This dimension's value is set to be the boundaries if it exceeds its predefined boundaries. After that, the new food source is assessed. The behaviour of bees in nature is represented in Fig.3.

Fig.3: Behaviour of bees

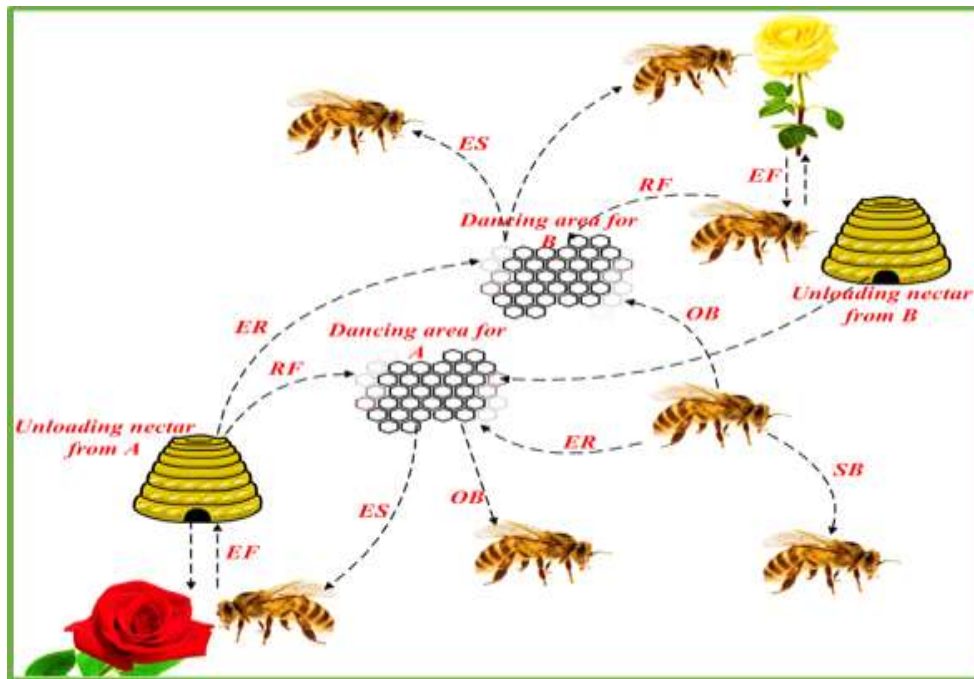


The original food supply and the new one are both subjected to a greedy selection and efficient one is kept in memory. The three phases of bees are recycled until the termination requirement is reached. After that, the best food source that provides the best solution is obtained.

a) ABC Algorithm for Network Routing

The principles of artificial bees are utilized to solve the optimization problem to attaining efficient network routing. The behaviour of ABC optimization in network routing is represented in Fig.4.

Fig.4: Behaviour of ABC optimization in network routing



They are used to test and enhance forward route progress in the model. The parameter in equivalence to the bandwidth available at the forward point in assessment time point of the virtual network under consideration is the nectar acquired as food from adjacent nodes. When the messages are in various states of dispatch, the general algorithm reverts to a table-driven method that restores geographical connection. The employed bees are randomly assigned to the food source for exploitation in the model. Every employed bee selects a food source in the vicinity and assesses its nectar quantity using the fitness function in each iteration. After witnessing the employed bees dance, the onlooker bee moves to N_i food supply, with probability P_i specified as follows,

$$P_i = \frac{F(N_i)}{\sum_{k=1}^{f_s} F(n_k)} \quad (4)$$

Here, $N_i \in (n_1, n_2, \dots, n_e)$ represents i^{th} the food source position. The feasibly connected nodes are denoted by ϵ . The entire quantity of nectar that are obtained from N is given by $F(N_i)$. The entire food source is denoted by f_s . The numerator is the amount of nectar at node N_i and the denominator is the entire amount of nectar accumulated from the current node to all of its neighbours. The dance denotes the amount of free bandwidth available. The higher the bandwidth available, the more bees goes to the node.

Let $F_{\max 1}$ be the current node's first neighbour to determine the intermediate pathways. This function calculates the filtered highest value across all the neighbours of the current node. The onlooker discovers a N_i food supply in the vicinity, which is represented by the equation given below.

$$N_i(n+1) = C_i(n_i) + F_{\max 1}^w(C_i(n_i)) \quad (5)$$

Here, the + sign denotes the development of an intermediary path between the current node and the node with the most bandwidth in the destination direction. The next intermediate node is chosen by a group of onlooker bees. The number of onlooker bees is proportional to the number of neighbours each node has, which is denoted by w . $F_{\max 1}^w(C_i(n_i))$ represents the nearest neighbour selection from the current intermediate node. $C_i(n_i)$ denotes the present intermediate node. $F_{\max 1}^w$ delivers the node address with the high bandwidth among all of the current intermediate node's neighbours. The result is combined with the current node to produce the next intermediate route. $C_i(n_i)$ is now upgraded as follows,

$$C_i(n_i) = N_i(n_i + 1) \quad (6)$$

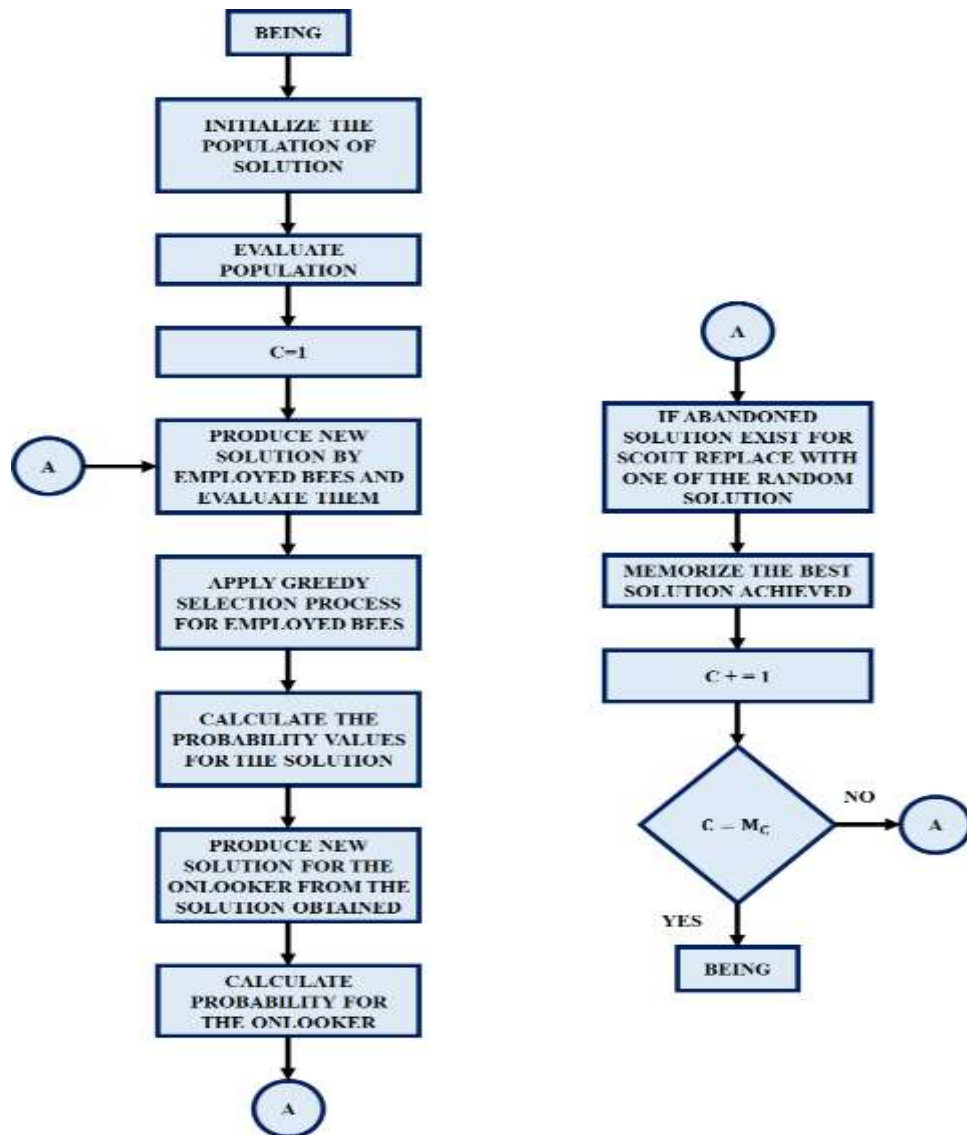
This procedure is continued until the target is reached or there are no more links to investigate.

When the system is configured, a random activity begin to use a portion of the link's bandwidth. The size of the packets transmitted is set at 250 KB and the incoming packets are kept in 1MB of buffer space on each node. A single packet takes one second to send from each node and each link's bandwidth use is monitored. Based on a threshold bandwidth, a decision on whether or not to evaluate the link is made. If the link's bandwidth exceeds a certain threshold, the link is able to participate in packet routing. After obtaining the quadrant structure, this decision is made.

The routers chosen are those that have bandwidth over the threshold and they readily transfer messages. Identifying the nodes that meet the Quality of Service (QoS) measure is what network awareness is all about. This allows for a simple routing decision.

The fitness value is calculated when the neighbours have been established. If this new fitness value is higher than the previous one, then the bees migrate to this new food source; otherwise, they stay in the same node. When all employed bees have completed their quest for food, the knowledge is shared with onlooker bees. The onlooker bees now choose these food sources based on a probability P_i defined in (1), which indicates the best bandwidth on the $N_i(t)$ and $N_i(t+1)$ link. The flowchart of ABC algorithm for network routing is represented in Fig.5.

Fig.5: ABC optimization algorithm for network routing



In the ABC algorithm, the cycle or count for the ABC algorithm's performance is represented by C . The maximum cycle or the total number of times ABC repeats, is represented by M_C .

The goal of a bee's quest for food is to maximize the E/T ratio. Here, E is the nectar food found, while T denotes the time spent on foraging. T is not authorized over a specific level in the network for communication efficiency. In addition, foraging takes place over a period of time specified by the network's stability in that specific location.

In addition, MANET is vulnerable to major security risks that are difficult to combat. Because of the open medium and lack of a defined line of defense, security is a critical concern with MANET. Hence, RSA cryptography is developed for preventing the network from unwanted threats.

C) RSA Algorithm

The end-to-end secrecy and data aggregation is achieved by using encryption based on privacy homomorphic. Additive PH and multiplicative PH are two types of privacy

homomorphism. In additive homomorphic, the encrypted data is performed using an additive homomorphic encryption technique without the requirement to decode any individual data. Since it has lower operating costs than multiplicative PH, it is more suited for using in wireless sensor networks. A multiplicative homomorphic allows for multiplicative operations on encrypted data without the requirement to decode individual bits. Asymmetric PHs and public key encryption are two types of privacy homomorphic supporting cryptographic techniques. The following are the RSA cryptographic algorithms:

a) RSA key generation steps

The pseudo code for RSA generation is presented in Algorithm 1.

Algorithm 1: Pseudo code for RSA key generation

RSA Key Generation

Input : Two large prime numbers S and R
Output: Public key (e, m) and Private key (d, m)

1. Select two large prime numbers S and R such that $S \neq R$.
2. Compute the modulus $m = S \times R$.
3. Compute Euler's Totient function $\phi(m) = (S - 1) \times (R - 1)$.
4. Choose integer e such that $1 < e < \phi(m)$ and $\gcd(e, \phi(m)) = 1$.
5. Compute private key exponent d such that $d \times e \equiv 1 \pmod{\phi(m)}$.
6. Public Key = (e, m).
7. Private Key = (d, m).
8. Distribute the public key to sensor nodes and cluster heads.
9. Keep the private key securely at the sink/base station.

- Both cluster members and CH have access to the public key, which is (e, m).
- Only the sink or base have access to the private key, which is (d, m).

b) Encryption

The pseudo code for encryption key is presented in Algorithm 2.

RSA Encryption

Input : Message M, Public key (e, m)
Output: Ciphertext C

1. Sensor node obtains the public key (e, m).
2. Compute ciphertext using RSA encryption:
 $C = (M^e) \bmod m$
3. Transmit encrypted packet C to the base station.

c) Decryption

The pseudo code for decryption key is presented in Algorithm 3.

Algorithm 3: Pseudo code for RSA Decryption key

RSA Decryption

Input : Ciphertext C, Private key (d, m)
Output: Original message M

1. Base station holds the private key (d, m).
2. Recover original message using RSA decryption:

$$M = (C^d) \bmod m$$

3. The packet is successfully decrypted.

Hence, the end-to-end secrecy and data aggregation is achieved by using encryption based on privacy homomorphic. This is the achieved by the utilization of RSA cryptography model. The simulation is performed using NS2 software.

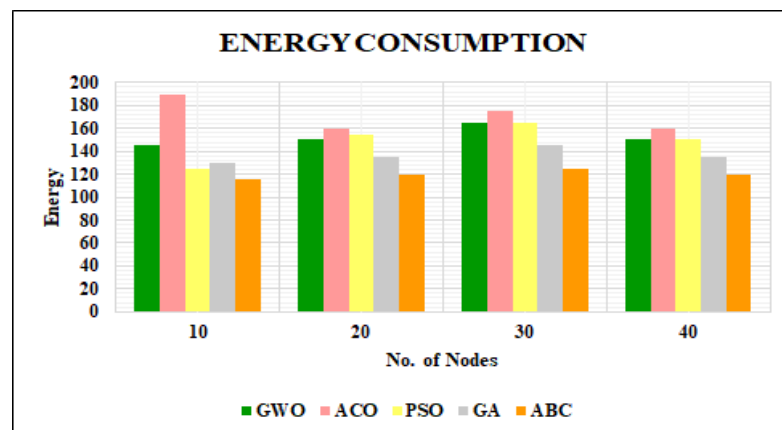
IV. RESULT AND DISCUSSION

The network topology in MANET becomes very dynamic as a result of the increased mobility, resulting in network congestion. In that aspect, a clustering based routing protocol called ABC optimization algorithm is introduced to route the mobile nodes in MANET. In addition, MANET is vulnerable to major security risks that are difficult to combat. Because of the open medium and lack of a defined line of defense, security is a critical concern with MANET. Hence, RSA cryptography is developed for preventing the network from unwanted threats. The proposed ABC algorithm is compared with various other protocols to assess various parameters such as energy consumption, routing overhead, average delay, life time and throughput which are discussed below,

a) Energy consumption

The sensor nodes utilize their energy to send data, receive data, aggregate data, and calculate routing. The energy consumed in the sleep and idle periods is significantly lower than in the other stages. As a result, the energy used in these two periods is not taken into account. The residual energy of each node in the simulation is calculated based on the quantity of messages, distance of transmission and complexity of algorithm. The energy consumption of ABC algorithm is compared with GWO, ACO, PSO and GA which is represented in Fig.6.

Fig.6: Comparison of energy consumption

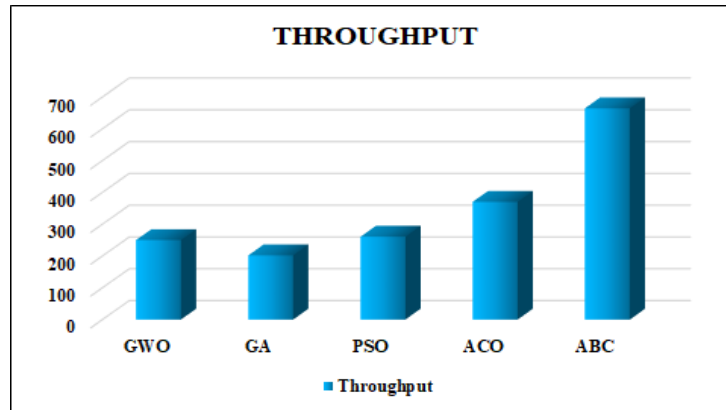


From the graph it is evident that, the ABC optimization algorithm consumes less energy than comparison protocols. Also, less energy is consumed by ABC algorithm in both large and small network. The proposed technique additionally employs on-demand clustering, which takes into account the residual energy's standard deviation as well as the round's threshold value. As a result, the proposed protocol minimises network energy usage by 115 joule/sec for 10 number of nodes and 135 joule/sec for 40 number of nodes.

b) Throughput

When data is sent from the source to the destination, high throughput implies fewer packets are lost. The retransmission works against throughput efficiency. If the retransmission rate is high, the throughput efficiency is low. The throughput analysis of ABC algorithm with other protocols are represented in Fig.7.

Fig.7: Throughput comparison

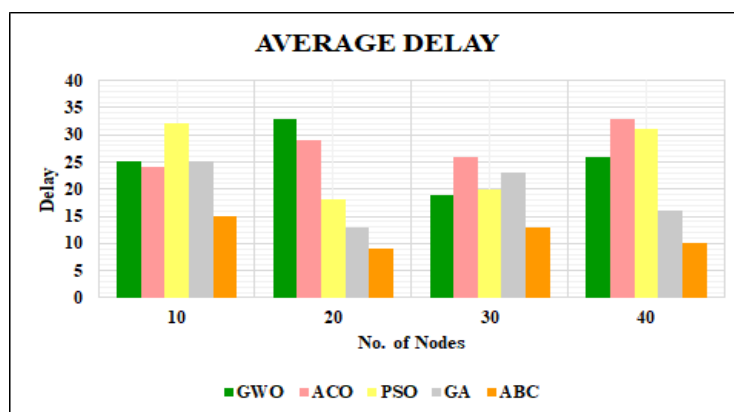


As the total node increases, the throughput value for all comparison protocol decreases. The ABC algorithm is shown to outperform other comparison protocols, with the greatest throughput of 665 bps (bits per second). With an increasing number of vehicles, throughput of ABC algorithm eventually rises.

c) Average delay

A stable cluster structure is formed by a low delay in packet forwarding and the best individual is chosen as the cluster head to preserve network topology. The packets were efficiently sent due to selective nodes and load-balancing features. The average delay comparison of ABC algorithm with other protocols are represented in Fig.8.

Fig.8: Average delay comparison

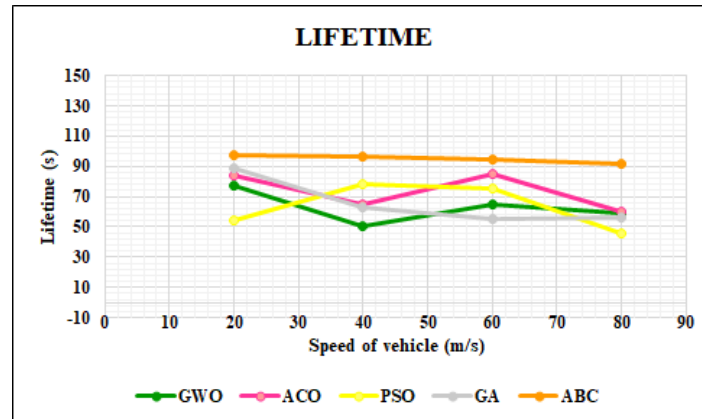


From the graph it is evident that, the ABC optimization algorithm shows minor delay than the comparison protocols. Furthermore, the control packets are transferred inside the cluster member for the majority of the simulation duration. Since the ABC algorithm takes less time of 9 and 15 sec for delivering packets to their destination of 10 and 40 number of nodes, is more efficient than the other protocols.

d) Lifetime

The load balancing perspective-based cluster members who are simply participating in the clustering process are the major cause for the network lifespan increase. When the network increases in size, the longevity of network also increases. When the velocity vector change is severe, the nodes do not participate in the clustering process. The network lifetime while changing the speed of vehicles for different comparison protocols are represented in Fig.9.

Fig.9: Lifetime

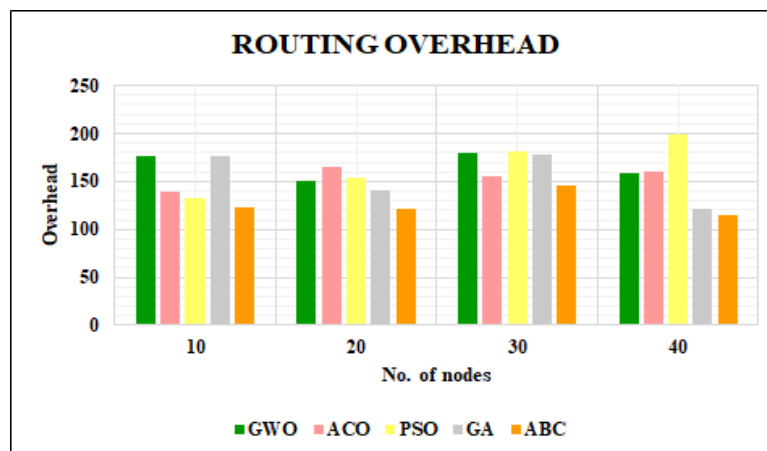


From the graph it is seen that, the ABC optimization algorithm shows increased lifetime than the comparison protocols. The percentage of network lifetime achieved by the ABC optimization algorithm is given by 97.5, 96, 94.5 and 91.5 respectively.

e) Routing overhead

The routing overhead is determined by dividing the total number of control packet bytes delivered to the destination node by the total number of packet bytes sent to the destination node. The routing overhead for comparison of ABC algorithm with other protocols are represented in Fig.10.

Fig.10: Routing overhead comparison



From the graph it is seen that, the routing overhead of ABC optimization is lower than the other protocols. The comparison protocols uses velocity vectors for selecting stable

cluster members. But in ABC algorithm, the worst individuals are replaced by optimal suitable hops. Hence, it possess reduced overhead than other protocols.

f) Performance comparison of RSA cryptography

The RSA cryptography works well in attaining time consumption for generating a key to encrypt and decrypt messages. The time consumed to perform encryption and decryption in RSA cryptography is represented in Fig.11 and Fig.12 respectively.

Fig.11: Time to perform encryption

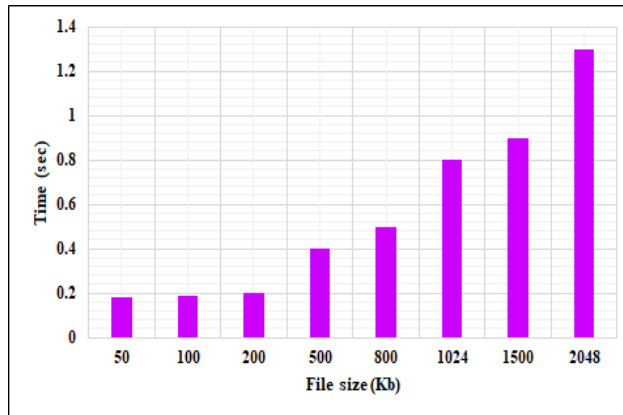
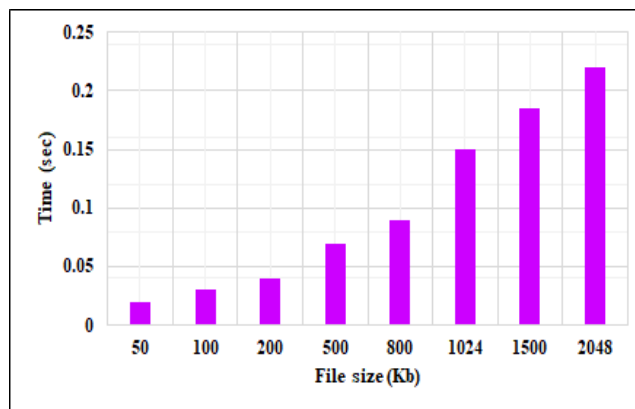


Fig.12: Time to perform decryption



The gradual increase in time for encryption and decryption is based on the file size, indicating that it takes less time to accomplish this process.

V. CONCLUSION

In this study, ABC optimization algorithm is utilized for routing the mobile nodes in MANET. The nodes in MANET communicate with one another freely and dynamically. The proposed ABC algorithm is compared with various other protocols to assess different parameters. From the results, it is evident that, the ABC algorithm minimises network energy usage by 115 joule/sec and average delay by 9 sec for 10 number of nodes. Also, the routing overhead of ABC algorithm is reduced when compared with other protocols. The ABC algorithm is shown to outperform other comparison protocols, with the greatest throughput of 665 bps (bits per second). Furthermore, the percentage of network lifetime achieved by the ABC optimization algorithm is given by 97.5, 96, 94.5 and 91.5

respectively. In addition to this, there is a chance of initiating routing assaults by malicious node to disrupt routing processes. Hence, RSA cryptography technique is developed to prevent insider attack in network. Also, the performance metrics of RSA cryptography is analyzed. The RSA cryptography works well in attaining time consumption for generating a key to encrypt and decrypt messages. The gradual increase in time for encryption and decryption is based on the file size, indicating that it takes less time to accomplish this process.

REFERENCES

1. Amit Sinhal and Sanjay K. Mishra, "Analysis on Clustering Approach in Manet", *JETIR*, Volume 4, Issue 07, pp 103-107, 2017.
2. Sandeep Monga, J.L Rana and Jitendra Agarwal, "Clustering schemes in mobile ad-hoc network (MANET): a review", *International Journal of Scientific & Technology Research*, Volume 8, Issue 08, pp 1168-1176, 2012.
3. Namkyu Kim, Woongsoo Na and Sungrae Cho, "Dual-channel-based mobile ad hoc network routing technique for indoor disaster environment", *IEEE Access*, Volume 8, pp 126713-126724, 2020.
4. Bradley Fraser, Andrew Coyle, Robert Hunjet and Claudia Szabo, "An analytic latency model for a next-hop data-ferrying swarm on random geometric graphs", *IEEE Access*, Volume 8, pp 48929-48942, 2020.
5. Mahmood K. Ibrahim and Ameer M. Aboud, "A Secure Routing Protocol for MANET", *International Journal of Computer Science Engineering and Technology (IJCSET)*, Volume 4, Issue 7, pp 223-230, 2014.
6. Naghma Khatoon and Amritanjali, "Mobility aware energy efficient clustering for MANET: a bio-inspired approach with particle swarm optimization", *Wireless Communications and Mobile Computing*, pp 1-13, 2017.
7. Mohamed Elhoseny, R Sundar Rajan, Mohammad Hammoudeh, K Shankar and Omar Aldabbas, "Swarm intelligence-based energy efficient clustering with multihop routing protocol for sustainable wireless sensor networks", *International Journal of Distributed Sensor Networks*, Volume 16, Issue 9, pp 1550147720949133, 2020.
8. Fouziah Hamza and S. Maria Celestin Vigila, "Cluster Head Selection Algorithm for MANETs Using Hybrid Particle Swarm Optimization-Genetic Algorithm", *Int. J. Comput. Netw. Appl.*, Volume 8, Issue 2, pp 119-129, 2021.
9. Suma R. and C. Siddaraju, "Integration of particle swarm optimization with an adaptive K-Nearest Neighbor for energy-efficient clustering in MANET", *Journal of Advance Research, Ideas and Innovations in Technology*, Volume 6, Issue 6, pp 233-240, 2020.
10. Mani Bushan D'Souza, Enoch Alousious Fernandes, Manjaiha D.H. and Jeevan Pinto, "Applications of Genetic Algorithms in Manet", *International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM*, pp 218-220, 2017.
11. Veena Trivedi and Padmalaya Nayak, "Modified AODV using genetic algorithm to minimize energy consumption in MANET", *Int. J. Innov. Technol. Explor. Eng.*, Volume 8, pp 525-530, 2019.
12. Antra Bhardwaj and Hosam El-Ocla, "Multipath routing protocol using genetic algorithm in mobile ad hoc networks," *IEEE Access*, Volume 8, pp 177534-177548, 2020.
13. Bhuvaneswari Madasamy and Paramasivan Balasubramaniam, "Enhanced Load Balanced Clustering Technique for VANET Using Location Aware Genetic Algorithm", *Promet-Traffic & Transportation*, Volume 34, Issue 1, pp 39-52, 2022.
14. Sandeep Raskar and Kamatchi Iyer, "Self-adaptive multi-purpose Grey Wolf optimization for efficient routing of wireless ad hoc networks", *International Journal*

- of Modeling, Simulation, and Scientific Computing, Volume 9, Issue 05, pp 1850036, 2018.
15. Muhammad Fahad, Farhan Aadil, Zahoor-ur- Rehman, Salabat Khan, PeerAzmat Shah, Khan Muhammad, Jaime Lloret, Haoxiang Wang, Jong Weon Lee and Irfan Mehmood, "Grey wolf optimization based clustering algorithm for vehicular ad-hoc networks", *Computers & Electrical Engineering*, Volume 70, pp 853-870, 2018.
 16. Dong Yang, Hongxing Xia, Erfei Xu, Dongliang Jing and Hailin Zhang, "Energy-balanced routing algorithm based on ant colony optimization for mobile ad hoc networks", *Sensors*, Volume 18, Issue 11, pp 3657, 2018.
 17. Deepak Sinwar, Nisha Sharma, Sunil Kumar Maakar and Sudesh Kumar, "Analysis and comparison of ant colony optimization algorithm with DSDV, AODV, and AOMDV based on shortest path in MANET", *Journal of Information and Optimization Sciences*, Volume 41, Issue 2, pp 621-632, 2020.
 18. Dweepna Garg and Parth Gohil, "Ant Colony Optimized Routing for Mobile Ad Hoc Networks (MANET)", *International Journal of Smart Sensors and Ad Hoc Networks*, Volume 2, Issue 3, pp 4, 2012.
 19. Menal Dahiya, "MANET's: Security Attacks and Securing Routing Protocols", *Advances in Wireless and Mobile Communications*, Volume 10, Issue 4, pp 693-697, 2017.
 20. Rashidah F. Olanrewaju, Burhan Ul Islam Khan, Farhat Anwar, Bisma Rasool Pampori and Roohie Naaz Mir, "MANET Security Appraisal: Challenges, Essentials, Attacks, Countermeasures & Future Directions", *International Journal of Recent Technology and Engineering (IJRTE)*, Volume 8, Issue 6, pp 3013, 3024, 2020.
 21. Lu Sixu, Wu Muqing and Zhao Min, "Particle swarm optimization and artificial bee colony algorithm for clustering and mobile based software-defined wireless sensor networks", *Wireless Networks*, Volume 28, Issue 4, pp 1671-1688, 2022.
 22. Praveen Bondada, Debabrata Samanta, Manjit Kaur and Heung-No Lee, "Data Security-Based Routing in MANETs Using Key Management Mechanism," *Applied Sciences*, Volume 12, Issue 3, pp 1041, 2022.
 23. Umair Amin and Munam Ali Shah, "A novel authentication and security protocol for wireless adhoc networks", 2018 24th International Conference on Automation and Computing (ICAC), IEEE, 2018.
 24. K. Vinoth Kumar, T. Jayasankar, V. Eswaramoorthy and V. Nivedhitha, "SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks", *International Journal of Intelligent Networks*, Volume 1, pp 36-42, 2020.
 25. Vallala Sowmya Devi and Nagaratna P. Hegde, "Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer", *Wireless Personal Communications*, Volume 100, Issue 3, pp 923-940, 2018.
 26. S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues," *IEEE Communications Magazine*, 2021.
 27. Y. Sun, J. Zhang and H. Zhou, "Energy-Efficient Routing Protocols in MANET: A Survey," *IEEE Access*, vol. 9, pp. 101390–101408, 2021.
 28. M. B. Rasheed and M. A. Al-Shaboti, "Cluster-based routing techniques in mobile ad hoc networks: A review," *Wireless Networks*, vol. 28, pp. 1523–1545, 2022.
 29. A. A. Abbasi et al., "Energy-aware clustering algorithms in MANET: A comprehensive survey," *Computer Networks*, vol. 203, 2022.
 30. H. Gupta and R. Sharma, "Swarm intelligence-based routing optimization in MANETs," *IEEE Access*, vol. 10, pp. 45127–45140, 2022.
 31. S. Kaur and P. Singh, "Particle swarm optimization based clustering in MANET," *Wireless Personal Communications*, vol. 121, 2021.

32. M. K. Marina and S. R. Das, "Performance of hybrid swarm optimization routing in mobile ad hoc networks," *Ad Hoc Networks*, vol. 120, 2021.
33. R. Singh and V. Sharma, "Energy efficient PSO-based clustering algorithm for MANET," *International Journal of Communication Systems*, vol. 34, 2021.
34. A. M. Hameed and M. A. Ahmed, "Hybrid GA-PSO routing for dynamic MANET environments," *Future Internet*, vol. 14, 2022.
35. Z. Li, J. Wang and Y. Zhang, "Grey wolf optimization based routing in mobile ad hoc networks," *IEEE Access*, vol. 9, pp. 75420–75430, 2021.
36. M. Dorigo and T. Stützle, "Ant colony optimization for adaptive routing," *Swarm Intelligence*, vol. 16, pp. 125–148, 2022.
37. K. Arora and S. Chaudhary, "Comparative analysis of swarm-based routing algorithms in MANET," *Journal of Network and Computer Applications*, vol. 204, 2023.
38. D. Karaboga and B. Basturk, "Artificial bee colony algorithm: Theory and applications," *Applied Soft Computing*, vol. 127, 2022.
39. P. Kumar and S. Patel, "Artificial bee colony based cluster head selection for MANET," *Wireless Networks*, vol. 29, pp. 4105–4118, 2023.
40. A. Mishra et al., "Security challenges in mobile ad hoc networks: A survey," *IEEE Access*, vol. 9, pp. 120547–120565, 2021.
41. H. Al-Hamadi and I. Al-Shaikhli, "Secure routing in MANET using cryptographic approaches," *Journal of Information Security and Applications*, vol. 64, 2022.
42. W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson, 2022.
43. M. A. Khan et al., "Secure and energy-efficient routing protocols for MANET," *Ad Hoc Networks*, vol. 137, 2023.
44. S. Jadhav and P. Patil, "Trust and cryptography based secure routing for MANET," *IEEE Access*, vol. 11, pp. 40211–40225, 2023.
45. N. Sharma and R. Gupta, "AI and optimization based secure MANET routing techniques," *Future Generation Computer Systems*, vol. 148, pp. 214–229, 2024.