A Secured Routing Protocol for MANET

Abstract

Recently, the privacy and security in MANETs is a major concern because of its frequent utilization which includes emergency operation, survival search, battlefield communications and sensor dust. Though, owing to mobility and consistent topology alterations in MANETs, designing routing protocols for those networks is a challenging task especially in the large-scale network. Moreover, inappropriate data usage initiates data leakage which may result in faulty outcomes. Hence, secured routing approach which comprises a trust and energy efficient routing framework to secure routing with an improved approach of bat algorithm and Firefly for optimization that is based on the integration of Inter-cluster and Intra-cluster Multihop Secured Routing Protocol (BF-ICMHSRP) in MANET is proposed in this study. The proposed BF-ICMHSRP algorithm simulation experiments will be conducted using NS2. The simulation produces two output files, a trace file used for data processing and a NAM file used to visualize the simulation. BF-ICMHSRP algorithm performance will be compared with traditional bio-inspired technique. The performance of the proposed approach is evaluated using different metric named as, average End-to-End Delay, Average throughput, Routing overhead Ratio, Packet delivery Ratio, Average Energy Consumption, Received Signal Strength (RSS) and Link Available Time (LAT).

Keywords: Ad hoc network, Energy efficiency, secure routing, MANET, Bio-inspired technique, cryptography

1.0 Introduction

Mobile Ad-hoc Networks (MANETs) is one among the emerging technology in the communication domain because of its advantageous characteristics including its flexible structure and its application in the military tactical and rescue process (Tseng et al., 2003).Moreover, it is distributed method which assists the communication through the wireless links in between the nodes of individual or group of hops in which the nodes performs the operation of both the host and the router. The topology of the network gets changed in a rapid manner, and the decisions are made in a distributed way. Hence, owing to the network's dynamic manner, the routing process for the MANET becomes the challenging process, and moreover, the wireless link turned into major fallible in the MANET (Zhang et al., 2015). Generally, routing task involves the packets or data transmission done from the original node to the end node. Moreover, it regulated the data flow within the networks and made the decision for selecting the proficient destination path. Yet, the MANET often alters its topology which then causes the routing of the packets to be complex (Li & Wang, 2007). Therefore the major objective of the routing process in the MANET includes the detection of the end- route, and the scaling process includes maintaining the route and overhead reduction. Hence, for these objectives, several routing protocols have been framed from the earlier years. However, they include certain challenges in the MANET routing such as vulnerability to certain attacks and poor throughput ,PDR and end-to-end delay (Junhai et al., 2009). Therefore, to overcome these challenges, BF-ICMHSRP in MANET is proposed. Hence, in this study, proposed pair and Identity-based routing approach attained enhanced security routing by generating the key pair and effective broadcasting communication in the mobile Ad-Hoc networks attained by a combination of inter and intra–clustering approach. Moreover, Firefly approach provides the optimum message transmission, and the Bat approach utilised to attain the delay aware node-disjoint routing paths and dynamic multiple energy.

The rest of the paper is structured in the following order a brief survey of related works on clustering algorithms is presented in Section 2. In Section 3 we described the system model and an overview of the proposed algorithm. Section 4 presents the simulation results of the proposed technique and Section 5 presented the conclusion of our proposed work and discussed the future extensions which are needed to be focused.

2.0 Review of literature

This section presents the previous studies relating to the MANET's routing process are reviewed which includes the bio-inspired techniques, multipath routing and the energy–effective routing approaches.

A research by Taheri et al. (2015) established AnoMul (anonymous multicast routing protocol) to improvise the multicast protocol's privacy characteristics in MANET .This developed model expanded the anonymous routing from the unicast to multicast communications which then delivered the added privacy providence. The future consideration should be focused on the United mesh having individual leader every time, and moreover, it should concentrate on the location privacy in the cases for the cluster of senders and receivers.

A study by Ebrahimi and Jamali (2016) developed a firefly approach to detect the black hole attack in MANET. In this firefly approach, attractiveness factors and objective function are utilized. From the simulation results, it is found that the proposed approach outperformed the conventional AODV approach regarding the number of lost packets, throughput, an end to end delay and packet delivery ratio. However, it has the constraints within the energy consumption and with increased overhead which are needed to be addressed in future.

A work by Uddin et al. (2017) implemented the Fitness Function approach in AOMDV routing approach to enhance the energy consumption called FF-AOMDV (Ad Hoc On-Demand Multipath Distance Vector with the Fitness Function). The simulation results indicated that the developed FF-AOMDV provides better results than the conventional approaches. Hence in this protocol, destination path calculations are based on bandwidth, energy and distance. Therefore, the future focus is to concentrate on several other network resources that could extend the network lifetime and improve the QoS.

A study by Sumathi and Gunasekaran (2018a) proposed Ant-primarily based Misbehavior node detection technique with the utilization of ant approach to improving the performance of the developed protocol. Moreover, the misbehaviour nodes are then evaluated appropriately regarding PDR, throughput. Moreover, ACO technique is examined to identify and lessen the impact of the attack in certain another routing approach and utilized this ACO for attained enhanced path detection using max-min optimization. Therefore, several other

optimization approaches with misbehaving node recovery are to be implemented to attain the better performance in future.

ANT colony based AOMDV protocol developed by Kanani and sinhal (2013) attained the better PDR and packet drop value. However, it has the disadvantage that it's routing overhead value are higher which are needed to be reduced for attaining maximum performance. Moreover, fitness function implementation in AOMDV routing approach (FF-AOMDV) designed by Uddin et al. (2016) detect the enhanced routing with reduced energy consumption. Though, it has lesser network lifetime that affects the overall performance which is to be addressed in future. Similarly, Bat optimization based AOMDV approach developed by Prabha and Ramarajan (2015) attained the load balance with improved PDR value. But it has the larger end-to-end delay value which is needed to be reduced.

Moreover, QoS routing approach developed by the Ahmadi et al. (2015) provided the improved lifespan of the network. However, there is a constraint with these QoS routing such that the packet delivery ratio should need to be enhanced and certain another QoS constraints like the bandwidth are to be validated. Residual Energy based Reliable Multicast Routing Protocol made by Gopinath and Nagarajan (2015) implemented the multicast backbone for enhanced stability. However, there is a lack of secureness in the routing processes which are needed to be addressed. A research by Basurra et al. (2015) framed ZCG which has lesser energy consumption and also has dis-advantage that parallel collision broadcasting could not be attained in an efficient manner. Hence fairness among nodes is needed to be addressed. Similarly, Rafsanjani and Fatemidokht (2015) framed FBeeAdHoc routing protocol to provide enhanced security against various attacks. However, this approach required the optimisation approach to identify the selfish nodes and also to attain improved optimisation in fuzzy membership functions.

From these above-reviewed studies, it is stated that the convention routing protocol suffers from the lack of secureness among several attacks and there is a lack of optimisation technique to improve the performance by reducing routing overhead and end-to-end delay and enhancing throughput, network's lifespan and the packet delivery ratio. Hence, the major motive in our study is to provide the enhanced security in the routing process and to attain the enhanced packet delivery ratio, throughput, and network's lifespan with decreased routing overhead and end-to-end delay by the implementation of firefly optimisation and bat algorithm.

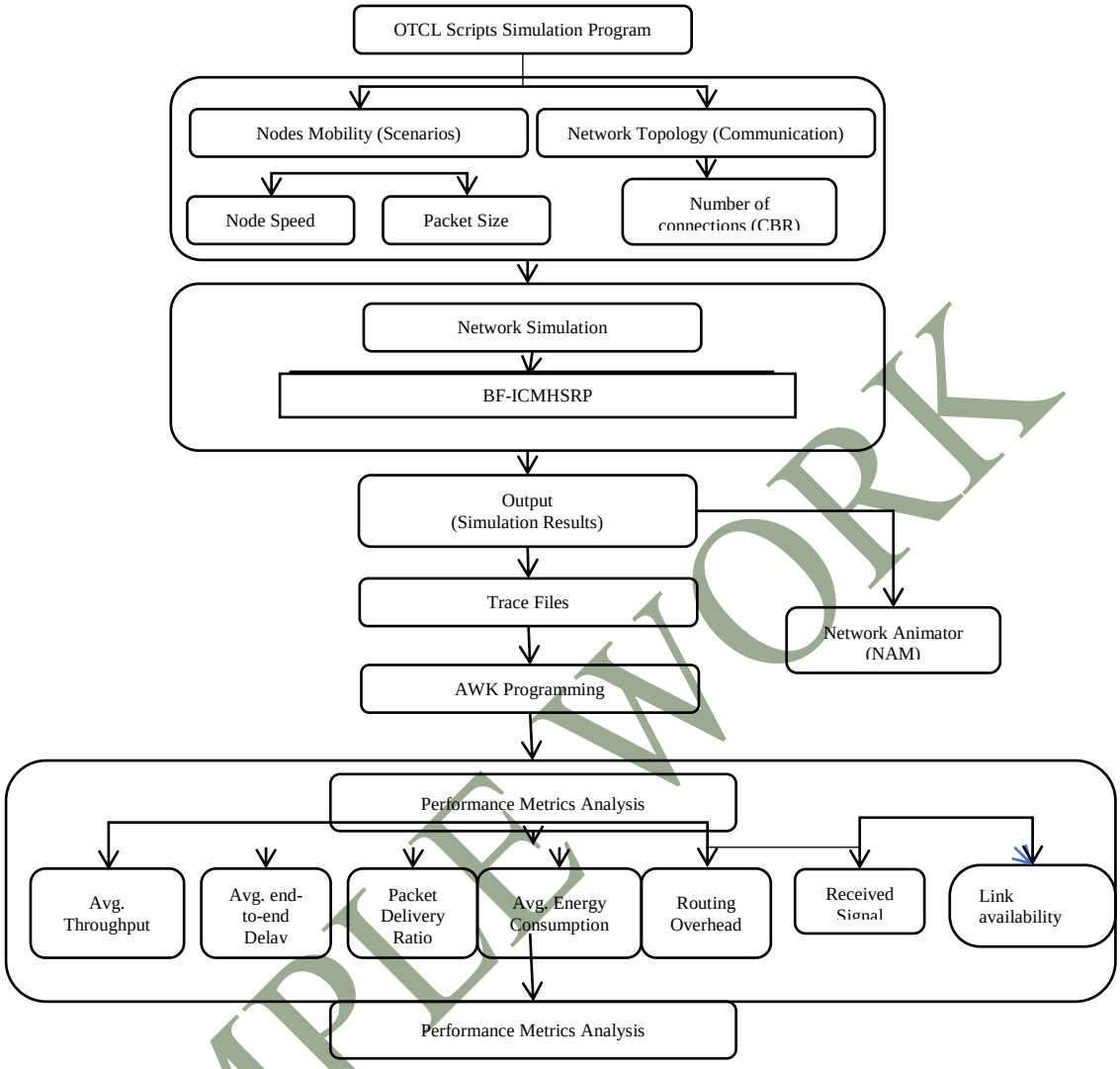
3.0 Methodology

In this study, routing protocol based on pair and identity cryptography framework is proposed to attain efficient, secure routing .Moreover, to enhance the processing speed of the proposed technique,the combined inter-intra clustering route formation is used. In this proposed technique, bio-inspired optimisation approach, i.e., Firefly and bat approach was implemented to identify the best path and to achieve the optimised message transmission.Hence,Our proposed approach identified the best path and provides the enhanced secured routing with reduced routing overhead, lesser energy consumption,improved PDR and throughput value.The experimental simulation is performed in NS2 to evaluate the performance of the proposed algorithm.

3.1 System Framework

The system framework for our proposed BF-ICMHSRP model includes the OTcl scripts program which will specify the network settings including the packet size, node speed and the network topology includes the number of connections to be made. Then the network simulation is done using the proposed routing protocol. The simulation result contains two files that are trace and NAM file to process data and to view simulation. The performance of proposed technique was examined with performance metrics like average throughput, average end to end delay, packet delivery, energy consumption, routing overhead.

Figure 1: Flow of execution in NS2



3.2 Secure routing protocol based on Pair and Identity-Based Cryptography technique

In this section, a secured Identity (ID) key managing arrangement in ad hoc network is proposed. Identity-Based cryptography states the cryptosystem within the private and public keys depends upon the client's identity. Also, there is no certificate required for the authentication process. Public keys having ID node are given earlier to MANET structure to eliminate the need for public key transfer to packets. The identifier node's ID is created from the public key with the one-way hash function. Moreover, the ID and public keys are provided before the MANET distribution. Hence, the node could not alter its ID throughout the MANET's lifetime which avoids the unapproved usage. Hence with the proposed secure routing protocol, the source/destination node ciphers the RREQ (Route Request) packet by utilizing the source or destination node's private key, and then the route sequence number

could not be changed by the malevolent node. The input for our proposed secured protocol includes the messages in packet, Encryption, decryption and signature generation steps and the output attained concentrates on PDR (Packet delivery ratio), packet loss, accuracy and packet delay. Within our proposed secured protocol, encryption and decryption steps are undergone as follows,

Encryption:

Input for encryption process **is** represented as I ∈ id (identity), PP (system parameter), M (message) and output generated as ciphertext, i.e., C∈ C.

Decryption:

Similarly for decryption process, Identity (id), ciphertext C∈C and system parameters (PP), resultant private key d_{id} are taken as input and delivers the resultant message.

Key-pair Generation

To frame the key-pair ,RSA (Rivest–Shamir– Adleman)-key cryptography algorithm has been used in our proposed technique.Moreover, multiplication can be calculated in polynomial time whereas factoring time expands exponentially proportionate to number's size. The algorithm for this cryptography technique is as below:

Choose a, b such that both a and b are prime.

By multiplicating these two a and b, calculate k value

k=a*b and (k) = (a-1)*(b-1)

Choose the integer s in which gcd((k),s)=1 where 1<s<(k).

Determine $f=s^{-1}$ mod (k) whereas sf=1 mod (k)

Public key KB={s,k}.

Private key KV={f,k}

The steps for performing the sign generation and verification in our proposed protocol are as follows

Sign Generation

i. For the sign generation, the appropriate hash function was applied to the message m for getting the hash result J= H (m).

ii. Moreover, for signing the message m, we utilise M<k for computing the signature G=J (mod k) where f is the signer's private key.

Sign Verification

i. To check message *m*, digital signature *G* was utilised to compute.
J= G (mod k) where *s* is the public key of the signer.

ii. J'=H (J) has attained and compared with J.

Message authentication is processed if obtained J` and J is similar. Otherwise, the data's are dispositioned.

Digital Signature Standard (DSA)

To analyse the data integrity and signature identity, DSA is computed in our proposed approach by utilizing the parameters and rules set. Generally, every client owns a public and private key pair. Therefore, within our framed Signature generation, the digital signature is a huge numeric combination specified as a string of binary digits in a computer language could be created by using the private key, and the public key was utilised for the signature verification step.

Moreover, the Hash function is utilized within the signature generation for attaining the consisted format of data known as a message digest. This message digest is the input for DSA for generating a digital signature which is sent to verifier with signed data to verify the signature utilizing user's public key. This designed DSA has been applied in an email, e-funds transfer, data storage whereas data integrity affirmation and origin validations are needed.

3.3 Intra and Inter clustering Multihop routing process

To increase the processing speed of route discovery, our proposed routing protocol utilises the clustering approach by the arrangement of entire nodes of the network in a

hierarchical manner. In our proposed cluster- routing, clusters are framed at the initial stage and the routing process performed in this cluster stage along with path setup using cluster maintenance process. Moreover, the radius of clusters is normally set as multi-hops (two or three). After the cluster formation, head node is selected for managing the clusters which act as the base station to control the access and assured the bandwidth in actual traffic. Other than the head node, every member node within the clusters allocated with node ID (NID) and cluster ID (CID).

However , in the conventional techniques , cluster networks generally have two links such as intra-cluster link (link nodes within the cluster) and inter-cluster link (link clusters) separately.Hence, to reduce the delay at the intra-cluster path and also to decrease control overhead at the inter-cluster path, hybrid inter and intracluster routing are framed in our proposed approach.

3.3.1. Intracluster routing process

In our proposed intra-cluster routing process, cluster head (CH) is assigned to perform the routing process from the present cluster to another CH and Packets are sent to the destination through low layer intra-cluster routing and also through high layer inter-cluster routing. Moreover, Link State Routing (LSR) is selected for the intra-clustering process, and every member node gets identified by the head node using NID.

Specifically, Head node gathers every link-state information from each member node creates the intracluster topology message and promotes it to every member node within the cluster. After obtaining this message, member nodes could generate routing tables for intra-cluster communications. Finally, Packets created within the clusters and packets transferred via clusters are sent to a gateway node in the cluster for reaching another cluster.

3.3.2. Inter-cluster routing process

Within our proposed inter-cluster routing, Source node gets communicated with another cluster's node by sending the Route Request (RREQ) to discover the path. This RREQ has been sent to member node and then forwarded to CH instantly. This CH analyse whether the cluster has the destination address or not. If it is present in the cluster, the head added its CID on (Route Reply) RREP and sent in a reverse route to the source. In case, if

cluster did not have the destination address, then the RREQ send to another cluster continuously until it detects the destination.

Hence other than the conventional node level multi-hop networks, any member node may collect packets from outside in our proposed routing and then send it to the gateway node. The packet from Source CH node utilises the intercluster link to attain another cluster hop and reaches the gateway of the present cluster through the intra-cluster path. Packets are then transferred via the inter-cluster path to attain its nearer cluster.

Therefore, our proposed Inter and Intra clustering process are performed as per the following steps.

- Source node forwards RREQ to its CH.
- CH analyses if Destination node exists in members-table and sends a packet to the member. If it does not exist, then packets are sent to gateway nodes in its member-table.
- While an intermediate node received RREQ packet, it started analyzing if it is destination node or checks whether there is any path exist to reach the destination and reply with RREP packet if the path exists.
- Finally, when the Gateway node attained the RREQ packet, it will send the packets to CH in its gateway table.

3.2.1 Firefly Colony Optimization Algorithm

In our proposed approach, Bio-inspired firefly optimisation is implemented to attain the improved message transmission within the established path identified by intra-inter clustering routing. Moreover, our framed Firefly Algorithm utilizes the swarming behaviour of fireflies to converge to an optimal solution and implements the flashing behaviour the unisexual fireflies for propagation.

Hence, the proposed algorithm could be made with specific constraints which are as follows:

- Unisexual firefly's gets attract with other fireflies.
- Every firefly's brightness is proportional to its attractiveness which acts as the primary constraints.

$$V=\beta o\, e^{-\gamma r2} \text{ ---------- (1)}$$

Where the attractiveness at the distance r=0 is β0 and the light absorption constant is ɣ.

Therefore in our proposed work, the movement of the less bright firefly toward the brighter firefly is computed by

$$pi = pi + de^{-\gamma r2} (pj - pi) + \eta (rand - 1/2) \text{ -------- (2)}$$

Where η is the randomization, parameter and rand is a randomly selected number between the interval [0,1].

The pseudo code of the FIREFLY Algorithm

Step-1: Create initial population of fireflies P randomly. P = {p_1,p_2,…p_n}
Step-2: Calculate the brightness (V)of each firefly by using objective function j(pi) as
V = {V_1, V_2….V_n} = {j (p_1), j (p_2), j (p_n)}.
Step-3: Assign light absorption coefficient ɣ
Step-4: While (t ≤ max iteration)
For i=1 to n all n fireflies
For j=1 to i all n fireflies
If (I_j> I_i)
Move firefly i to firefly j by using Eq. (2).
End If Attractiveness varies with distance r using Eq(2)- ɣr
Evaluate new fireflies and update brightness by using Eq. (1).
End for j
End for i
End for t = t+1
End while
Step-5: Rank fireflies according to their fitness and find the best one.
Step-6: If Stopping criteria is reached, then go to step-7.
Else go to step-4.
Step-7: Stop.

3.4 Bat optimization algorithm

To detect the optimised route with reduced delay and enhanced delivery ratio, Bat approach has been implemented in our proposed protocol. In our proposed bat approach, the paths are validated by altering the nodes energy (Vj) and Position (Pj) using DLE (Data Link Escape). Moreover, with the Pareto solutions, weighted factors are valued to attain Bat or path fitness

3.4.1 Optimization through Bat Algorithm

The pseudo code of Bat Algorithm

Step-1: Initialize the bat population path by considering the position Pj and energy Vj using DLE for j = 1...n.
Step-2: For d = 1 to N (points on Pareto fronts)
Step-3: Produce R weights wR ≥ 0 such that $\sum^{R}_{R=1} f_{R=1}$
Step-4: Fitness for multi-objective to be assigned: $P\psi=\sum f_R^{do1}, f_R^{do2}$
While (t < Tmax) // number of iterations
Rank for the obtained paths
Obtain BB
Generate LBB around the obtained BB
Generate new solutions by random fly
If (fitLBB < fitBB)
Update LBB as BB
end if
Rank BB as Global best bat
end while
Record Global best path as a non-dominated solution
End for

In this proposed approach, new solutions are created based on the movement of virtual bats using equations:

$$Rit= Rmin+ (Rmax- Rmin)\ D(0,1) \text{------ (3)}$$

$$Kit+1=Kit+ (yit-best)\ Rit \text{ ---------- (4)}$$

$$Yit+1=yit+Kit \text{ ---------- (5)}$$

Whereas D(0,1) is the uniform distribution. With the pareto solutions, the weighted factors are calculated to attain Bat fitness. Moreover, fitness (pψ) having normalized weights including delay (do2) and the delivery ratio (do1) is attained by applying eq 3 and 4.

$$P\psi=f\ do1+f\ do2 \text{ ---------- (6)}$$

$$\text{Where } f\ do1=1-do1 \text{ and } f\ do2 = do2\text{------- (7)}$$

Fitness based on weights is calculated for the initially populated paths and are ranked. Based on the rank the path with minimum fitness is named Optimum Bat (OB) as shown in

$$OB=\min [p\psi(qi)] \text{ ----------(8)}$$

$$OB=Q: Q€\ qi \text{ ---------- (9)}$$

In which `qi is initial bat population, and Q is bat path within initial bat population, By doing the converged fitness bat (OB) based alteration of the improved individual by an

enhanced individual in a random manner, LBB(Local best Bat) could be attained. If OB is more than LBB fitness, then the OB could be updated as LBB's fitness which then enumerated as a Global best bat. Hence the route related to this obtained global best bat is selected for data transferring process.

3.5. Proposed Algorithm

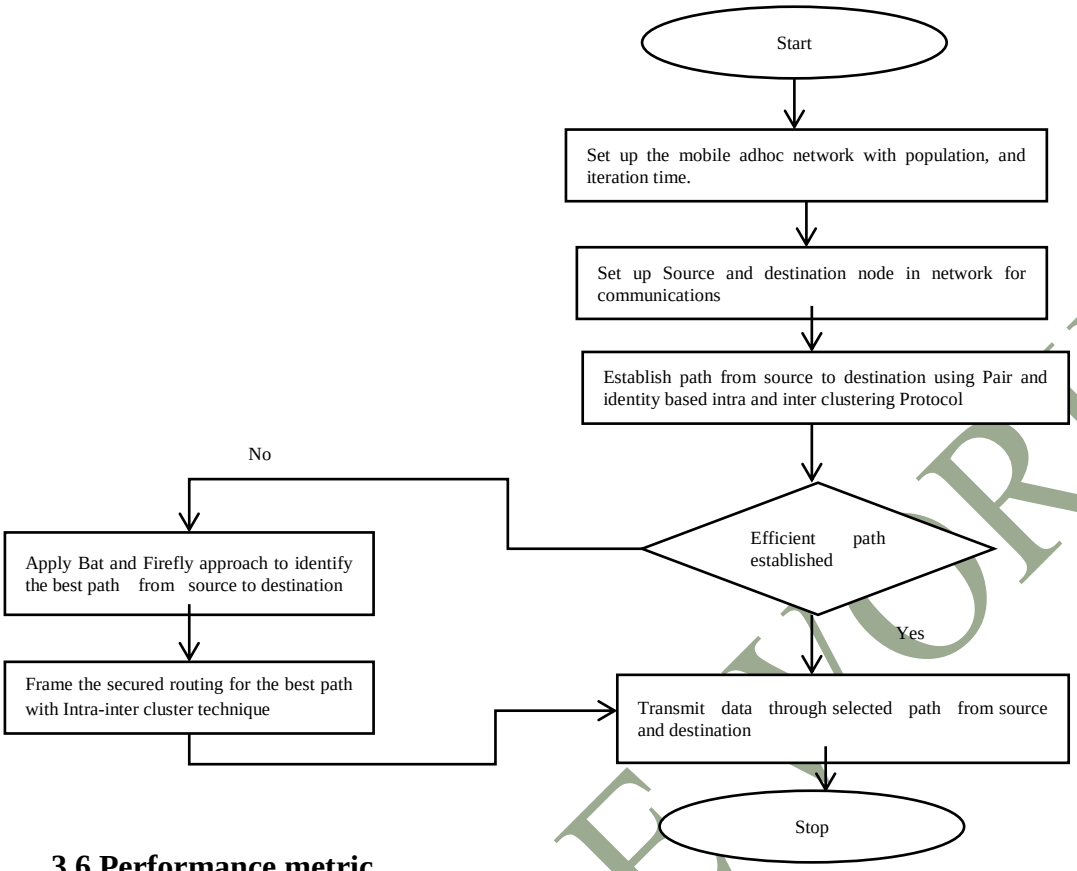
Our proposed BF-ICMHSRP protocol with the designed pair and identity key generation and the optimisation using bat and Firefly was described as follows.

Pseudo Code of the proposed BF-ICMHSRP algorithm

Input: Population N; Iterator time T;
Output: Shortest Path (p_S, Global best firefly's brightness x(t)
Step 1: Initialize the bat population x_i=(i= 1, 2…n), Initialize the number of nodes in the graphs as fireflies
$X = (X_1, X_2, \ldots X_n)$, Setup the position for each node for movement.
Step 2: Define light absorption coefficient γ is transmission range
While (t < Maximum no. of iterations)
for i=1:N do
for j=1:N do
Choose the cycle lengths based on their individual speed
Formation of the cluster in the network (Inter and intra cluster communication)

if f(xj (t) < f(xi(t)) then
Move xi(t) toward xj (t)
f(xi(t)) ← Evaluate Fitness of Firefly
t ← t + 1
Compute p_{best}, g_{best}
Find the current best transmission range with less communication cost
Rank the nodes
end if
Select the optimal path
If (rand > r_i)
Select a result between the best solutions
Generate a solution and proceeding for next solution level.
End if
Increase r_i and attain opt the route p_S
Randomly select two large primary numbers (a and b)
Compute X=a.b and Φ (X) = (a-1)(b-1)
Public encryption
Private decryption
End for
End for
End while

Figure 2: The flowchart for our proposed algorithm is described below:



3.6 Performance metric

The performance metrics were generally used to select the enhanced routing protocol in the MANET field. The major objective of our proposed technique is to identify the reliable and stable route with the maximised energy, signal strength, with an extended lifetime. Hence by uniting the Signal Strength with the Delay data based on energy could enhance the entire throughput higher than the conventional AODV protocol. Therefore to check the performance of our proposed protocol =evaluation metric parameters including the average End-to-End Delay, Average throughput, Routing overhead Ratio, Packet delivery Ratio, Average Energy Consumption, LAT, and RSS was calculated.

3.6.1 Average end-to-end delay

The average total delay occurs in between the transmission of data packets from its source node to its end node is known as the average end-to-end delay. The delay considered is included in the node's queuing delay, route discovery time, transmission delay at MAC layer, transmitting and propagating time within the WSN(Sharma & Patheja, 2002).

3.6.2 Average Throughput

The data quantity in bits obtained by the receiver is known as the throughput in which the throughput per duration unit is calculated as the mean throughput. It is also stated that the successive proportion of delivery via a communication line is the network throughput (Behera & Panigrahi, 2015).

$$T = \frac{Total\ number\ of\ receiving\ packets\ from\ node}{Data\ transmission\ period} * 8$$

3.6.3 Routing overhead Ratio

The proportion of overall transmitted control packets quantity to entire data packets quantity received. Hence with the reduced NRO, there is enhanced performance.

$$NRO = \frac{\sum number\ of\ routing\ packets\ sent}{\sum number\ of\ data\ packets\ received}$$

3.6.4 Packet Delivery Ratio (PDR)

PDR is stated as the proportion of received packets with the packets that are sent over the network. Moreover, it is utilised to calculate the path's link stability. When the nodes quantity gets raised, the size of the network also gets raised, and larger value of PDR indicated the enhanced performance of protocol (Baisakh, 2013).

$$PDR = \frac{\sum number\ of\ packets\ sent\ received}{\sum number\ of\ packets\ send}$$

3.6.5 Average Energy Consumption

The average quantity of energy consumed by every node for transmitting the data packets from source to destination side within the multihop format with the unit Joules are mentioned as follows:

$$\text{AEC} = \frac{\text{Total energy consumed}}{\text{Total no.of available nodes}}$$

3.6.6 Link Available Time

LAT indicates the extension of connecting duration of two nodes which is determined based on the node's direction of movement. The factors to be considered for attaining the LAT include the distance of the node within them, node's transmission range and its signal strength. LAT constraints are determined in the route generation whereas the higher LAT constraints cause the reduced number of links (Zhao, 2012).

3.6.7 Received Signal Strength

RSS is used to determine the better next hop within the network.Moreover, To predict the LAT within two nodes, RSS and change in RSS (Δ RSS) are estimated in which the Δ RSS is to determine the nodes direction. If ΔRSS is positive which means the nodes get in the direction of them and if Δ RSS is negative, the nodes are moving in a direction far from another node (Bhavsar,2014).

4.0 Experimental results

4.1 Simulation setup

Our proposed BF-ICMHSRP algorithm simulation experiments will be conducted using NS2. For this purpose, we will design the network with a sample of 50 nodes using network simulator. In these simulation experiments, a network setting OTcl scripts will be defined, such as routing protocol, propagation model, network traffic, and some nodes to be used and obtained two output files, a trace file used for data processing and a NAM file used to visualise the simulation. The performance of the proposed algorithm is evaluated using performance metrics such as routing overhead, PDR, energy consumption etc.

4.2 Results and discussion

The objective of our proposed protocol is to provide secure routing with enhanced performance. Therefore, the results obtained for our proposed algorithm were used to analyse the routing protocol performance in various circumstances and with various performance metrics. In the present work, we utilised the performance metrics such as the throughput, PDR, Average end-to-end delay, routing overhead, Energy consumption, RSS and LAT of the network to evaluate the performance.

Figure 3: Routing overhead of the proposed protocol

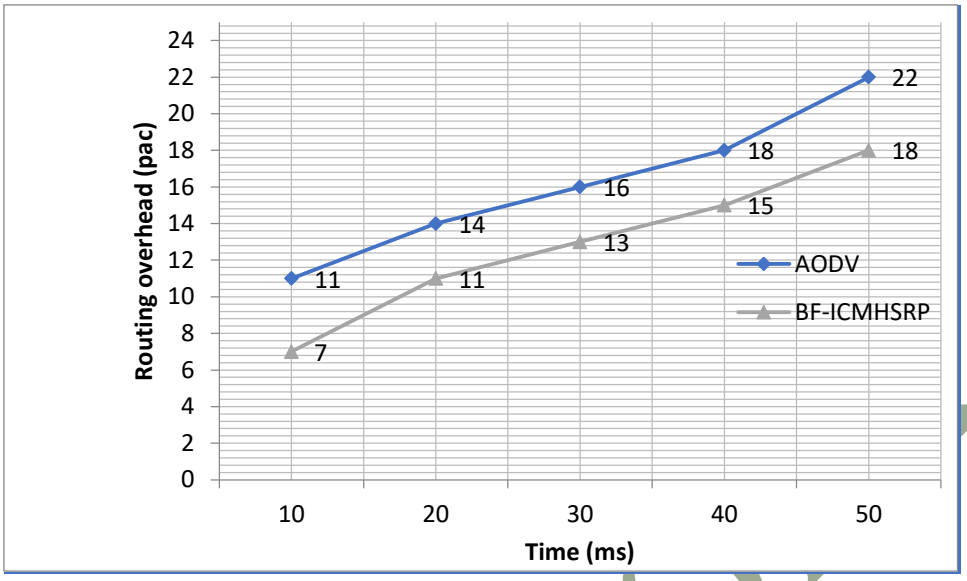
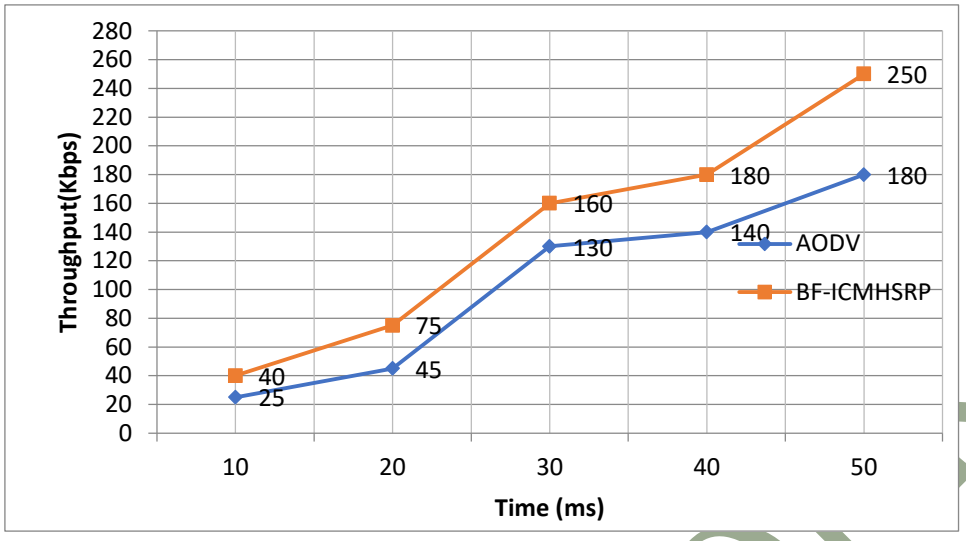


Figure 3 displayed the comparison of conventional routing overhead value with our proposed routing overhead. It is clear from the figure that proposed algorithm attain the lesser routing overhead compared with conventional AODV routing algorithm. Because, In the conventional routing approach, AODV protocol identifies the route based on the demand and moreover, the individual route discovery may cause the larger routes for the destination point which may increase routing overhead in the conventional routing algorithm.However, in our proposed technique , the route discovery or maintenance is originated with the advanced cluster-routing protocol, and hence it causes lesser routing overhead while compared with the previous routing algorithm.

Figure 4: Throughput Graph



From Figure 4, it is shown that throughput value of conventional AODV increases initially and maintains its value when the time increases. However, throughput value of proposed protocol increases with increase in time constantly due to its optimized routing process. Hence, our proposed algorithm shows enhanced performance than the conventional AODV protocol.

Figure 5: PDR Graph comparison

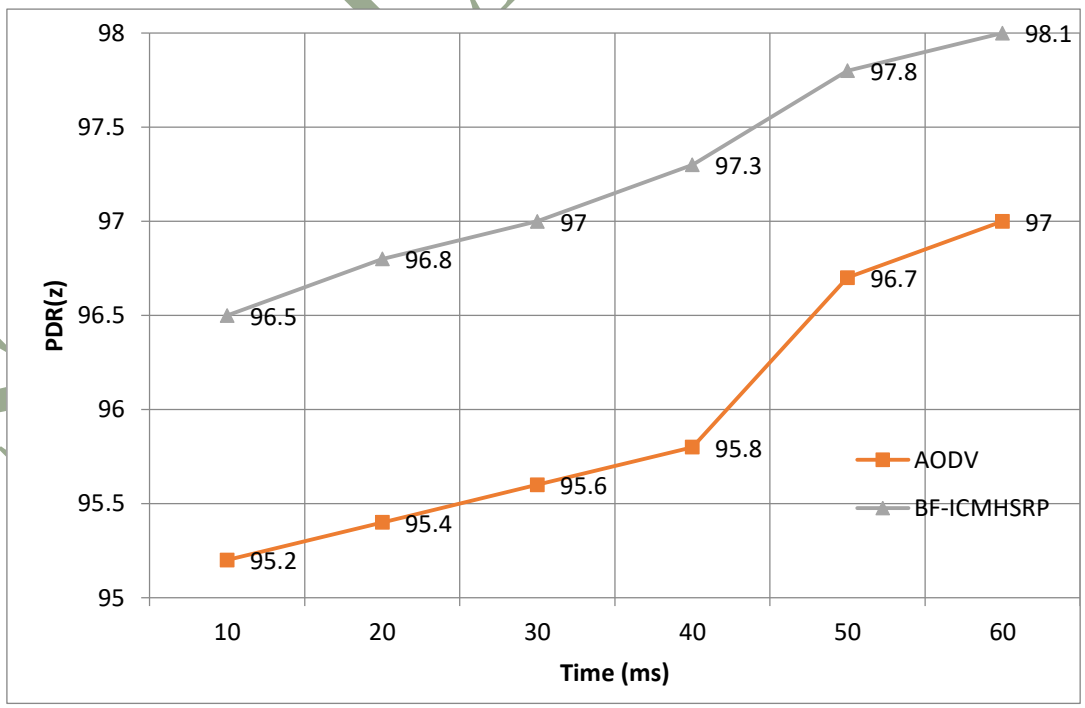


Figure 5 demonstrated the comparison of PDR value of the proposed technique with the conventional approach. Hence due to the enhanced route discovery approach, increase the

probability of the nodes detection for sending the packets is increased, which causes the increase in Packet delivery ratio in our proposed technique hence it is proven that the PDR of the proposed technique shows the enhanced performance while comparing the existing AODV protocols.

Figure 6: RSS of network

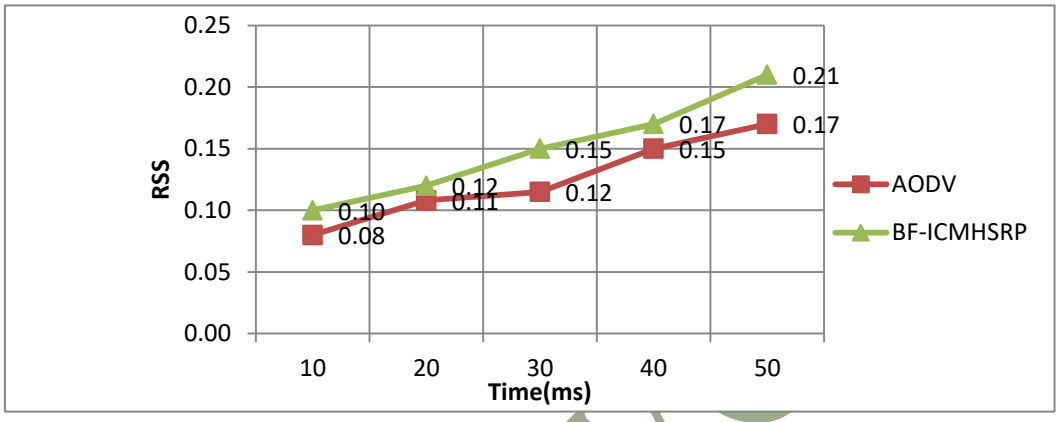


Figure 6 shown the RSS of the proposed algorithm with the conventional AODV routing protocol. Due to inter-intra cluster routing basis, the best hop was discovered in our proposed technique which made the RSS value to be better than the conventional AODV routing protocol.

Figure 7: End to end delay calculation

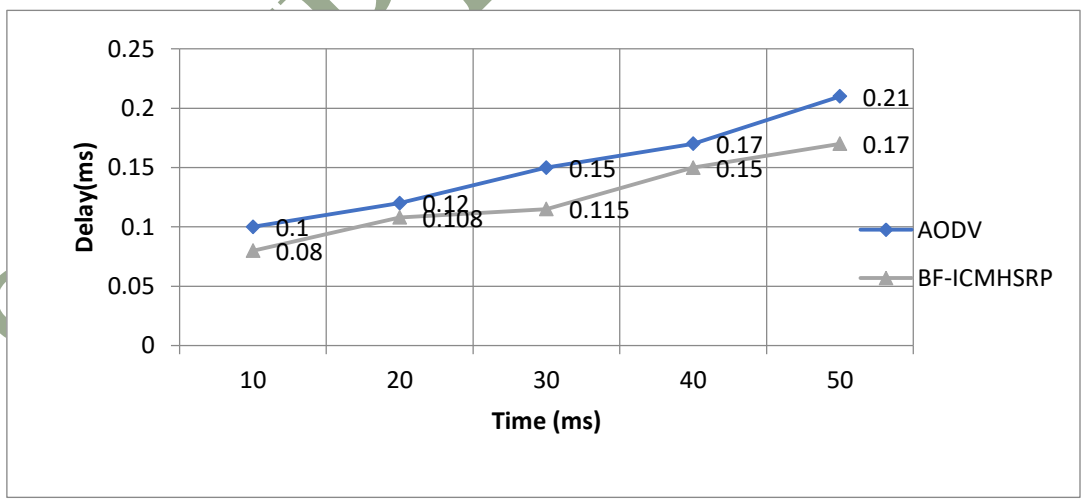


Figure 7 displayed average End-to-end delay value of both proposed and conventional AODV. However, within conventional AODV approach, which routes are generated based on the demand, which causes the higher delay. At the initial stage, there exists the less number of nodes which causes the high delay due to the route formation and maintenance of table.

But in our proposed technique, with the inter-intra clustering routing, the route formation has been made with a lesser delay which then enables enhanced performance than the existing technique due to its combinational routing behaviour.

Figure 8: Link Availability time

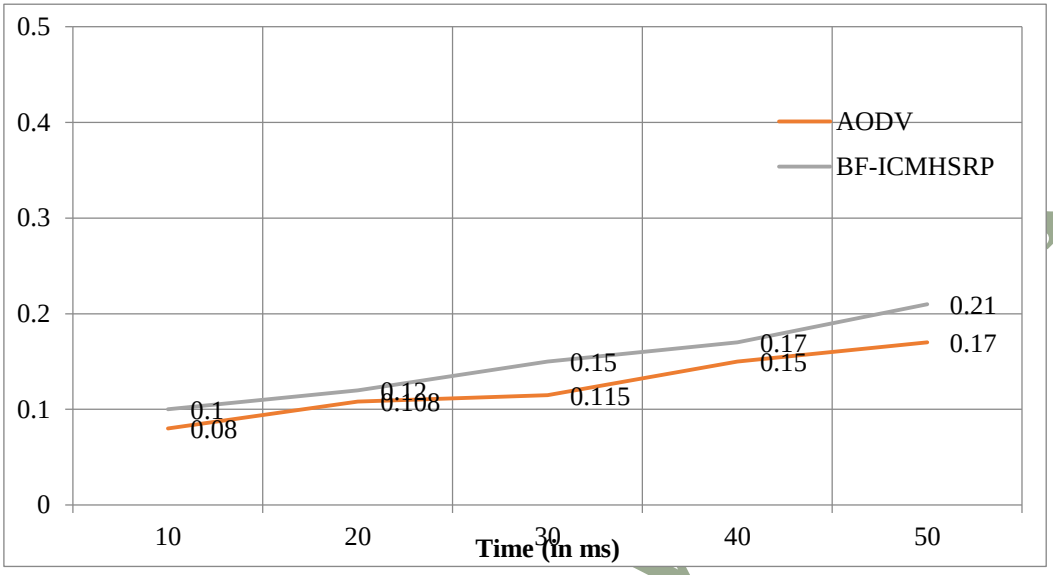
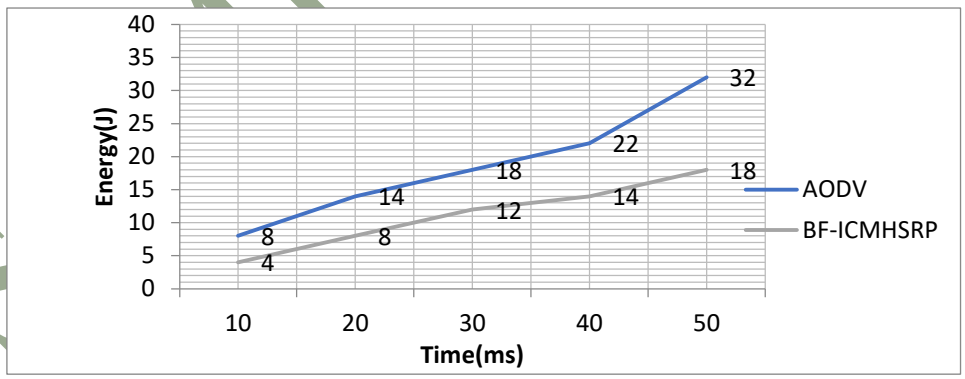


Figure 8 demonstrated the comparison graph of LAT of proposed technique which is better than the conventional AODV protocol. However, due to the lesser link breakage, LAT value gets increased in our proposed approach.

Figure 9: Energy consumption



Energy consumption comparison was demonstrated in figure 8. Hence our proposed scheme attained the reduced energy consumption value as because of its choice of the best path with optimization approach which decreases the unwanted buffering and transmitting overhead.

Table 1: Comparison of PDR value proposed with Conventional Bio-inspired AODV algorithm

Author	Algorithm	PDR
Kanani and Sinhal (2013)	AOMDV-ANT	94.49
	AODV-ANT	84.58
Biradar et al. (2014)	GAOMDV	95.10
Ebrahimi and Jamali (2016)	Firefly -AOMDV	77.91
Prabha and Ramaraj (2015)	BAT-AOMDV	91.90
Author(2018)	BFICMHSRP	98.10

From this table 1, It is identified that our proposed algorithm attained the PDR value (99.810) which is more enhanced than the conventional approaches firefly-AOMDV with PDR of about 77.91 ((2017),BAT-AOMDV with PDR of about 91.90 by Prabha and Ramaraj (2015),GAOMDV (Genetic-based Ad-hoc On-Demand Multipath Distance Vector) framed by Biradar et al. (2014) with PDR of 95.10 and Ad-hoc On-Demand Multipath Distance Vector(AOMDV) based Ant Colony Optimization technique (PDR-94.49) by Kanani et al. (2013) who even developed AODV-ANT which has PDR value 84.58.

Table 2: Performance comparison of End to End delay

Author	Algorithm	End-to-End delay
Sumathi and Gunasekaran (2018)	ANT-AODV	0.49
Prabha and Ramaraj (2015)	BAT-AOMDV	0.377
Ebrahimi and Jamali (2016)	Firefly -AOMDV	0.310
Author (2018)	BF-ICMHSRP	0.17

Table 2 made the comparative analysis of the proposed algorithm's End to end delay of about 0.17 which is founded to better than the conventional approach of ant colony based AODV technique which has the delay of 0.49, BAT-AOMDV with a delay of about 0.377 delay, Firefly-AOMDV with a delay of 0.310.

Table 3: Performance comparison of routing overhead

S.No	Author	Method/Technique	Nodes	Routing overhead
1	Javaid et al. (2015)	AODV- link sensing mechanisms	25	5
2	Kaur and Kumar (2017)	Ant colony optimization along with firefly algorithm	25	5.5
3	Author (2018)	BF-ICMHSRP	20	4.8

Table 3 illustrates the obtained results of routing overhead of proposed approach along with the existing method. By the experimental, the obtained routing overhead is 4.8 for 20 nodes. When compared with the existing technique, the proposed framework has a lower overhead than the existing technique.

Figure 10: Performance comparison of packet delivery ratio

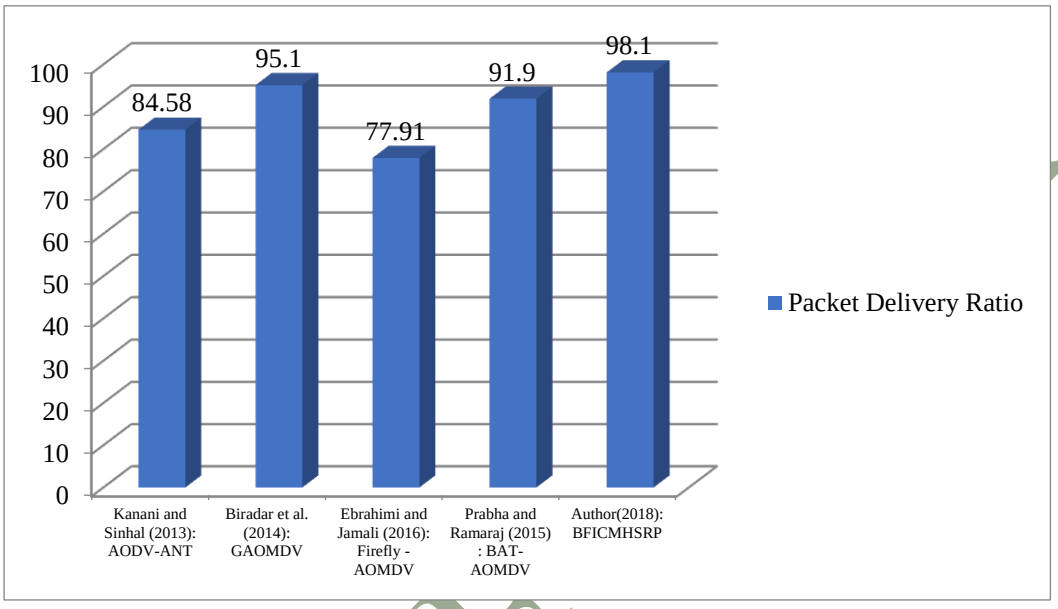


Figure 10 illustrates the performance comparison of packet delivery ratio for the various routing protocol. It's evaluated based on the measure of the ratio of a total number of transmitted packets to the total number of transmitted packets. From the observed results, the proposed routing protocol is higher than the existing technique. From the above results, the PDR and reliability of existing approach are greater than the existing method.

Figure 11: Performance comparison of End-to-to delay

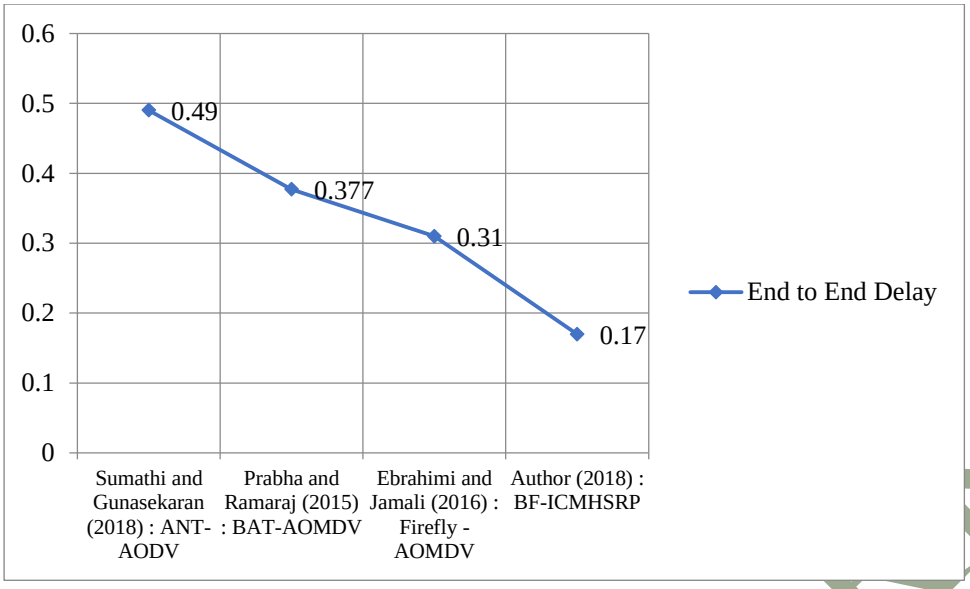
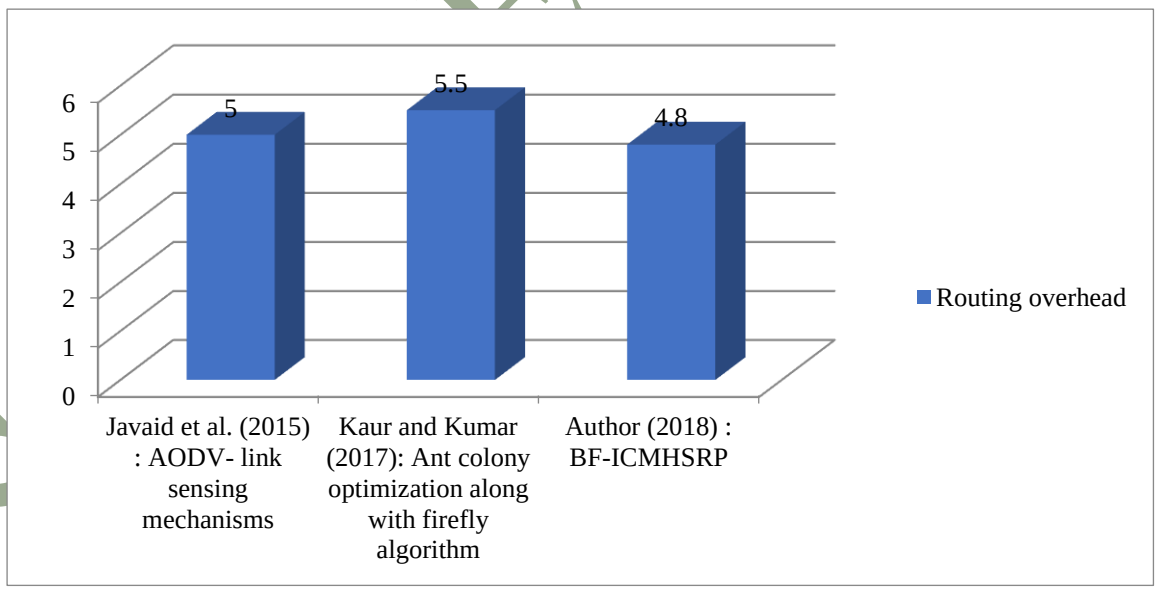


Figure 11 shows the comparison of end to end delay in the routing protocol. It is measured based on the ratio of time taken by the packet to reach its destination. The proposed method shows very less end to end delay which means routing protocol has a better end to end delay as compared to other existing protocol. Also, it taken least time for the packet to reach its destination.

Figure 12: Performance comparison of routing overhead



The pictorial representation of routing overhead for proposed and existing technique has shown in figure 12. It is measured based on the ratio of total packet size including packet request and error rate to the delivered data to the destination (total packet size). The comparison shows, the proposed method outer performs the existing method in terms of reducing the routing overhead in a network.

5.0 Findings and conclusion

In this study, secured routing protocol BF-ICMHSRP based on the hybrid combination of bat and firefly optimization is proposed. In this technique, with the integration of inter and intracluster multihop route formation, the efficient cluster setup is formed within which the communications among the nodes are performed with lesser cost, and the optimal path between the source and destination node has been established with hybrid bat and firefly optimization approach. Moreover, within this proposed approach, pair and identity based cryptographic key generation is framed to provide the enhanced security in the routing process by generating the ID based on DSA such that the generated ID could not be altered by the node during its MANET's lifetime which avoids the inappropriate usage. The simulation of the proposed secured routing protocol was performed using NS2 and its performance was evaluated with certain performance metrics which indicated that the proposed algorithm outperformed the conventional bio-inspired routing approaches with its reduced routing overhead value, improved throughput, high PDR, lesser end to end delay, reduced energy consumption and better RSS and LAT. Therefore, the future research should be focused on the advancement of the proposed protocol by considering improved performance with lesser route breakage and to maintain the load balance in case of larger traffic. Moreover, this work could be extended to implement in real MANET based Battlefield Communication System applications.

References

Ahmadi, M., Shojafar, M., Khademzadeh, A., Badie, K. & Tavoli, R. (2015). A Hybrid Algorithm for Preserving Energy and Delay Routing in Mobile Ad-Hoc Networks. *Wireless Personal Communications*. 85 (4). p.pp. 2485–2505.

Baisakh, B. (2013). A Review of Energy Efficient Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. *International Journal of Computer Applications*. 68 (20). p.pp. 6–15.

Basurra, S.S., De Vos, M., Padget, J., Ji, Y., Lewis, T. & Armour, S. (2015). Energy efficient zone-based routing protocol for MANETs. *Ad Hoc Networks*. 25. p.pp. 16–37.

Behera, A. & Panigrahi, A. (2015). Determining the Network Throughput and Flow Rate Using GSR and AAL2R. *International Journal of UbiComp*. 6 (3). p.pp. 09–18.

Bhavsar, C. (2014). *A Survey on Cross-Layer Reliable Routing Protocols in MANETs*.

Biradar, A. & Thool, R.C. (2014). Reliable genetic algorithm based intelligent routing for MANET. In: *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*. January 2014, IEEE, pp. 1–8.

Biradar, A., Thool, R.C. & Thool, V.R. (2014). Genetic Algorithm Based Unipath and Multipath Intelligent Routing for Mobile Ad-hoc Networks. *International Journal of Advances in Computer Science and Technology*. 3 (4). p.pp. 276–282.

Ebrahimi, M. & Jamali, S. (2016). Securing AODV Routing Protocol Against the Black Hole Attack Using Firefly Algorithm. *International Journal of Applied Operational Research*. 6 (4). p.pp. 53–63.

Gopinath, S. & Nagarajan, N. (2015). Energy based reliable multicast routing protocol for packet forwarding in MANET. *Journal of Applied Research and Technology*. 13 (3). p.pp. 374–381.

Javaid, N., Khan, Z.A., Qasim, U., Jamil, M., Ishfaq, M. & Alghamdi, T.A. (2015). Modeling Routing Overhead of Reactive Protocols at Link Layer and Network Layer in Wireless

Multihop Networks. *Mathematical Problems in Engineering*. [Online]. 2015. p.pp. 1–14. Available from: http://www.hindawi.com/journals/mpe/2015/105245/.

Junhai, L., Danxia, Y., Liu, X. & Mingyu, F. (2009). A survey of multicast routing protocols for mobile Ad-Hoc networks. *IEEE Communications Surveys & Tutorials*. 11 (1). p.pp. 78–91.

Kanani, C. & Sinhal, A. (2013). Ant Colony Optimization based Modified AOMDV for Multipath Routing in MANET. *International Journal of Computer Applications*. 82 (10). p.pp. 14–19.

Kaur, N. & Kumar, D. (2017). *Modified Bio Inspired Technique to Improve Performance of MANETs*. [Online]. 3 (6). p.pp. 95–98. Available from: https://wwjmrd.com/upload/1507805713.pdf.

Li, F. & Wang, Y. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*. 2 (2). p.pp. 12–22.

Prabha, R. & Ramaraj, N. (2015). An improved multipath MANET routing using link estimation and swarm intelligence. *EURASIP Journal on Wireless Communications and Networking*. (1). p.p. 173.

Rafsanjani, M.K. & Fatemidokht, H. (2015). FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs. *AEU - International Journal of Electronics and Communications*. 69 (11). p.pp. 1613–1621.

Sharma, S. & Patheja, P.S. (2002). Improving AODV Routing Protocol with Priority and Power Efficiency in Mobile Ad hoc WiMAX Network. *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*. 2 (1). p.pp. 87–93.

Singh, G., Kumar, N. & Verma, A.K. (2014). ANTALG: An Innovative ACO based Routing Algorithm for MANETs. *Journal of Network and Computer Applications*. 45. p.pp. 151–167.

Sumathi, M. & Gunasekaran, M. (2018a). ACO based AODV Method for Detection and Recovery of Misbehaving Node in MANET. *Global Journal of Computer Science and Technology: E Network , Web and Security*. 18 (1).

Sumathi, M. & Gunasekaran, M. (2018b). ACO based AODV Method for Detection and Recovery of Misbehaving Nodes. *Global Journal of Computer Science and Technology*. 18 (1).

Taheri, S., Hartung, S. & Hogrefe, D. (2015). Anonymous group-based routing in MANETs. *Journal of Information Security and Applications*. 22. p.pp. 87–98.

Tseng, Y.-C., Ni, S.-Y. & En-Yu Shih (2003). Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network. *IEEE Transactions on Computers*. 52 (5). p.pp. 545–557.

Uddin, M., Taha, A., Alsaqour, R. & Saba, T. (2017). Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function. *IEEE Access*. 5. p.pp. 10369–10381.

Zhang, X.M., Zhang, Y., Yan, F. & Vasilakos, A. V. (2015). Interference-Based Topology Control Algorithm for Delay-Constrained Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*. 14 (4). p.pp. 742–754.

Zhao, S. (2012). *Scholarship At Uwindsor Identity-Based Cryptography To Mobile Ad-Hoc Networks Identity-Based Cryptography To*.

End of the Sample Work