CLBNSRM - CONFIDENCE LEVEL BASED UNBLEND NEIGHBOR SELECTION &BLEND NODE REPORT BASED OPTIMIZED ROUTE FORMATION IN MANET

S. J. Patil[1],L.S. Admuthe[2] and M. R. Patil[3]

[1]Research Scholer,Department of Electronics and Communication,
VTU, RRC, Belgavi, Karnataka, India.
[2] Department of Electronics Engineering, DKTE'S Textile & Engineering Institute,
Ichalkaranji. Maharashtra, India.
[3]J.A.G.M. Institute of Technology, Jamkhandhi, Karnataka, India.

ABSTRACT

A mobile Ad-hoc network (MANET) is an impulsive network that can be recognized with no predetermined infrastructure. To achieve safe path selection cryptographic key exchange was implemented mostly in turn of huge computational cost. Confidence based coordination in MANET focuses on routing challenges created by selfish nodes, as energy utilization & time factor are key issues in this aspect. The present protocol is focused on fuzzy optimization-based node confidence estimation and path selection with minimum energy utilization. The node with maximum confidence value will give high priority to include in the path for transmission. In the implemented protocol to build a novel confidence-based model multidimensional factors like confidence value, link cost, degree of node and node energy are included as decision-making factors. The proposed protocol CLBNSRM estimates confidence level in four steps to decide a trustworthiness of neighboring node. To estimate the efficiency of the present confidence model various protocols are compared by using attributes like the number of nodes, node speed, malicious node variation, etc. Moreover, different parameters like Packet delivery ratio, Throughput, Residual energy, and Packet dropped are considered with these attribute variations. Experimental results indicate that PDR and Throughput increase although in presence of malicious nodes, along with the utilization of minimal energy. Statistical analysis is carried out for mathematical modeling. This analysis shows that a linear model of an implemented protocol is better than compared protocol with all the aspects.

KEYWORDS

MANET, Path Selection, Confidence, Priority, Fuzzy Optimization.

1. INTRODUCTION

A mobile Ad-hoc network (MANET) is a self-constructed system with many wireless mobile nodes. The nodes in the network do not only act as destination node but also forward packets to neighbor nodes as a router. Hence, its popularity has been increased due to its vast application in the field of military action, emergency rescue operations, law enforcement and security prone environments. Rapid expansion in mobile devices and interest in mobile communication, mobile Ad-hoc networks have been receiving a lot of attention in the recent past [1].

The mobile Ad-hoc network (MANET) is susceptible to various attacks due to its features like dynamic topology, open environment, limited physical security, limited bandwidth, energy exhaust, etc. The various attacks are imposed in MANET due to its easy compromisation [2].

DOI: 10.5121/ijcnc.2020.12206

Since the attacks like a black hole, gray hole, DoS are interrupting node communication lead to losing integrity, loss of authenticity and exhaust of battery power consequently collapse of the network. Hence, standard Ad-Hoc communication needs data validation against misbehaved nodes. Trust estimation based structural design is the recent trend in the mobile network. In the past, key sharing security systems are engaged to attain defence however, they might have invited further computational cost and raises the overhead complexity. The cryptographic key sharing consists of encryption and decryption methods with a reliable third-party device placement that controls the key sharing, signatures, hash functions and node privacy [3]. But these judgments fail to handle the malfunction of node position, where the node drops the packets. In case, that data gets modified by any node is also needed to be checked and eliminated from the network.

Confidence based defence mechanism is considered to compute the belief cost of each node based on the sequence of contact records passed out by that node. The character-based confidence values are computed based on unblendU_B(one hop) and blend B_N(two hop) node reports. If the contact is unbeaten, then the communicated node is measured as a confident device. The unblend(U_B) contact may be bogus due to, instant link loss and blockage. Although confidence is computed based on character record, for that correct validation is required to carry further communication. If the volume of the contract record increases, the confidence level get weakens.
The confidence level based optimized path selection preserves confidence accounts of each device and uses effortless statistical functions to work out the confidence in its nearby nodes. The C_L based path establishment using fuzzy logics not only watching the character of the node but also assists to pick up the output result. In the environment, the node accumulates a packet of the previous node and retransmit it to the next hop up to the ultimate destination. The broadcast among the nodes measured as uniform qualities and it uses 802.11 wireless network MAC standards. These wireless channels are susceptible to some form of harassment imposed by egotistic or miss behaved nodes.

In this proposed protocol, opinion-based confidence assessment and route formation based on the fuzzy decision is implemented. The discrimination of the reliable node and a malicious node is identified by computing confidence level C_L for all nodes based on the U_B knowledge and advice of the node from its nearby nodes.

The rest of the article is organized as follows: Section 2 gives a short overview of trust management and routing protocols. The points and steps made to implement CLBNSRM are described in Section 3. In section 4 simulation model and parameters considered are discussed. In section 5 results are discussed and statistical analysis is carried out. InSection 6, the conclusion of the present study and scope for future work are discussed.

2. Related Works

In recent years, a lot of research work has been undertaken on trust management models, attacks on MANET and trust-based protocols. Although the application of trust management models in mobile agent systems has received much attention, still overall efficient models including the energy system have to be received. In this section related research work regarding trust management models, attacks and trust - based protocols with fuzzification are discussed in brief.
Generally routing protocols in Ad-hoc networks are classified as proactive & reactive. Proactive routing protocols are table-driven protocols and need more computational cost. This may result in to high utilization of bandwidth and energy which are generally known to be limited resources. However, reactive routing protocols are on-demand routing protocols which find the path to the destination whenever necessary, hence limited resource like bandwidth and energy are conserved. Therefore, later one has driven the attention of researchers in MANETs. Perkins et.al.[4] have put forwarded single path routing protocol AODV which is the combination of DSR and DSDV. In this protocol, authors consider that every node is co-operative and honest.

In the existence of security protocol reduction of attacks can be achieved. The mobile hosts dynamically found paths among one another for communication. Consequently, the accomplishment of MANET communication highly relies on the association of the involved mobile nodes [5]. MANET, networks are more susceptible to attacks than infrastructure networks. So, safety is a vital issue in MANET to afford secure communication among mobile nodes [6]. During the previous decade, broad studies have been conducted on routing in mobile ad-hoc networks, and have resulted in a number of established routing protocols [7]. Ad-hoc networks frequently suffer from malicious attacks because of its features like dynamic topology, lack of central monitoring and management, open medium, no clear defence mechanism. These factors have distorted the combat field circumstances for the MANET against the security pressure [8]. The ultimate goal of the security solutions for MANETs is to provide security evinces, such as authentication, confidentiality, integrity, anonymity, and openness, to mobile users [9]. The design behind hybrid routing protocols is to employ both routing protocols, proactive mechanisms in some areas of the network at convinced times and reactive routing for the rest of the network. The proactive operations are restricted to a small domain in order to diminish the control delays and overheads [10].

Trust-based reactive routing protocols like trusted AODV, DSR & TORA were analyzed through their performance with respect to variation in the number of malicious nodes along with another experimental setup Pirzada et.al [11]. According to Guo. et. al. [12] Trust-DSR facilitates five route selection strategies that are dependent on trust evaluation of transmission links. Since the selection of route is limited on route gained from standard DSR. However, the ultimately selected route might not be necessary the most trusted. Xia. et.al [13] have discussed the trust administration model for mobile Ad-hoc networks based on the systematic hierarchy process and fuzzy theory. In this research trusted routing algorithm, reactive routing protocol based on standard dynamic source protocol and fuzzy trusted dynamic source routing protocol is proposed. In this work, authors have focused on direct trust, recommended trust, incentive function, and the active degree to calculate overall trust. Furthermore, in recommended trust direct recommendation experience and indirect recommended experience have been considered as analytical hierarchy process and fuzzy theory.

A fuzzy-based Ad-Hoc on-demand distance vector routing protocol was put-forwarded by Manicakam [14] and fuzzy logic is used for evaluating trust. The Threshold trust value was set so as to verify the trust on the neighbor's node. Here, in this protocol only modified attacks were identified, that only at the route discovery stage. Junhai et.al [15] implemented a trust model based on the fuzzy recommendations for mobile Ad-hoc networks. In this model, authors have included five types of fuzzy trust recommendation relationships based on fuzzy relation theory and a mathematical description for MANET's. Furthermore, authors have considered fuzzy direct trust model, fuzzy indirect trust model and the fuzzy global trust model for calculating overall trust on the neighbor node. In-depth, the fuzzy recommendation trust model, fuzzy transitivity recommendation trust model and fuzzy consensus recommendation trust model were considered for calculating the fuzzy indirect trust. This protocol has considered average energy consumed as a matrix, but still, energy cost for computing trust value is not considered. Furthermore, this model neither considered average energy consumed nor residual energy in comparison with other trust models.

Shuaishuai et. al. [16] have proposed a novel trust management system, so as to secure the data plane of Ad-hoc networks. In this management system fuzzy logic is used to calculate the path trust while graph theory is adopted to calculate node trust value. In fuzzy-OLSR, authors have [17] considered only first handed information and purposefully avoided second-handed information to overcome the overhead problem in the network. But in this model along with first-hand information, second and third hand information are gathered so as to build not only trust but also confidence on a neighboring node. Although in fuzzy-OLSR importance given to overhead, the confidence on the neighboring nodes is more important hence the present study is focused on secured path without running the confidentiality. However, energy -efficient module is also included so as to improve the performance of the protocol.

3. FUZZY BASED CLBNSRM IMPLEMENTATION

In the present confidence model estimation of confidence, assessment of confidence, estimation of U_B confidence of nodes, confidence of blend nodes, and overall, the confidence level was considered.

3.1 Confidence Estimation:

Confidence is a conviction of a node on a new device for a definite mission. A confidence network is measured as a bound for subjective chart $C=\{D, N, t\}$,where $D=(d_1, d_2, \ldots.d_n)$describes the device counts in the region and N = {n_{12}, n_{23} …n_{ij}}, $i \neq j$, is the confidence association between neighbors in$D$, n_{ij} is the U_B link between two neighbors d_i and d_j, that brings$t$. The confidence assessment between 0 to 1, signified by,CL (n_{ij}) ε [0,1], and |N| is the count of $U_B$links in the environment.

- All nodes observe and record the character of its neighbors in the random deployment environment.
- Each node will also collect the character of its next neighbor from blend nodes (BN) and record it for additional validation.
- Every node has the knowledge to compute the confidence of its neighbors based on the transactions handled between them.

Usually, trust-based protocols do not give precise results with respect to stratification in depth. Here, fuzzy logic is a significant tool through which one can precisely stratify the confidence level. Hence, fuzzy logic is used to compute C_L based routing for proper decisions.

3.1.1 Confidence Assessment:

Confidence assessment (C_A) is computed for each node to recognize its character and consistency for efficient contact. To achieve the confidence level (C_L) from the network the subsequent assumptions are prepared

- The communicating nodes forever having confidence in themselves.
- Almost all nodes should behave & co-operate with each other.
- A Minimum number of nodes might misbehave as selfish in the network.
- The C_L of the route is computed based on the honest transaction between nodes.

Nodes need to check the packet forward count (F_C) which is the ratio of the number of packets forwarded correctly to the number of packets supposed to be forwarded. Packet lifetime (P_{LT}) is the TTL value from the packet header. HopCount(H_C) is total number of hops. Packet Loss Count (P_{LC}) is the total number of packets dropped in the network and Resend (R_S) is the timer, when it becomes zero, source has to send packet once again. Source packets can be retransmitted based on the complete confidence in the route nodes and the strength of the channel in the path. A confidence assessment needs to record honest co-operation between the U_B nodes which is shown in Figure.1 and their third neighbor confidence report. In this way selfish behavior is measured in this network.

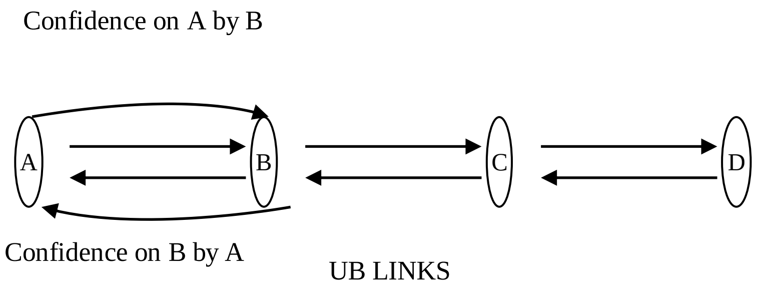


Figure1.Unblend Links

Algorithm 1: Confidence Assessment C_A

```
Initiate $C_L$ Verification(i,j)
{
if ($U_B$(i,j)node $F_C$ = $C_L$ &&$P_{Lc}$<$C_L$ then
{
if ($H_C$ >0) then
{
Check $P_{LT}$ > 0
Forward Data to j
} else
{
Drop packet
}}}
```

Algorithm 1 (pseudo code) shows how confidence assessment is done. Initially, packet forwarding count and packet loss count are checked with C_L. If it is less than C_L, then two more conditions are checked such as hop count and packet life count. If these are greater than zero the packet will be sent to next node j, otherwise, packet will be deleted.

3.1.2 UB Confidence Estimation between Nodes (Direct):

The U_B confidence is computed by estimating the characteristics of its face-to-face next U_B neighbor reportsC_R. To compute the U_B node confidence at every interval, just make- believe that the confidence implications of each node must be equal to 1 at the initial stage of the communication to all nodes. Algorithm 2 gives an idea about how the U_B trust estimation between two adjacent nodes. The received data is checked for hop count, end of the queue and validation of packet expiry count, if it satisfies, then packet forward count will be updated otherwise P_{LC} will be updated. If it doesn't satisfy the above condition, then U_B trust level will be updated by using the formula stated in equation 1.

Algorithm 2: UB Trust Estimation between Nodes

```
Once receiving the data
        if ((hc !=0) || (queue != deadline) {
        if ($RS < PLC$)     {
Validate packet expiry time, before PLC, if yes
        $FC = FC + 1$  Update forward count
             } else
              {
        $PLC = PLC + 1$  Declare Attack Presence
               }
               }
j drops data after collecting, then validate
        else if ($hc == 0$) || (Queue == Deadline) {

        $PLC = PLC + 1$  Selfish Node
             }
        Update the UBCL.
        return TL
```

$$UBCL(ij) = \frac{s}{s+(\gamma * f)} \tag{1}$$

Where,

s = packet send number.
f = Received Hello count
γ = Conversion factor.

Which is calculated as follows:

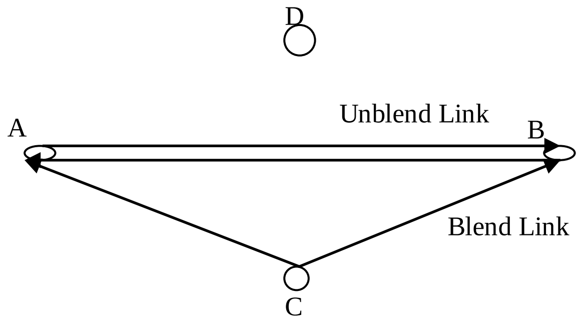
$$\gamma = 1 + \frac{\log_{10}\frac{(1+f)}{(s+f)}}{\log_{10} 2} \tag{2}$$

3.1.3 BLEND Nodes Confidence Report (Indirect):

The B_N confidence report is collected based on the suggestions from the other neighbors. In this case nodeihas zthadjacent nodes in the surroundings where,ρ ={n_1,n_2....n_z} that is sum of nodes in the network. Imagine that node ¡likes to maintain a confidence-based dealing with its second B_N inside ith area that is HC>*1*.

The B_N confidence is gained from the nearest nodes reports as shown in Figure 2. Initially, node verify the C_L of all its nearby $U_B$neighbors and make a decision to select a collection of nodes whose confidence (C_L>L) than the given limitations L as shown in algorithm 3. Also, within the node ¡coverage rangeR_C, it broadcast theC_L report through the message of confidence level report announcement C_{LRA} to all of its nearby nodes j. The C_{LRA} message reached up to the B_N node. Let j, be the neighbor node and neighbor of neighbor, which is located within the $U_B$and B_N neighbor of ith node limitation. Later, the nodes of j will send a reply to the node ¡enclosed with $C_L$report as $C_{LRA\text{-}replay}$message. So, theB_N report C_L about node i can be computed and tag with reply message as

$$B_{Nij} \; = U_{Bij} \times U_{Bjz} \tag{3}$$



C – States the Confidence about B to A

Figure 2. Blend Node Confidence

Algorithm 3: Blend node confidence check

```
$B_N$ Checks $C_L$ (i,j) in second hop {
For$i$ = 0 to $C_{LRA}$ Message time {
Obtain thenearby nodes $C_L$ Report
node[i]=id(i);Check Node address as identification
}
if $C_L$ ((node[i] $U_B$) > L ) then {
$C_L = C_L +1$
$C_L[i] = \frac{U_{Bij}}{\sum_{j=1}^{z-s} U_{Bij}}$,
        }}
}
```

The B_N nodeC_L report obtained from the nearby second hop neighbor nodes may beC_L< L, then the observing confidence report obtained from the C_R of a node may produce the terrible suggestions about ith node. So, the witnessing nodes of neighbors notices and removing the selfish nodes whose C_L is less than the L and thus the network is protected by the unkind remarking nodes. The C_L of all nodes will be computed and updated in a C_L report as shown in table 1. Here the value of C_L sorts off least value 0 which signifies as dishonest node to maximum value 1 indicates the complete C_L of a node.

Table 1: Node CL Report

C_L	C_L **Linguistic**
$0 < 0.3$	Absolute Selfish
$0.3 \le n < 0.5$	Suspicious
$0.5 \le n < 0.7$	Least C_L
$0.7 \le n < 0.8$	C_L
$0.8 \le n \le 1$	High C_L

The algorithm 4 shows that the device i can construct a C_L path to j through z - s routs, in case the $B_N C_L$> L of j. If so, node i will select one of its nearby devices with the greatest C_L, to resend the data to j. The fuzzy C_L path selection supports the linguistic form (LF) as confidence scores of a node on the other nodes.

Algorithm 4: Blend nodeB_N confidence $C_L$update

```
For i =1 to d
 {
Update $C_L$ [j]
 }
i$^{th}$node updates the $C_L$ from z$^{th}$ node by

                    $C_L$ [i] =$\frac{U_{Bij}}{\sum_{j=1}^{z-s} U_{Bij}}$, else
          }
          Update $C_L$
```

3.1.4 Overall Confidence Estimation

Equation 4 depicts that the overall confidence is computed based on the suggestions observed from the nearby nodes, as well, based on direct confidence. Each U_B and $B_N$will compute the C_L of its nearby nodes based on the truthful packet relocation within the expiry period. At initial C_L and the link, abilities are assigned as 1.

$$OC = \beta * UBCL + (1 - \beta)BNCL \tag{4}$$

3.2. Fuzzy Logic

Fuzzy logic is a multi-valued logic in which the values of variables may be any real number between true (1) and false (0). With fuzzy logic, an input can be mapped into an output space.

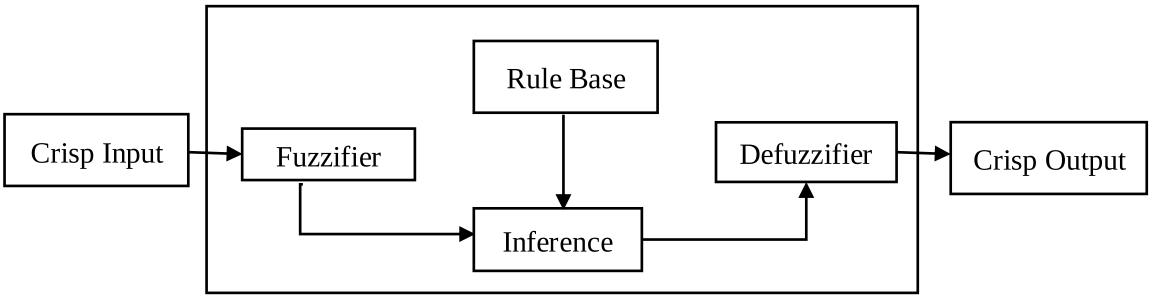


Figure 3. Fuzzy logic architecture

Fuzzy logic is composed of if-then rules. The if-part of the rule is called the originator while thenpart is called the consequential. A fuzzy logic system maps crisps inputs to crisp outputs. There are four mechanisms in a fuzzy logic system, namely rules, fuzzifier, inference mechanism, and defuzzifier as shown in Figure 3. Rules are fundamentally if-then rules which must be evaluated during an input/output process. The output of the system depends on these rules. Fuzzifier is responsible to take crisp numbers as input and give fuzzy sets as output. The beginning of rules is dependent on the output of the fuzzifier. The Inference mechanism in the fuzzy logic system is the decision making part. Defuzzifier maps the fuzzy output of the inference mechanism into crisp numbers to make it function for further processing by the system [18]. A triangular fuzzy number is chosen for better results and can be defined by a triplet (a1, a2, a3). The membership function is shown in equation 5.

$$\mu A(x) = \begin{cases} 0, & x < a1 \\ \frac{x - a1}{a2 - a}, & a1 \leq x \leq a2 \\ \frac{a3 - x}{a3 - a2}, & a2 \leq x \leq a3 \\ 0, & x > a3 \end{cases} \tag{5}$$

3.2.1 Fuzzy Inputs:

Total four inputs (Linguistic variables) used as crisp set of fuzzy. These are discussed in this section

1. Node C_L**:** Node C_L above 0.8 in the path is considered. Here node C_L is calculated based on blend confidence and suggestion of nearby nodes. The mean value of the unblendC_L of the nearby nodes that are having a superior suggestion is only considered.

$$CL = \beta * UBCL + (1 - \beta)BNCL \tag{6}$$

2. Channel Bandwidth: It is considered to know the capacity of the link. It is a ratio of bandwidth to node MAC bandwidth.

$$C = \frac{Bandwidth}{NodeMACbandwidth} \tag{7}$$

3. Hop count: It gives the total number of intermediary nodes through which data must go by a source to destination. It is considered to get the shortest path from source to destination. Energy obligation is directly proportional to the hop count so the hop count plays a major role in saving the node energy.

4. Node Energy: The node energy is calculated by using the following formula and used as one of the inputs of a fuzzy crisp set.

$$Egy = \sum \frac{Egy}{IE} \tag{8}$$

Where, IE is the initial energy

3.2.2 Fuzzification membership functions:

The set of memberships for the given inputs are the triangular function and the different range of the input as mentioned in table 2.

Table 2: Parameters Chart

Parameters	**Rules**		
C_L	Superior	Standard	Low
Hops	Superior	Standard	Low
Channel Bandwidth	Superior	Standard	Low
Node Energy	Superior	Standard	Low

In general, using fuzzy inference decision-based path selection corresponds to C_L specified as linguistic forms (LF). The process of Fuzzification links the input to the equivalent LF as low, standard and superior as shown in figure 4.

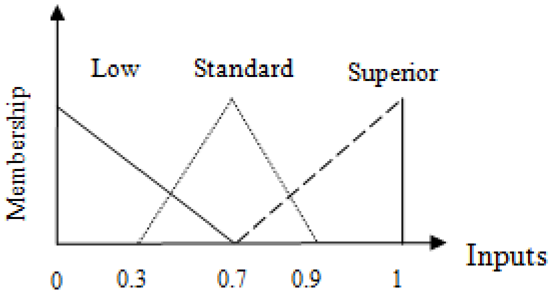


Figure 4. Membership Functions

3.2.3 Output of fuzzification:

The final output of the present fuzzification model obtained in five levels as shown in figure 5.

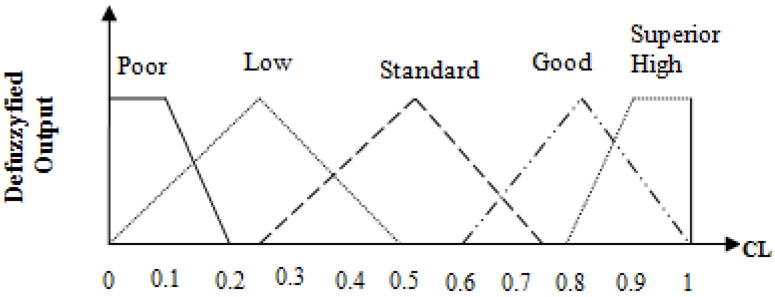


Figure 5. Defuzzyfied results for C_L

In the present model, four inputs were given to the fuzzy system and five levels of confidence were obtained varying from 0 to 1. Here 0 indicates poor C_L while 1 indicates superior high C_L. In between poor and superior high another three levels of C_L were obtained that is a low standard and good. The collection of LF sends the C_L of the route is given by

C_L-PATH = Superior high / Good / Standard / Low / Poor as end result.

3.3 Statistical Analysis:

The statistical analysis was carried out by feeding the results of protocols in the software R-3.4.2. The correlation analysis was done for attributes and parameters regarding to all three models. To check significance level p-values were calculated. Furthermore, the generalized linear regression model was fit for protocols to obtain future values of particular attributes for various parameters.

4. PERFORMANCE EVALUATION

4.1. Performance Evaluation

To observe the performance of CLBNSRM, AOTDV and AOMDV NS-2.34allinone simulator is used. The application layer protocol used was Constant Bit Rate (CBR) it generates the data in the network. The Transport agent used was User Datagram Protocol (UDP) which configures the transport layer. Two Ray Ground model was used as the propagation model. This model is appropriate for long-distance communication. As shown in table 3 the simulation model considers a square network area of 1000m x 1000m to transmit data packets of 512 bytes. The node variation considered is 50 to 150 with a step size of 25 nodes. The network is simulated for 100 seconds and repeated for various attributes. The performance of the proposed CLBNSRM is evaluated and compared with the existing AOTDV and AOMDV. To get better results from various attributes like number of node variation, node speed variation and the number of malicious nodes variation is considered. The simulation parameters are summarized as shown in Table 3.

Table 3: Simulation parameters considered

Network Simulator	NS-2.34allinone
Network area	1000 X 1000
Number of nodes	50, 75, 100, 125, 150.
Speed of the nodes	0, 5, 10, 15, 20, 25, 30m/s.
Malicious nodes	1, 2, 3, 4, 5.
Traffic load	CBR
Packet Size	512 bytes
MAC protocol	IEEE802.11b
Simulation time	100s. and repeated for various attributes

4.2 Performance metrics considered

4.2.1**Packet delivery ratio:** The ratio of the data packets delivered to the destination nodes to those sent by the source nodes.

4.2.2**Throughput:** It is the average rate of successful message delivery over a communication channel.

4.2.3**Residual Energy:** The remaining energy of the nodes in the network is called as residual energy.

4.2.4 **Packets Dropped:** It is the total number of packets dropped in the network.

5. RESULT AND ANALYSIS

In the present study number of performance, matrices is analyzed for AOMDV, AOTDV, and CLBNSRM and represented in graphs. Performance matrices like Packet delivery ratio, Number of packets dropped, Throughput and Residual energy is considered. These performance matrices also corresponded with various attributes like the number of nodes, node speed and number of malicious node variation.

In node variation, the number of nodes was varied between 50 and 150 with a step size of 25 nodes, node speed 25m/s, pause time 20s, area considered 1000m x1000m and simulation time 100s. In the node speed variation, the nodes start with a low velocity of 0 m/s and then the node velocity increases up to 30 m/s. The data rate is kept constant and the number of nodes and pause time was fixed at 50 and 25 respectively.The third scenario is considered by varying malicious nodes from 1 to 5. In this setting the total number of malicious nodes in the network was inserted purposefully to observe its effect on different parameters like PDR, throughput, packet dropped, residual energy, etc.

5.1 Packet delivery ratio:

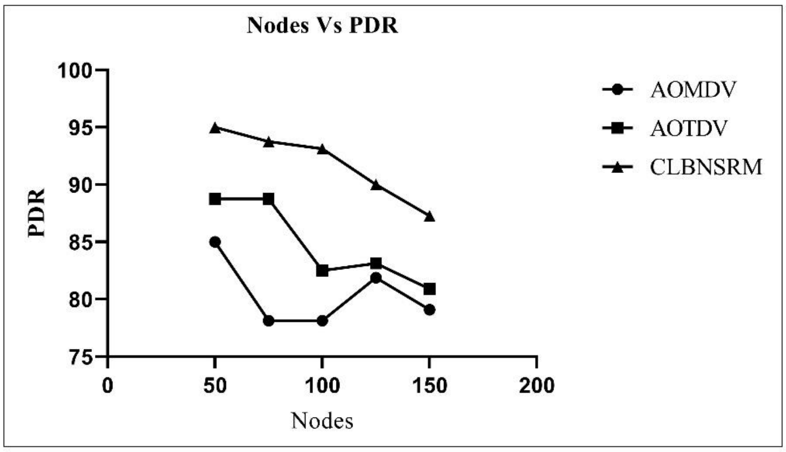


Figure 6. Comparison of nodes Vs packet delivery ratio.

The Packet delivery ratio has been evaluated by corresponding node variation which is presented in figure 6. Results show that PDR was more in CLBNSRM as compared to AOTDV and AOMDV in every variation with respect to a number of nodes. Among the three protocols proposed CLBNSRM shows the best output than others. Due to the selection of neighbors based on confidence the path was constructed properly. Ultimately minimizes the packet misuse and dropdown hence increases the PDR.

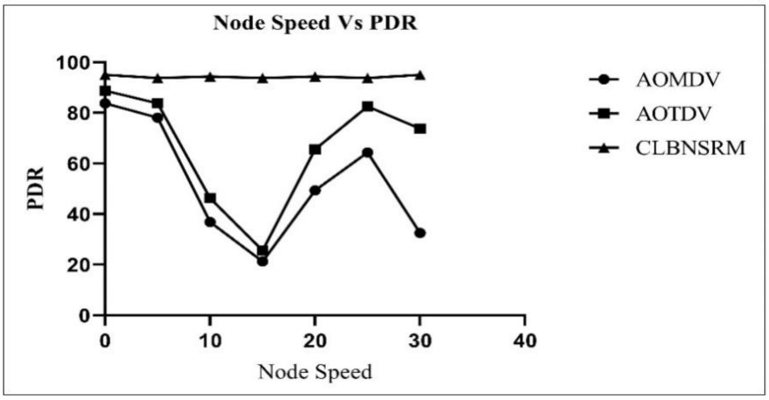


Figure 7. Comparison of node speed Vs packet delivery ratio.

The Packet delivery ratio was corresponded with node speed and is shown in figure 7. The packet delivery ratio with reference to AOMDV and AOTDV shows dropping initially up to node speed 15 m/s and a gradual increase was noted up to 30m/s and thereafter again it was dropping. However, PDR of CLBNSRM has a quietly different scenario. The PDR is comparatively higher and there was no effect observed on PDR with the change in node speed. Precisely, one can say that PDR is significantly better and undisturbed with variation in the node speed.

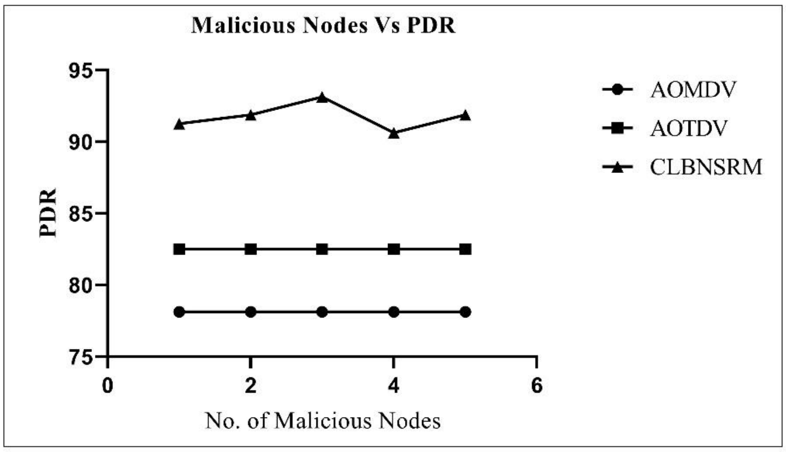


Figure 8. Comparison of malicious nodes Vs packet delivery ratio.

The packet delivery ratio is also corresponded with variation in a number of malicious nodes and exhibited in figure 8. The results for AOMDV and AOTDV show that PDR was lower and further the PDR of AOMDV was lowest than even AOTDV. In comparison with CLBNSRM, it was far better than the other two protocols.

5.2 Throughput:

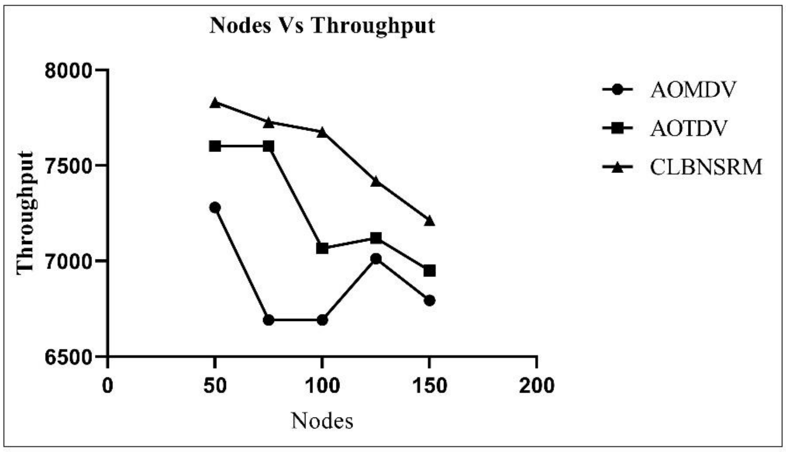


Figure 9. Comparison of nodes Vs throughput.

Evaluation for throughput with respect to AOMDV, AOTDV, and CLBNSRM is given in figure 9. The results of throughput for AOMDV was noticed declining as the number of nodes get inclined up to 100 nodes and slightly inclined at 125 nodes and again declined. However, the results of AOTDV were quite good with reference to the throughput but not satisfactory. In CLBNSRM, throughput level was noticed much higher than the other two protocols. The Throughput of CLBNSRM was declined with an incline number of nodes, but the variation is not significant as compared to AOMDV and AOTDV.

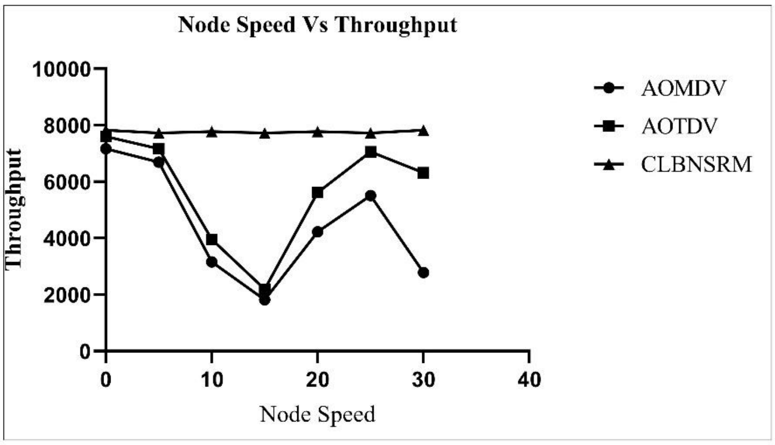


Figure 10. Comparison of nodes speed Vs throughput.

Throughput has corresponded with node speed which was shown in figure 10. The throughput of the present protocol has not much affected by node speed. However, node speed significantly affected throughput with reference to AOMDV and AOTDV. In AOMDV and AOTDV, throughput got declining as the speed of nodes increased up to the certain extent and again gets increased and the sudden drop was noted. The result of CLBNSRM for node speed variation was higher as well as constant.

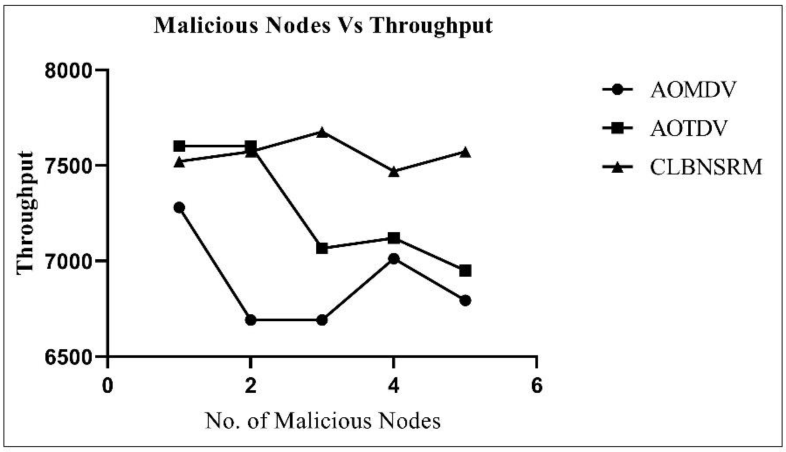


Figure 11. Comparison of malicious nodes Vs throughput.

Throughput has also corresponded with variation in the number of malicious nodes and results are exhibited in figure 11. The Throughput of AOTDV and CLBNSRM was the same when the numbers of malicious nodes were less. But as the number of malicious nodes gets increased in the network, the throughput of AOTDV gets declined while in the case of CLBNSRM it was constant throughout the variation in the number of malicious nodes. On the other hand, the throughput of AOMDV was declined initially and later on it was increased.

5.3 Residual Energy:

Addressing the energy issues in MANET is a need of the present day. There are several protocols in which energy as a parameter was not at all considered. While there are some protocols that have considered energy as parameters. But the energy efficient model was not put forward by any researchers. Here in CLBNSRM protocol, an emphasis is given to energy efficiency. The results of residual energy with respect to node variation for all three protocols are depicted in figure 12. Consumed energy was deducted from total energy to obtain residual energy, so, the residual energy is inversely proportional to consumed energy. In the present study, residual energy for CLBNSRM is higher throughout all variations. However, residual energy for the other two protocols was gradually declining up to 125 nodes and thereafter slight increment was observed.

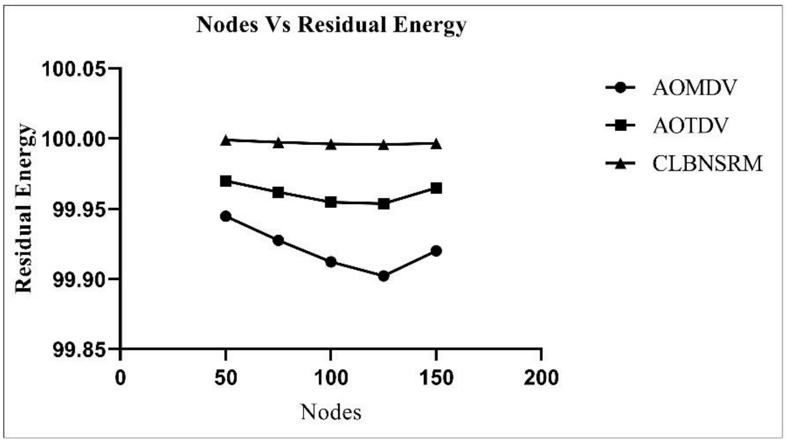


Figure 12. Comparison of nodes Vs residual energy.

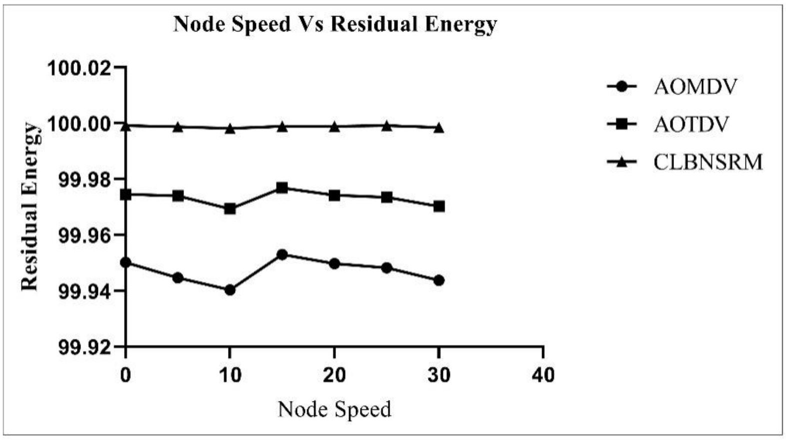


Figure 13. Comparison of node speed Vs residual energy.

Present study is also carried out to evaluate residual energy about node speed (figure 13) and found that CLBNSRM have better result than other two protocols. The study depicts that along with increased node speed variation the residual energy is not at all fluctuate and also saved more energy. It might be due to constant number of nodes which ultimately reduces the control overhead in the network. Hence, in comparison with AOMDV and AOTDV, CLBNSRM is far better to residual energy after varying node speed.

Residual energy was corresponded with introduction of malicious nodes in the network. The results for all three protocols are given in figure 14. The study indicates that CLBNSRM was notably higher as compared to AOMDV and AOTDV. The present protocol efficiently eliminates malicious nodes from the network. Hence, unwanted energy consumption was get reduced and it was conserved as energy.

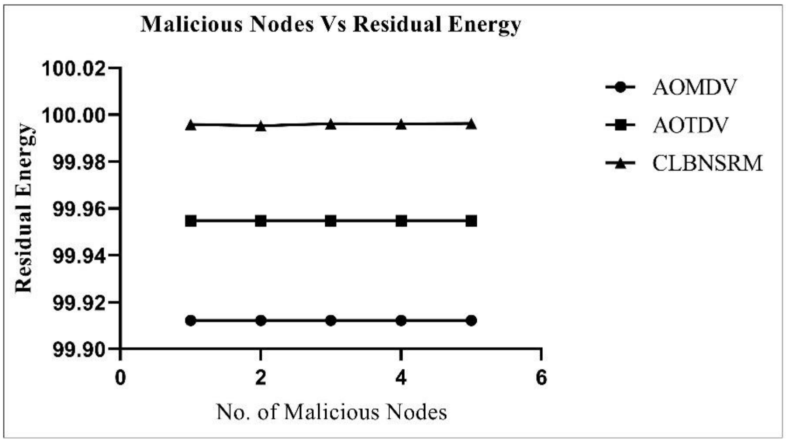


Figure 14. Comparison of malicious nodes Vs residual energy.

5.4 Packet Dropped:

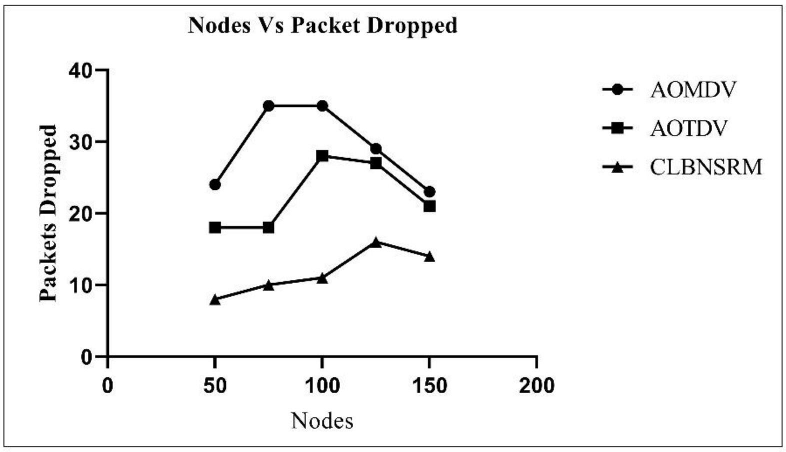


Figure 15. Comparison of nodes Vs packet dropped.

In figure 15. Packet dropped was corresponded to node variation for three protocols. The results indicate that AOMDV and AOTDV have high packet drop ratio. However, in CLBNSRM packet drop ratio is lower up to 100 nodes and there after slight increase was noted. Still in comparison with the AOMDV and AOTDV, CLBNSRM was having minimum packet drops.

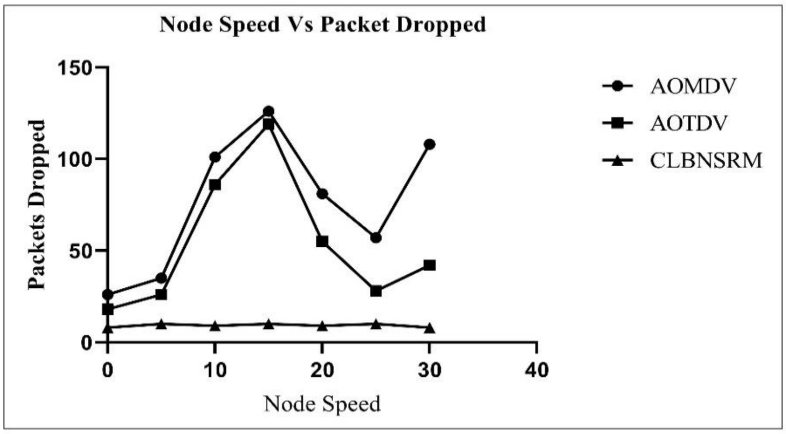


Figure 16. Comparison of node speed Vs packet dropped.

Packet dropped ratio was also corresponded to node speed (Figure 16). The results of packet dropped verses node speed indicated that AOMDV as well as AOTDV have maximum packet dropped at 15 m/s of node speed. In the case of both protocols, throughout all the node speed variation packet dropped was noticed. However, In the case of CLBNSRM packet dropout ratio was noticed minimum.

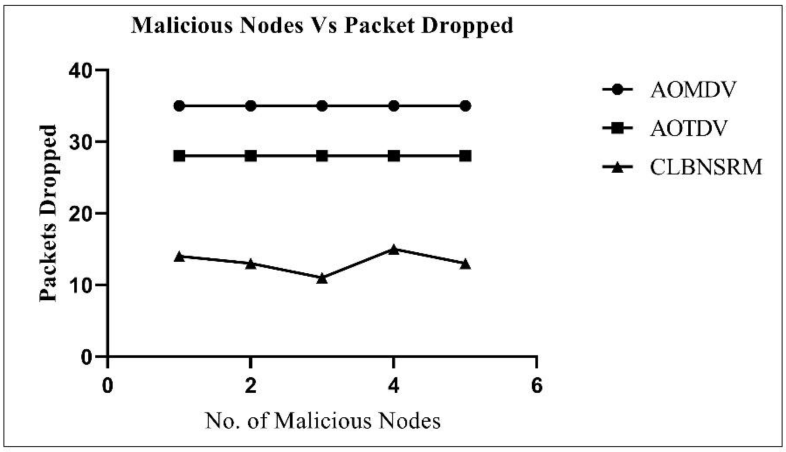


Figure 17. Comparison of malicious nodes vs packet dropped.

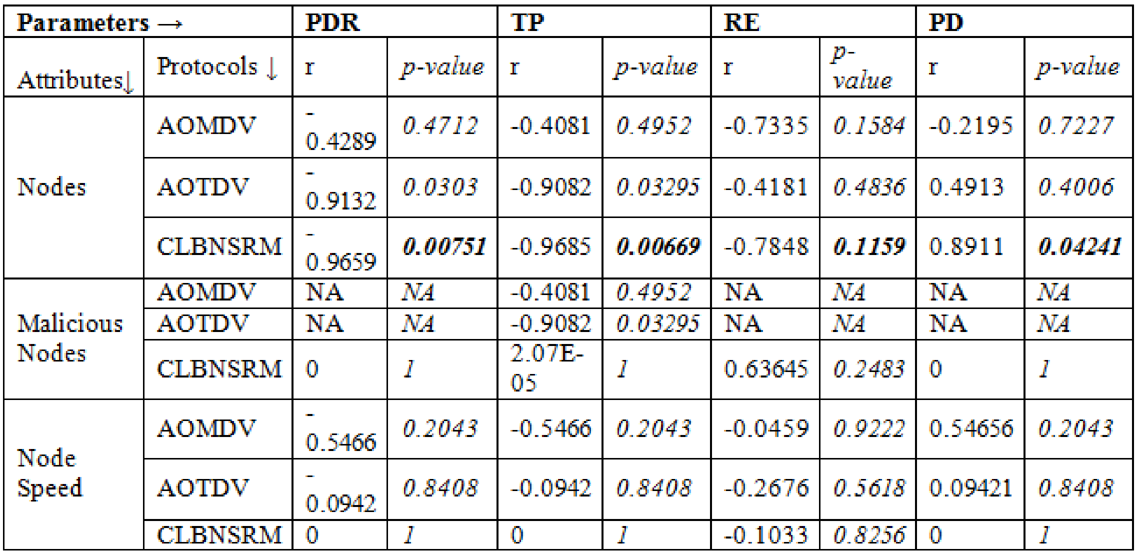
Packet drop to explain the network weakness and improper path selection to exchange the packets between sources to a destination. The above figure 17 shows the minimum packet loss in CLBNSRM than the other available protocols. This shows the strong path selection based on each node confidence level using proposed protocol.

5.5 Statistical Analysis

5.5.1 Correlation Analysis:

In the implemented protocol three different attributes were corresponded with the parameters Packet delivery ratio (PDR), Throughput (TP), Residual energy (RE) and Packet dropped (PD) for AOMDV, AOTDV and CLBNSRM. Since to check Statistical relation between attributes and parameters and also significance level was carried out.

Table 4: Correlation analysis of protocols.



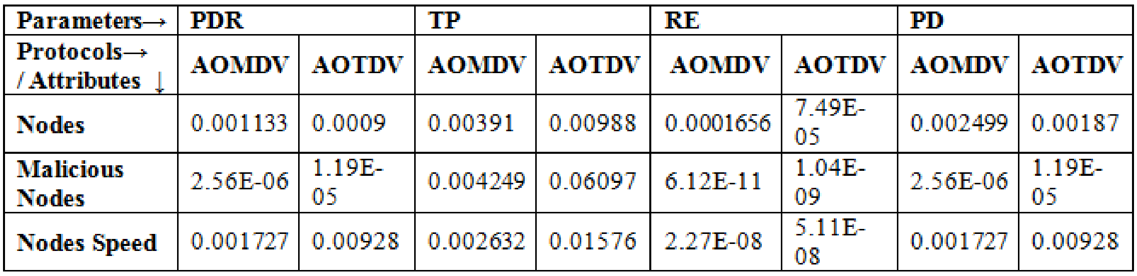
Parameters →		**PDR**		**TP**		**RE**		**PD**	
Attributes↓	Protocols ↓	r	*p-value*	r	*p-value*	r	*p-value*	r	*p-value*
Nodes	AOMDV	-0.4289	*0.4712*	-0.4081	*0.4952*	-0.7335	*0.1584*	-0.2195	*0.7227*
	AOTDV	-0.9132	*0.0303*	-0.9082	*0.03295*	-0.4181	*0.4836*	0.4913	*0.4006*
	CLBNSRM	-0.9659	***0.00751***	-0.9685	***0.00669***	-0.7848	***0.1159***	0.8911	***0.04241***
Malicious Nodes	AOMDV	NA	*NA*	-0.4081	*0.4952*	NA	*NA*	NA	*NA*
	AOTDV	NA	*NA*	-0.9082	*0.03295*	NA	*NA*	NA	*NA*
	CLBNSRM	0	*1*	2.07E-05	*1*	0.63645	*0.2483*	0	*1*
Node Speed	AOMDV	-0.5466	*0.2043*	-0.5466	*0.2043*	-0.0459	*0.9222*	0.54656	*0.2043*
	AOTDV	-0.0942	*0.8408*	-0.0942	*0.8408*	-0.2676	*0.5618*	0.09421	*0.8408*
	CLBNSRM	0	*1*	0	*1*	-0.1033	*0.8256*	0	*1*

Firstly, in the node variation there was a significant correlation corresponded with PDR, TP, RE and PD as in all the parameters p-values are 0.00751, 0.00669, 0.1159 and 0.04241 respectively as shown in table 4. Based on p-values it indicates that CLBNSRM is effective protocol than AOMDV and AOTDV. Although p-value is not significant for malicious nodes and node speed variations corresponded with various parameters in comparison with remaining protocols this protocol shows quite significant.

5.5.2 Model Comparison:

In this section CLBNSRM is individually compared with AOMDV and AOTDV by estimating paired t-test for various attributes corresponded with respective parameters and respective p-values are noted.

Table 5: Comparison of CLBNSRM with other protocols by considering p-values.



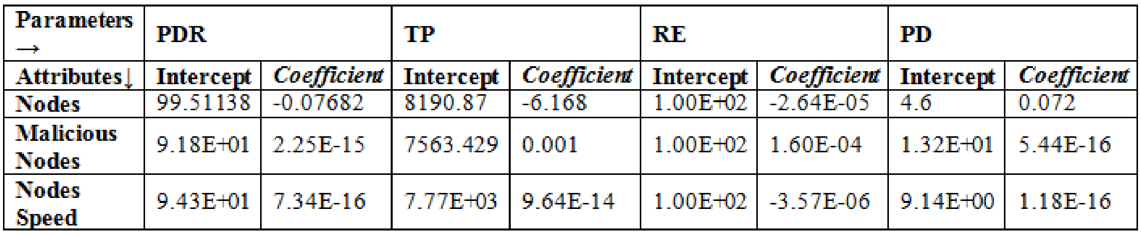
Parameters→	PDR		TP		RE		PD	
Protocols→ / Attributes ↓	AOMDV	AOTDV	AOMDV	AOTDV	AOMDV	AOTDV	AOMDV	AOTDV
Nodes	0.001133	0.0009	0.00391	0.00988	0.0001656	7.49E-05	0.002499	0.00187
Malicious Nodes	2.56E-06	1.19E-05	0.004249	0.06097	6.12E-11	1.04E-09	2.56E-06	1.19E-05
Nodes Speed	0.001727	0.00928	0.002632	0.01576	2.27E-08	5.11E-08	0.001727	0.00928

P-values for PDR, TP, RE and PD about to nodes variation, malicious node variation and node speed variation of CLBNSR with AOMDV and AOTDV is represented in table 5. The results show, that CLBNSRM is highly significant protocol in comparison with AOMDV and AOTDV based on of p-value.

5.5.3 Generalized linear model:

To estimate the mathematical model of implemented protocol generalized linear model is considered. The model gives equation with y-intercept and coefficient of respective attributes as shown in table 6. From these equations, one can estimate the future values of particular attributes.

Table 6: Linear Model between CLBNSRM with parameters and different attributes



Parameters →	PDR		TP		RE		PD	
Attributes↓	Intercept	*Coefficient*	Intercept	*Coefficient*	Intercept	*Coefficient*	Intercept	*Coefficient*
Nodes	99.51138	-0.07682	8190.87	-6.168	1.00E+02	-2.64E-05	4.6	0.072
Malicious Nodes	9.18E+01	2.25E-15	7563.429	0.001	1.00E+02	1.60E-04	1.32E+01	5.44E-16
Nodes Speed	9.43E+01	7.34E-16	7.77E+03	9.64E-14	1.00E+02	-3.57E-06	9.14E+00	1.18E-16

6. CONCLUSION AND FUTURE SCOPE

In the present work, ideal confidence-based model has been proposed. Here unblended and blend confidence were estimated and incorporated into fuzzy logic along with bandwidth, hop count and node energy. This model creates a trustworthy path to the destination by excluding all malicious nodes in the limelight of the fuzzification process. It also facilitates a reliable way to deliver packets. The present protocol discovers multiple trustworthy paths from source to the destination for proper communication. To estimate the efficiency of the CLBNSRM various attributes and parameters were considered and compared with other reactive routing protocols such as AOMDV and AOTDV. Furthermore, the energy module was included and it has been found that the present model is energy efficient than the other considered protocols. In the evaluation of various parameters like PDR, Throughput, Residual energy and Packet dropped by varying attributes like the number of nodes, node speed and number of malicious nodes in the network. Finally, based on a mathematical model it can be concluded that the present CLBNSRM protocol gives a better result than the compared models in all the aspects. For future work, model will be evaluated for various types of attacks. This work can be extended with the neuro-fuzzy technique for confidence calculations.

REFERENCES

[1] S Buchegger, Le Boudec, (2005) Self-policing mobile ad-hoc networks by reputation.IEEECommun. Mag. 43 (7):1-7.

[2] Sun YL, Han Z, Yu W, Ray LKJ (2006) Attacks on trust valuation in distributed networks. Proc. 40th Annual Conf. on Information Sciences and Systems, :1461–1466.

[3] Wu B, Wu J, Fernandez EB, Ilyas M, Magliveras S (2007) Secure and efficient key management in mobile ad hoc networks.J. Netw. Comput. Appl., 30, (3):937–954.

[4] C. E. Perkins and E. M. Royer, (1999) Ad-hoc on-demand distance vector routing. Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, pp. 90-100.

[5] Sachin Lalar, (2014) Security in MANET: Vulnerabilities, Attacks & Solutions. International Journal of Multidisciplinary and Current Research, l (2):62-68.

[6] Mousumi Sardar and Koushik Majumder, (2013) A Survey on Trust Based Secure Routing in MANET. Computer Science & Information Technology (CS & IT), 243-253.

[7] CH V Raghavendran, G Naga Satish, P Suresh Varma, (2013) Security Challenges and Attacks in Mobile Ad-Hoc Networks. I.J. Information Engineering and Electronic Business, 3:49-58.

[8] Swaijit Kaushal, Reena Aggarwal, (2015) A study of different types of attacks in MANET and performance analysis of AODV protocol against wormhole attack. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 4 (2):301-305.

[9] B Harikrishna, N Anusha, G Murali, (2015) Security in Mobile Ad-hoc Networks: Challenges and Solutions. International Journal of Mechanical Engineering and Information Technology, 3 (1):968-971.

[10] P Narendra Reddy, C H Vishnuvardhan, V Ramesh, (2013) Routing Attacks in Mobile Ad-hoc Networks. International Journal of Computer Science and Mobile Computing 2 (5):360-367.

[11] Pirzada A. A, McDonald C, Datta A, (2006) Performance comparison of trust-based reactive routing protocols.IEEE Trans. Mobile Comput., 5 (6):695–710.

[12] Guo W, Xiong ZW, Li ZT, (2005) Dynamic trust evaluation based routing model for ad hoc networks. Proc. Wireless Communications, Networking and Mobile Computing, 2:727–730.

[13] H Xia, Z Jia, L Ju, Y Zhu, (2011) Trust management model for mobile ad-hoc network based on analytic hierarchy process and fuzzy theory. IET Wireless sensor systems., 1(4):248-266.

[14] Martin J, Manickam L, Shanmugavel, S, (2007) Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET. Adv. Comput. Commun. (ADCOM 2007):414–421.

[15] Junhai Luo, Xue Liu, Mingyu Fan, (2009) A trust based on fuzzy recommendation for mobile ad-hoc networks. Computer Networks 53:2396-2407.

[16] Shuaishuai Tan, Xiaoping Li, and Qingkuan Dong, (2016) A trust management system for securing data plane of ad-hoc networks. IEEE transactions on vehicular technology, 65(9):7579-7591.

[17] Zia Liiah, M Khan, I Ahmed, N Javaid, and M. I. Khan. (2016) Fuzzy-based trust model for detection of selfish nodes in MANETs. IEEE 30th International Conference on Advanced Information Networking and Applications. :965-972.

[18] Jerry M Mendel, (1995) Fuzzy logic systems for engineering: a tutorial. Proceedings of the IEEE, 83(3):345–377.

AUTHORS

S. J. Patil - Received the BE degree in Electronics from DKTE’s TEI, Ichalkaranji, affiliated to Shivaji University, Kolhapur, and an ME degree from the same University, currently working as an Assistant Professor in the Department of Electronics, DKTE’s TEI, Ichalkaranji, Shivaji University, Kolhapur. He has more than 12 years of teaching experience. He is a Ph.D. research scholar of VTU, RRC,Belgavi in the field of Wireless Networks.

Lalita S. Admuthe - (M’15) member of IEEE, Computer Society. The Author has received an M.E. and Ph.D. Degree in electronics engineering both from Shivaji University Kolhapur, India in 1994 and 2013 respectively. Author’s research interestincludes Neural Networks, Wireless Networks, Fuzzy Logic and Optimization Problems.

Since 2013 she has been a Professor in Electronics Engineering at DKTE’s Textile and Engineering Institute Ichalkaranji. Currently, she is working as Dy-Director and Head of Electronics Engineering Department in the same institute. Her teaching experience includes the topics of Artificial Neural Networks, Radom Signal Processing, Computer Architecture and,Parallel Processing.

Meenakshi R. Patil (M-07, SM-17) became member IEEE in 2007 and a senior member of IEEE in 2017. The Author is graduated in Electronics and Communication Engineering from PVPIT Budhagaon in 1994 and received post-graduate degree in Electronics Engineering from WCE Sangli in 2002. The Author has completed her Ph.D. degree from Shivaji University Kolhapur in 2011. Authors research interest includes digital watermarking, Digital Image processing, Communication and, network security.

From 1999 to 2007, she was the head of department BCE Shravanbelgola. Since 2011, she has been a Professor with the AGM Group of institutions Hubbali, Karanataka, India. She is currently working with JAGMIT Jamkhandi, Karnataka, India. Presently five research students are working on various fields in Signal processing and communication under her supervision.