An Improved Trust Depending Cluster Communication Using Multi Point Access Optimization Algorithm in MANET

D. Sampath Kumar and S. Veni
Dept. of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India.

Abstract
Mobile Ad Hoc Network (MANET) nodes are always unstable, hence it moves haphazardly in a network area. The nodes does not handle the time slot allocation concerns in communication period proficiently. The execution time nodes are dynamically different for its location and resource obtainability. If any of the nodes does not acquire the communication for that specific time, transmission gets unsuccessful. It cause more energy usage, and exploit end to end delay. Therefore, Improved Trust depending Cluster Communication (ITCC) technique is anticipated to accomplish the secured communication in clustering. Cluster head monitor the each cluster member activities, from original state to ultimate state. Those particulars are sustained on buffer of every cluster head node. To design multi point access optimization procedure is functional to mobile network, by means of that buffer data of cluster head to allocate multi point access, when one node miscarries to accomplish communication then allocate subsequent neighbour node as of multi point access for clustering nodes. It decreases energy usage and end to end delay. The recommended protocol exploits the Hybrid Cat Swarm Optimization (HCSO) technique for approximating the optimal path for all the neighbouring nodes from source node. If neighbouring node is a cluster node, the source node communicates with receiver node’s data packets over the selected neighbouring node. The performance contrast the anticipated ITCC protocol with the prevailing Trust-Based Task Assignment (TBTA) and Energy Efficiency Optimization (EEO) approaches show that the anticipated ITCC protocol offers optimal outcomes.

Key Words: MANET, trust evaluation, improved trust depending cluster communication, hybrid cat Swarm Optimization.
1. Introduction

With the increase of wireless technology, an infrastructure less network termed MANET deals an outstanding solution about the services that necessitates dynamic topological modifications, mobile conferences, rescue operations, etc. The MANET is an assortment of mobile and wireless machine nodes. This MANET is formed deprived of centralized control and fixed infrastructure. Normally, the MANETs are formed by wireless links, and are built at any place and time. The important process of this scheme relies on nodes assistance within the system. Nevertheless, distributed cooperation depends on the trust node in the network. Owing to the node behavior, the trust level is resolute to permit appropriate communication amongst the nodes in MANET as the trust less node has less total of energy for transmission or else the source node does not deliberate any of the physical activities of the neighbour node. Consequently, the trust replica is indispensable in MANET to improve the network efficacy. It guarantees that the appropriate and consistent operation of MANET can be proficient merely in the form of trust management structure amongst the communicating nodes in the network. Hereafter, it is important to extent the nodes trust value in accordance to approximately definite metrics.

Trust computation in MANET is a stimulating task owing to the unpredictable alteration in network composition, active nature of MANETs, and an un-derived previous trust relationship amongst the nodes. This calculation is merely resolute to choice the finest routing path for packet transmission deprived of changing the operation of the MANET. The bandwidth and the battery power are the significant limitations of the mobile nodes. These restraints mean that nodes must have trust in their neighbours for association and collaboration as the actions of the node changes over time. In MANET, trust scheming on a particular node by any other node experiences a cost on resources. Observing the node behaviour is very tough on the decentralized communication scheme. Myriad researches progress approximately trust management structure to elucidate the trouble in trust calculation of MANET but the execution of this structure suits the pertinent characteristics of MANET. It is still an open research question, which requirements further discussion and examination. In definite cases, the network topology of MANET are sustained stable, however in other cases, the topology of the network alterations offers alteration in the nodes mobility and frequent link failure. The channel quality of the wireless channels are affected owing to numerous factors like fading, multipath, dynamic change in topology, and problems. Therefore, the creation and maintenance of the MANET is not an easy task [1].

To address the trust disputes and to offer an obstacle free communication amongst the nodes, a trust based cluster multipath optimum routing protocol is suggested. The trust management structure of the anticipated ITCC calculated the maximum trust value for every communicating node in MANET. The foremost objective of clustering in mobile ad-hoc network surroundings how an
optimal cluster head be chosen and how can the optimal amount of clusters be realized through division deprived of degrading the complete network’s recital. The recommended framework considers the trust value of every neighbour node of the source node somewhat than considering trust value of each single source node. Furthermore, the aggregate equation is exploited to obtain the best routing by considering the trust value of multipath. To evaluate the optimal routing path, the trust value for all the neighbouring nodes during packet transmission is predictable. Lastly, the trusted nodes are recognized to decrease the traffic. After the organization of nodes into trusted and non-trusted nodes, the HCSO inspired routing protocol is utilized for approximating the optimal path for file transmission. Primarily, the location of the cats are prepared into a haphazard location, then the location of the cat is reorganized to a novel location. The cat behaviour has two kinds like tracing and seeking modes. Based on the velocity and location data of the cat, the fitness function is projected. From the fitness values of all the cats, the optimal fitness value is selected.

The comparison is made amongst the anticipated ITCC scheme and the prevailing Trust based Bat-Inspired Routing (TBIR) protocol, Lightweight and Dependable Trust System (LDTS), and Trust Derivation Dilemma Game (TDDG) methods. The prevailing method lacks with respect to packet delivery ratio, loss rate, throughput, and the trust value. This method displays inefficiency in treating the attacks from malicious nodes internally, that leads to the severe effect on privacy and security of the complete system. This scheme computes the nodes trust value in view of the single source node, which outcomes in the collection of poor routing path. In the anticipated technique, the trust is considered by the neighbour nodes, which leads to the assortment of the finest routing path.

- The foremost contributions of the anticipated ITCC protocol are as trails,
- To check the root node is trusted or non-trusted node.
- Cluster formation between trusted nodes and selected the cluster head.
- To scheme a cat-inspired routing protocol for providing an obstacle free communication path amongst the sender and the receiver.

The remainder of the work is provided as trails: Section 2 analyses the prevailing trust based routing protocols and bio-inspired protocols for MANET. Section 3 describes the trust management framework and packet transmission based on hybrid cat-inspired procedure. The simulation outcomes of our projected trust management model in contrast with the prevailing system are simulated and revealed in section 4. Section 5 gives the paper with some desired solutions.

2. Related Works

This segment designates the numerous prevailing trust based routing protocols and bio-inspired protocols for MANET. Sridhar et al., 2017 [2] projected protocol (TES-AODV) integrates energy, security management, trust, and nodes.
designated for routing, with its energy and truth values. Threshold value is definite and nodes are ideal for routing, when the energy levels and trust values are higher than the threshold value. The transmissions are protected by using message digest algorithm, termed MD5 which produces specific signatures for each node that participates in routing, by providing routing consistency. The simulation outcomes have exposed improved development over quality of service metrics like Delay, PDR, Jitter, Throughput, and residual energy. Therefore TES-AODV provides consistent, more reliable, and secured data transfer associated with common DSR and AODV protocols.

Airehrour, et al. 2015 [3] suggested a secure trust-based routing protocol named Grade Trust for detecting the black hole attacks. When compared to the traditional routing protocols like Fisheye State Routing (FSR), and Ad hoc On-demand Distance Vector (AODV) the proposed Grade Trust increased the packet delivery ratio.

Tan, et al. 2015 [4] projected a trust based routing method for approximating the trust value of mobile nodes. By estimating the path with utmost path trust, malicious nodes were prohibited. For founding a secure route, the anticipated trust method was integrated with the traditional optimized Link State Routing Protocol (OLSR). Iterated outcomes demonstrated that the anticipated FPNT-OLSR produced optimal average latency, overhead values, packet delivery ratio, than the traditional OLSR.

Anwar and Huifang 2015 [5] recommended a particle swarm optimization based energy-aware multicast routing for MANET. When associated to the genetic algorithm based multicast routing, the PSO based routing provided high speed, recital and efficacy.

Wang, et al. 2014 [6] recommended a trust-based QoS replica for approximating the trust degree amongst nodes. The proposed trust-based QoS routing procedure developed trade-off amongst link delay and trust degree. When associated to the traditional watchdog-Dynamic Source Routing (DSR) and QAODV, the anticipated routing algorithm formed average end-to-end delay, routing packet overhead, and detection ratio of malicious nodes optimal packet delivery ratio.

Gera, et al. 2014 [7] anticipated a trust-based multipath routing system for discovering numerous paths amongst the source, and the destination. The secure path was utilized for transmitting the self-encrypted parts of the message. When associated to the trust based multipath routing protocols, the anticipated routing system was secure.

Kiran 2014 [8] recommended a new hybrid bio-inspired routing protocol termed bat-termite for MANET. The recommended protocol combined the characteristics of social insect termite, and mammal bats. The bat-termite procedure calculated an adaptive routing protocol grounded on building termites
nature. Further, the backup route preservation was improved by means of echo-location feature of the bats. When associated with D-termite, prevailing termite, AOMDV and AODV routing protocols, the anticipated bat-termite algorithm had the subsequent benefits: faster route discovery process, enlarged robustness, and quick route repair.

Manickavelu and Vaidyanathan 2014 [9] recommended a PSO-based prediction algorithm for approximating an optimal route and lifetime. The factors similar to nodes of relative mobility and energy drain rate were utilized for calculating the node’s lifetime. The position of each node was validated before data transmission.

Xia, et al. 2013 [10] anticipated a dynamic trust prediction replica for estimating the reliability of the nodes in MANET. The anticipated model was based on the historical behaviours. By ill-using the Trust-based Source Routing (TSR) protocol, the unswerving path was designated for data packet transmission. Experimental examination exhibited that the anticipated prediction model enlarged the average end-end delay and packet delivery ratio.

Bar, et al. 2013[11] calculated the trust value of node in a network based on the packet forwarding capability. By abusing the trust value, the nodes were ranked. The path with numerous amount of trusted nodes was designated by means of the AODV protocol. In preference to selecting the shortest path, the anticipated protocol took the trusted path for transporting the packets. Experimental examination demonstrated that the anticipated protocol fashioned minimal packet drop.

Karia and Godbole 2013 [12] projected an enhanced ant net global positioning scheme for routing in MANET. The anticipated scheme was based on the ant routing protocol of biology-inspired, and ant colony optimization. When associated to the Adhoc On-Demand Multipath Distance Vector (AOMDV) protocols and traditional DSR, the anticipated biology-inspired ant routing protocol fashioned average throughput, optimal end-to-end delay, route cost and packet delivery ratio.

Hoolimath, et al. 2012 [13] anticipated Optimized Termite (Opt-Termite) algorithm for MANET. The self-organization of the nodes was achieved by means of stigmergy idea. By balancing the load between the nodes, the optimization procedure was achieved. When associated to the outdated AODV protocol, the recommended Opt-Termite algorithm accomplished optimal recital.

Krishna, et al. 2012 [14] recommends QoS facilitated Ant colony-based Multipath Routing (QAMR) algorithm for sensing the optimal path and communicating the data. The recommended algorithm subjugated the foraging performance of ant for choosing the optimal way based on node stability and path preference possibility. The anticipated algorithm measured the QoS factors
like node stability, numeral of hops and path preference probability. Simulation outcomes shown that the projected procedure was scalable and proficient of creating higher load traffic. Sharvani G S 2012 [15] anticipated an ant’s food foraging behaviour grounded Modified Termite Algorithm (MTA) for an actual load balancing. The node stability factor was utilized for approximating the link stability.

3. Proposed Methodology

This segment offers a thorough description about the anticipated ITCC based protocol. The projected ITCC protocol delivers two main contributions like,

- Improved Trust Management Framework depending on cluster communication
- Packet routing based on hybrid cat-inspired algorithm

ITCC Framework

The most important concern in the wired/wireless network is the security, which practises the source for secure packet transmission. Henceforth, it is crucial to implement trust management in these types of networks to guarantee secure communication. In the prevailing methods, the MANET environment with security is delivered by key exchange method, which is a tedious procedure [16]. Our anticipated system trails a peer-peer communication and contents the predefined circumstance to launch a secure MANET environment. The complete stages complicated in the trust management structure is described in Fig.1.

3.1. Network Formation

The anticipated approach deliberates the MANET environment, which is organized with no centralized authority. The nodes situated on the network can connect over numerous indirect hops. The anticipated system engaged in MANETs routing protocols to carry out execution among counter and with non-cooperative nodes in MANET environment. A node that produces false routing messages, replay packets or incorrectly forwarding packet, which is measured as a malicious node. This system necessitates the subsequent features to achieve its function appropriately:

- For monitoring the neighbors, nodes should be operated in an promiscuous manner.
- The node’s transmission ranges are equal, in which all the links are bidirectional.
- Selfish nodes are provided based on misbehaving nodes and are not malicious.

The network operates in a multi-hop networking manner in which the data packets swaps among themselves and forwarded to adjacent nodes.
System Overview

This investigation presents a novel framework based on trust equation to depict the trust level of a piece node in MANET. The obtainable model is extensible and more appropriate for the MANET applications with changing security necessities and background set up. Trust is demonstrated as the forecast of doing specific node behaviour under definite environmental circumstance. Usually, trust models give a solution to the liabilities of the MANET. In trust model, each
and every node amongst the network methods the node cooperation so as to compute the neighbours trust level. The calculated trust value supports secure routing over the network and resolves numerous network glitches with better decision-making criteria by means of the trust values. As revealed in Figure 1, the nodes are prearranged, and the maximum trust value of nodes is predictable by forming appropriate infrastructure. According to our anticipated model, each and every node includes the trust values that give perspective of the nodal activities history of their individual neighbour in MANET. The trust equation cast-off in trust model deliberates the trust value of each and every neighbour node of the source node. The finest routing path is acquired in view of the node’s trust value in the network. To decrease network energy and to progress the scalability, the cluster based communication has been offered in this scheme. Lastly, the optimal multi-path are carefully chosen by means of HCSO algorithm grounded on trust values of each node.

3.2. Trust Value Calculation

In our anticipated method, the trust value is computed for the nodes available in network. The trust value of each path node is chosen for the communication. During the path selection, the secured communication is achieved in MANET. The trust value for every node is calculated by means of the subsequent equation

\[ T_e(r) = (1 - \alpha)t_s(r) + \alpha A_s(r) \]  \hspace{1cm} (1)

From equation 1, it is clear that ranges from 0 to 1. The factors \( t_s(r) \) and \( A_s(r) \) in this framework permits the node to obtain the most pertinent factor. \( t_s(r) \) signifies the trusted node and the value range from 0 to 1, where \( A_s(r) \) specifies the aggregate trust value of every neighbors and the value ranges from 0 to 1.

\[ t_s(r) = \beta C_s(r) + (1 - \beta)T_s(r) \] \hspace{1cm} (2)

Equation 1 and 2 are utilized for trust computation while \( \alpha \) and \( \beta \) in both equations specifies the weighted factor of trust level of source and destination. The term \( C_s \) specifies the present trust value while last trust level is specified by the term \( T_s \). Owing to the above trust assessment, root nodes are specified as trusted or non-trusted nodes. The trust estimation is calculated in specified algorithm 1.

**Algorithm 1: trust node evaluation**

D-routing detail

Pack-packet

Ts-Time slot

Step 1: Source -> (Pack, Ts, D)

Step 2: for each source find routing nodes

Step 3: if (Rn == Trust)

Step 4: time slot matched.
Step 5: Source select that routing node.
Step 6: routing node perform communication
Step 7: \( \text{else if } (Rn! = Trust) \)
Step 8: Time slot mismatched
Step 9: source node reject that routing node
Step 10: not broadcast packets
Step 11: End if.
Step 12: \( \text{node} < - \text{accept } (Pack, Ts, D) \)
Step 13: \( \text{Buffer}(Pack, Ts, D) \)
Step 14: end for

### 3.3. Cluster Communication

Grouping sensor nodes into clusters has been extensively accepted by the research community to convince the scalability goal and usually accomplish greater energy efficiency and extend network life span in MANET surroundings. In this cluster communication, all confidential nodes are produced as clusters. In this cluster nodes, the uppermost energy and mobility of nodes are chosen as Cluster Head (CH). The CH observes all cluster member nodes and their characteristics. The cluster nodes data’s are stored in membrane table. If the node is cluster member, then it’s chosen as routing node to transmit data packets. To examine malicious node and to decrease transmitting time, the optimal path has been chosen based on HCSO. Cluster configuration and routing node assortment is specified in algorithm 2.

**Algorithm 2: cluster formation and route node selection**

Step 1: for each cluster head monitor its cluster member node
Step 2: if (cluster member node=failed)
Step 3: search another node
Step 4: transmit data packets
Step 5: else
Step 6: if (cluster member node=success)
Step 7: select that node to transmit data packets
Step 8: end if
Step 9: Reduce energy usage, end to end delay
Step 10: End for

### 3.4. Optimal Path Selection Using Hybrid CSO

To recognize the malicious node and decrease the packet transmitting time, the optimal path has been chosen by HCSO based on nodes less energy and high
trust value. In CSO, natural cat’s activities has been determined. The cats are have two actions like seeking and tracing. In this HCSO, the cats are measured as routing nodes.

**Conventional Process of CSO**

Cat Movement = Tracing Mode + Seeking Mode

While realizing, CSO is used to resolve optimization crisis. The preliminary phase is to demonstrate the cats or amount of individuals to be utilize. The cat population has certain attributes:

- Location made of ‘X’ dimensions;
- Velocities based on dimension of each location;
- A fitness value of the cat relates with the fitness function;
- Finally, to set a flag to assign the cats’ tracing mode and seeking mode.

The CSO procedure provides the best solution in every cycle and when the termination is encountered, the best solution is obtained based on the finest location of cats in the population.

CSO has two sub-modes: tracing mode and seeking mode. The combination ratio is provided by the combination of tracing mode with the seeking mode. To guarantee the position of cats by determining the resting time and viewing the environment, initially the MR value is set with a lesser value. The CSO algorithm is demonstrated in 6 steps as provided in [17]:

**Step 1:** Place ‘N’ cats as in the algorithm

**Step 2:** Sprinkle cats randomly in M-dimensional space solution and give the values randomly, with the maximum velocity range to the each cat’s velocity. Then pick the cats randomly and place them in tracing mode based on MR, and others set of cats in seeking mode.

**Step 3:** Compute fitness value of randomly placed cat by pertaining the cats location with the fitness function, which signifies the goal, and sustain the finest cat in memory. The location of best cat (xbest) will be considered as it signifies the finest solution.

**Step 4:** The cats position is changed based on their flags, if catk is in seeking mode, the seeking mode procedure is maintained, or else the tracing mode procedure is pertained.

**Step 5:** Re-pick cats and set them in tracing mode based MR, then place the remaining cats in seeking mode.

**Step 6:** Ensure the termination, when the condition is fulfilled, and otherwise replicate Step 3 to Step 5.

**Hybrid CSO**

This examination, anticipates a novel algorithm (HCSO) to progress the recital and accomplish improved convergence in lesser iteration. By totalling a novel
factor, with the location equation the inertia weight will be randomly selected, by making the velocity equation in a new method to search the capability of the finest cats vicinity. With these factors, global and local search capability can be made balanced. The inertia weight helps in global search, as small inertia weight leads to easier local search. Huge value will be utilized initially and summarized slowly to least value. So, the maximum inertia weight is obtained in the initial dimension of every iteration and it will be reduced considerably in every dimension. The velocity updating equation for all cat to form a novel alteration. The anticipated fitness computation, from optimization viewpoint, favours exploration and exploitation in search procedure.

For examining, the fitness function is calculated for a novel locations which is positioned far away from previously computed locations. In addition, approximation is done based on the closer values. The anticipated technique computes actual fitness function of the individuals which are located closer to the location that holds minimum fitness value, that targets to progress minimum. After numerous iterations, the finest balance has been revealed i.e., \( d = 3 \) among the exploitation and examination within the search space (the context of BM application); therefore it has been cashed out in this paper.

The improved HCSO optimization technique, the fitness value based on the less energy and great mobility of nodes. The aim of this function is, to choose the high trusted and reduced energy based node selection for efficient routing procedure. The step by step procedure of HCSO is specified below

Step 1: Population of ‘N’ cats (i.e. root nodes) is produced with random locations within the searching network region, which is typically an area centered on the block position; and each cat is allotted with random velocities (i.e. node), the individuals database array is initialized as \( T \) in an empty array.

Step 2: Select the available cats (i.e. nodes) and place them tracing mode based on Maximum Ratio (MR), and place the remaining cats in seeking mode.

Step 3: The fitness value of cats’ are calculated based on their functionality. With reference to optimal path selection, the maximum trust value and will be selected based on less energy of the (matching criterion). In HCSO algorithm, to perform optimal routing, calculate the fitness value of all cat (i.e. node) based on maximum trust value.

Step 4: The fitness value will be estimated based on the cats locations (i.e. node) with the fitness function, and maintain the finest cat into \( T \) to satisfy the goal.

Step 5: All individuals of initial population must satisfy Exploration rule condition: If an individual \( P \) is positioned away from distance \( d \) that is related to the nearest individual \( Lq \), and the fitness value is computed based on actual fitness function. Calculation in the actual fitness function corresponds to the definite trust values.

Step 6: A group of cats are arranged (i.e. nodes) serially in this cluster in accordance to the fitness values.
Step 7: Update the evaluation based on the specific database array T.

Step 8: Relocate the cats (i.e. nodes) based on their flags, if cat\(_k\) is in seeking mode, the cat is associated with seeking mode, otherwise it is in tracing mode.

Step 9: Fitness values are calculated for every cat in seeking mode by the fitness computation scheme existing in [18].

Step 10: Based on the selected inertia weight (w) in a random manner the ranges of [0.4, 0.9] controls roaming cats (i.e. nodes) outside the network region.

Step 11: Pick the finest solution from the neighbor and substitute virtual cat (i.e. node), which has worst fitness value among the cluster that is available in an array T. The finest solution and the virtual cat should not originate from the similar group.

Step 12: Repeat step 9 with respect to each group.

Step 13: During the time of parallel tracing mode, the velocity is stated as in the specified equation:

\[
V_{k,d}(t) = V_{k,d}(t - 1) + r_1C_1(X_{\text{best},d}(t - 1) - X_{k,d}(t - 1)), \quad d = 1, 2, \ldots, M
\]

Where \(X_{\text{best},d} \rightarrow \) coordinates the finest solution of nearest one cluster.

Step 14: A novel form is utilized to update the location equation in which it is arranged in two terms. Initially, the average information of prevailing and present location and the average of prevailing and present information of velocity will be utilized. As a consequence novel position equation is illustrated below:

\[
X_{t} = \frac{X_{t} + X_{t-1}}{2} + \frac{V_{t} + V_{t-1}}{2}
\]

Step 15: Criterion for termination. In case of the equivalent iteration with the maximum \(t_{\text{max}}\), or the block MSE less than the specified amount \(\varepsilon\), iteration ends up; or else go to step 3. Based on the above parameters, the optimal routing has been chosen and packets are transmitted from source node to target nodes.

**Packet Format**

The proposed scheme packet format has been showed in figure 2. It illustrates the packets taken by each filed. In first and second fields are source and destination IDs and it takes 4 bytes. Third field is Source node analyse routing path and it takes 3 bytes. Then, an improved trust depending cluster communication field and it takes 3 bytes for effectual multipoint access. Fifth field is Multi point access optimization algorithm and it takes 2 bytes for analysing the algorithm. Final filed is Minimized usage path is selected and it takes 2 bytes.
4. Results and Discussion

To choose the finest routing path, the trust estimation is a significant feature in MANET. The validation of the anticipated ITCC protocol is executed by accomplishing wide-ranging simulation estimation on the set of nodes by means of the NS-2 simulator. For that reason, we aim the network with an example of 50 nodes by means of network simulator. Now, AODV routing protocol is utilized. The packets are traversed owing to the trust computation. The trust values are calculated when the request is offered. The trust values are calculated for the nodes in the network and trust level for every node is measured. If a request is acquired from a specific node, then the trust level of the node is computed based on the permitted request. Throughput is preserved, and the graphs are utilized to compare the outcomes of anticipated trust evaluation and clustering Methodology, which obviously demonstrates the performance development of the anticipated ITCC protocol. The performance is examined based on the subsequent metrics: Packet Delivery Ratio, energy consumption, communication overhead, network lifetime, end-to-end delay and failure detection efficiency.

Table 1: Shows the Simulation Parameters and their Values

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Nodes</td>
<td>100</td>
</tr>
<tr>
<td>Size of area</td>
<td>1000 X 1000</td>
</tr>
<tr>
<td>Mac</td>
<td>802.11g</td>
</tr>
<tr>
<td>Range of Radio frequency</td>
<td>250m</td>
</tr>
<tr>
<td>Time for Simulation</td>
<td>20ms</td>
</tr>
<tr>
<td>Traffic Source</td>
<td>FTP</td>
</tr>
<tr>
<td>Size of Packet</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Way</td>
</tr>
<tr>
<td>Protocol</td>
<td>LEACH</td>
</tr>
</tbody>
</table>

Performance Metrics

This section demonstrates the recital examination of the anticipated ITDCC protocol with the prevailing systems like TBTA [19] and EEO [20]. The subsequent are the metrics utilized for the performance examination.
Figure 3 demonstrates the computed average trust value of the sensor nodes. At this point, the X-axis signifies the amount of nodes taken for the research, and Y-axis signifies the normalized trust value with respect to probability. Now, 15 nodes are taken into account. This trust value is measured by means of the equation (1). Owing to the computed trust value the nodes are allowed to contribute in routing. In general, it is accounted that better recital in MANET is proficient by guarantying high packet delivery ratio. As it signifies the consistency of packet transmission.

Figure 4 shows the NS-2 simulation of proposed Improved Trust depending Cluster Communication protocol among 100 nodes. It illustrates the trust among nodes with clustering.
Figure 5 shows the energy consumption among various protocols like proposed ITCC and existing TBTA and EEO protocols. It illustrates the proposed ITCC attained less energy compared than existing protocols due to the effectual clustering and optimal path selection. The percentage ratio of received packets over the sent packets shown in Figure 6 and is experimentally high in proposed ITCC method. But, the packet delivery ratio of the existing TBTA and EEO are relatively low due to the computational complexity. The proposed method enhances the efficiency of MANET through high packet delivery.

Figure 7 shows the communication overhead among various protocols like proposed ITCC and existing TBTA and EEO protocols. It illustrates the proposed ITCC attained less communication overhead compared than existing protocols due to the optimal path selection.
Figure 7: Communication Overhead Performance Comparison among Various Protocols

Figure 8 shows the network lifetime among various protocols like proposed ITCC and existing TBTA and EEO protocols. It illustrates the proposed ITCC attained high network lifetime compared than existing protocols due to the effectual clustering and optimal path selection.

Figure 8: Network Lifetime Performance Comparison among Various Protocols

The failure detection efficiency is merely approximated owing on the detection rate. The variation among the detection rate and the failure detection rate is that the false rate is approximated by separating the entire number of nodes in good behavior by the set of good nodes. This failure detection efficiency of the anticipated ITCC technique outperforms than the prevailing TBTA and EEO technique that is graphically illustrated in Figure 9.
In MANET, it is more significant to choose the trusted node as a subsequent packet carrier amongst all the nodes in the network to reduce the delay all through packet transmission. The time duration is known as end-to-end delay where the data packets generated by the nodes in the destination. The interruption of the anticipated ITCC is low when contrast to the prevailing TBTA and EEO method that is evidently demonstrated in Figure 10.

The iterated outcomes reveals that anticipated ITCC scheme is more proficient for trust management with respect to ensuring greater energy consumption, Packet Delivery Ratio, communication overhead, network lifetime, end-to-end delay and failure detection efficiency.

5. Conclusion

Trust is the mainly significant feature of achieving secure communication in MANET. Several trust management systems have been dedicated in the literature that is mostly determined on considering the trust value of single source node merely. In this paper, the superiority of security model grounded on ITDCC is anticipated that considers the trust value of each and every neighbor nodes of the source node. The clustering formation has been enhanced the scalability of the network and decrease the energy consumption. In addition, a
proficient non-obstacle communication among sender node and destination node is offered by means of HCSO-inspired routing protocol. The vital advantage of the anticipated system is to find the finest path not merely considering a single source node but also in view of the trust value of neighboring nodes of the source node. The HCSO has been accomplished high convergence of outcome. Simulation outcomes shows that the anticipated trust management framework is determined for guaranting high Packet Delivery Ratio, less energy consumption, less communication overhead, high network lifetime, high failure detection efficiency and low end-to-end delay. This research essentially aims at selecting the finest routing path for calculating the trust. As a potential enhancement, the parameters like invalid path selection, and content modification can be measured during packet transmission for offering a secure packet transmission.

References


[9] Manickavelu D., Vaidyanathan R.U., Particle swarm optimization (PSO)-based node and link lifetime prediction algorithm for route
recovery in MANET, EURASIP Journal on Wireless Communications and Networking (2014), 1-10.


