Trust Sensitive Dual Cluster Head Based Routing Scheme to Isolate Misbehaving Nodes in MANET

Aruna Subramanian[a], Subramani Appavupillai[b]

[a]Sona College of Technology, [b]M.V.Muthiah Government Arts College for Women

Abstract

Routing protocols function as the obligatory force in MANETs to transfer data outside the physical wireless ranges of the nodes. In hierarchical cluster based routing; cluster head nodes and gateway nodes alone participate in routing decisions. Those nodes may fail to cooperate during route discovery due to selfish or malicious grounds. Hence, imposing cooperation among nodes in MANET to employ a secure route becomes an extremely significant issue. Cryptographic mechanisms can be used, but it acquires a high computational cost and may not categorize the nodes with malicious intention. Therefore, we proposed a dual cluster head based trust aware mechanism as an alternative to cryptographic technique to protect forwarded packets from malicious nodes. Our proposed protocol TWCBRP classifies the network into one hop overlapping clusters with primary and secondary cluster heads, which are accountable for conducting all the routing activities. It constantly assurances the trustworthiness of cluster heads by replacing primary with secondary cluster head, as soon as the former becomes malicious. Cluster members send routing packets only through trusted cluster heads and gateway nodes thus guaranteeing a secure path. The performance of TWCBRP is evaluated with Network Simulator2 and illustrates better performance in terms of packet delivery ratio, throughput, delay, and control overhead when compared to a distributed weighted cluster based protocol (CBPMD).

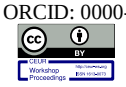
Keywords

MANET, malicious node, selfish node, trust, security.

1. INTRODUCTION

MANET is a self-configuring, decentralized type of unmanaged (ie., infrastructure less) wireless network with dynamic topology. It does not rely on fixed routers or access points as in the case of infrastructure wireless networks. Instead, each node performs as a host as well as a router and participates in routing process by forwarding data for other nodes. Nodes in MANET use flooding as the basic mechanism for forwarding data and control packets. So, the data is forwarded through intermediate nodes dynamically based on the network connectivity. There are number of characteristics in MANET such as mobility, dynamic topology, energy constrained operation, limited bandwidth, and security threats make it used in a number of applications for MANET. That is, they are appropriate for disaster situations like natural or human induced disasters, military battle-fields, and emergency medical situations, group communications, civil and business operations [21]. The nature of the mobile nodes in MANET brands them extremely susceptible to a variety of security threats because they usually own low computational resource as well as short radio transmission range due to the limited battery power they carry, and they might be moving constantly [1].

ISIC'21: International Semantic Intelligence Conference, February 25-27, 2021, Delhi, India
EMAIL: sarunasnivoss@gmail.com (A. 1);
subramani.appavu@gmail.com (A. 2)
ORCID: 0000-0001-7791-6955 (A. 1)



Therefore, there is an inducement for a node to misbehave in a malicious and selfish manner without cooperating with other nodes. The intention of malicious node is to attack and damage the network. Similarly, the intention of selfish node is to save its power, memory and CPU time [2]. A selfish node is not malicious and it does not intend to damage the network [3]. But, it normally restrains itself from other nodes which do not bring any benefit to the network. That is, they do not participate in routing process, intentionally delay RREQ, and drops data packets. Hence, imposing cooperation among nodes in MANET to employ a secure route becomes an extremely significant issue. Therefore, an unpredictable node can wreak substantial damage and undesirably affect the quality and reliability of data [4]. Cryptographic mechanisms can be applied in MANET routing schemes to secure data packets during the transmission of data packets in the network. But cryptographic techniques incur a high computational cost and cannot identify malicious nodes [5]. So, employing cryptographic techniques in MANET are quite impractical as MANETs have limited resource and vulnerable to several security attacks. Trust mechanism can be used as an alternative to cryptographic technique [5]. Trust mechanism computes trust value on nodes which helps to detect and isolate malicious and selfish nodes to provide secure data transmission.

2. PROBLEM IDENTIFICATION AND NETWORK MODEL

By electing single cluster head, it is very difficult to address the issue of cluster stability [6]. Furthermore, the elected cluster head may or may not cooperate during routing. Therefore, imposing cooperation among nodes in MANET becomes a significant issue in order to provide a secure route. Hence, we proposed a new trust aware weighted dual cluster head based routing protocol to provide a secure and stable route in MANET. dual cluster heads namely primary and secondary cluster heads are elected to sustain cluster stability. Hybrid trust mechanism is imposed on nodes in the clusters to detect and isolate malicious and selfish nodes and to provide a secure route. Supposedly, we can describe a MANET as an undirected graph $G= (V, E)$, where V represents a set of nodes v_i and E represents a set of links e_i. [7,8]. Therefore, building some sort of backbone structure for a network can enrich the performance of the whole network when the network becomes dense. The cluster structure is an efficient backbone infrastructure for MANETs [7, 21]. The network is partitioned into group of clusters. We define a cluster to be a subset of V and our proposed protocol elects two cluster heads namely primary and secondary cluster heads to maintain the stability of cluster structure. The nodes in a cluster are said to be geographically close to each other. The range of a cluster is measured by the number of hops from the cluster head to the extreme member node in its cluster. In our proposed work, we define the cluster radius to be 1 hop. That is, every cluster member node will be directly connected to its cluster head. Gateways are the non-cluster head nodes which lie on more than one cluster head's transmission range. Cluster heads and gateways form a backbone of the original network [8]. The cluster size is well-defined to be the number of nodes in the cluster, including cluster head and cluster members.

3. LITERATURE REVIEW

Broadcasting is a fundamental operation of MANET. This could be productive only if all nodes operate in a trustworthy manner. Therefore, establishing and quantifying behavior of nodes in the form of trust is essential for ensuring proper operation of MANET [4]. This is primarily important in case of tactical networks. Due to the dynamic nature of mobile nodes, trust computation of nodes in MANET becomes a relatively challenging task when compared to static networks. Also, the nodes in MANET are more vulnerable to attacks than nodes in wired network and thus performance degrades. So security is an important issue in MANET to provide secure communication between mobile nodes.

3.1 Definition of Trust and Motivation towards trust management

The concept of trust originally derived from social sciences field and is defined as the degree of subjective belief about the behaviors of a particular entity [9]. Trust has also received its attention in several literatures: psychology, sociology, economics, political science, anthropology and recently in wireless networks [7, 9, 22]. Blaze *et al*. [4] instigated the term" Trust Management" and acknowledged it as a separate component of security services in networks and clarified that" Trust management offers a unified approach for specifying and interpreting security policies, credentials, and relationships" [4]. It consists of three components: experience, recommendation and knowledge [4]. The 'experience' factor of trust for each node is directly measured by their immediate neighbors and kept updated at regular intervals in the trust table. The existing trust table is propagated to all other nodes as 'recommendation' part of the trust. At a regular interval, the previously evaluated trust is included in the current 'knowledge' factor of total trust. Now either these three factors individually or a combination of them can be used in computing the trust. Trust management in MANETs is preferred when participating nodes, without any earlier interactions, desire to establish a network with an acceptable level of trust relationships among themselves. Trust management has different applicability in many decision making situations including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes [10,20]. The term *trust management* is interchangeably used with the term *reputation management* [11]. However, there is a minor difference between trust and reputation. Trust is *active*, while reputation is *passive* [11].

3.2 Classifications of trust management schemes

The effort on trust computations can be largely classified into the following categories:

- Direct trust computation method – In this method, every node computes the trust value of its neighbors by itself.
- Indirect trust computation method- In this method, central agent manages (ie., helps) the node to compute the trust value of its neighbor nodes.

a) Distributed trust computation schemes

This can be further classified as: [24]

- Neighbor sensing based trust computation scheme (ie., Direct trust)
- Recommendations based trust computation scheme (ie., InDirect trust)

(i) ***Neighbor sensing method:*** Here, every single node observes its neighbors for their event reports and stores them up in their "knowledge" cache. A trustor node will compare its own observation report from the trustee node and also from other

neighbor nodes. Trust factor will be decided based on the amount of deviations between the observation reports [14].

(ii) ***Recommendation based scheme (ie., Indirect trust):***

Here, trust relationships on nodes are established based on recommendations alone [14].

(iii) ***Hybrid schemes:***

In hybrid schemes, the trust on a node is computed based on direct trust experience and recommendations from other nodes [14].

3.3 Related Works

In recent times, there has been considerable effort on various trust computing techniques with respect to MANET [11]. Buchegger et al [12] proposed CONFIDANT (ie., Cooperation of Node's Fairness In Dynamic Ad hoc NeTworks) protocol for detecting and isolating misbehavior nodes in MANET. In this method, confirmation from direct experiences and recommendations are collected. That is trust relationships and routing decisions are constructed on experienced, observed and forwarding behavior of other nodes. Dynamic Source Routing (DSR) is taken as a base routing protocol in this scheme.

M. Tamer Refaei et al [13] suggested a reputation - established mechanism as a means of building trust among nodes. Here a node autonomously evaluates its neighboring nodes based on completion of the requested services. The neighbors need not be monitored in promiscuous mode as in other reputation based methods. There is no need of replacing of reputation information among nodes, thus implicates less overhead. This scheme provides a distributed reputation evaluation methodology that is implemented autonomously at every node in an ad hoc network with the objective of identifying and isolating selfish neighbor nodes.

Haidar Safa et al [14] presented a cluster-based trust aware routing protocol (CBTRP) and it is a kind of reactive on-demand source routing protocol. To make sure safe routing path, the proposed CBTRP scheme first establishes the origin for a trusted environment by providing a trust based mechanism to differentiate trusted nodes from malicious ones. The trust value is computed based upon the information that one node can gather about the other nodes. Then, it organizes the network into one-hop disjoint clusters, whereby every node elects the most qualified and trustworthy node of its 1-hop neighbors to be its cluster-head. Cluster members in CBTRP forward packets only through the trusted cluster heads. Packets from malicious nodes are not processed and no packets will also be forwarded to them.

Paramasivam. B et al [15] proposed a secure as well as a fair cluster head selection protocol for improving security in MANETs. This model integrates security factors into the clustering approach for achieving attacker identification and classification. Byzantine agreement based cooperative technique is used for attacker identification and classification to make the network more attack resistant. The nodes that are totally surrounded by malicious neighbors fine-tune dynamically their belief and disbelief thresholds.

Venkanna.U et al [17] proposed a methodology to elect a accommodating node as the cluster head node by using key decision parameters such as trust value, remaining energy level, and time of availability values of nodes. Cluster stabilization is achieved by electing two cluster heads in which a secondary cluster head will take the role of the primary cluster head whenever the primary moves out of the cluster. The first step in this model is to structure the problem as a hierarchy for cluster formation. The second step is to calculate the relative local weights of key decision parameters namely TV, REL, and ToA towards the goal. The third step is to estimate relative local weight of each node in the cluster with respective to each decision factor. The fourth step is to determine the overall weight value of each node in the cluster.

Rahul. A et al [18] proposed a cluster based indirect trust mechanism to evaluate the trustworthiness of cluster heads. This model consists of three phases such as interaction phase, request phase and trust evaluation phase. In interaction phase, the member nodes will generate feedback values in the range from 1 to 10 depending on the number of successful interactions between the cluster members and cluster head. In request phase, if any node wants to access a secure connection with any of the service providers (CH), it requests the trust value of all its neighboring CHs. In trust evaluation phase, all the CHs will collect the recommendation values from its member nodes and aggregate the recommended values and issues the final trust value to the requesting node. The requesting node will establish its connection with the CH which has a highest final trust value.

4. PROPOSED APPROACH

4.1 Overview

Our proposed protocol, which is named "TWCBRP", is a trust aware dual cluster head based routing protocol to provide a secure and stable routing in MANET. Two cluster heads namely primary and secondary cluster heads are elected in order to maintain route stability. The primary objective is to isolate malicious and selfish nodes through trust computations of nodes for providing a secure routing.

a) Trust Computation of nodes in clusters

(i) Direct trust computation:

Each node computes the direct trust value by analyzing the behavior of its neighbor nodes. That is, the information on the subject of other nodes can be gathered by analyzing the forwarded, received and overheard packets. In TWCBRP, trust between two entities is represented by a 3-dimensional metric opinion [14] as follows:

$W_B^A = (b_B^A, d_B^A, u_B^A)$ …….. (1), such that $b_B^A + d_B^A + u_B^A = 1$

Where, W_B^A denotes node A's opinion about node B's trustworthiness, in which, b_B^A denotes the belief that A holds for B, d_b^a denotes the disbelief that A holds for B, and u_B^A denotes the uncertainty that A holds for B. In our proposed protocol, a node monitors other node's behavior using watch dog mechanism [19] to collect & record all positive (P) and negative (N) events about their trustworthiness. Therefore, the opinion metrics of W_B^A can be expressed as a function of P and N as follows:

$b_B^A = \frac{P}{P+N+2}$ ……(2) $d_B^A = \frac{N}{P+N+2}$ …….(3)

$u_B^A = \frac{2}{P+N+2}$ ……(4)

Where, each of the belief, disbelief and uncertainty values may range between 0 and 1 inclusively. The direct trust value of node B by node A is computed as follows:

$DTV_B^A = b_B^A$ ……(5)

Every time the number of positive or negative events changes, the corresponding opinion values will be recalculated using equations 2,3, and 4 respectively.

(ii) Indirect trust computation (ie., recommended trust)

The indirect trust value (ie., recommended trust value) of node B by all its one-hop neighbors is computed as follows:

$IDTV_B^A = \sum_{i=1}^{N} \frac{DTVi_B^{Ai}}{N}$ ……(6), where, N is the number of one-hop neighbor nodes of B, $IDTV_B^A$ is the recommended trust value on B by all its one hop neighbors 'A_i' based on their belief factors.

(iii) Final trust computation

The FTV of a node be governed by both the direct trust value and the indirect trust value. The α part of DTV and ß part of IDTV are used to calculate the FTV of a node B. It is computed as,

$FTV_B^A = \alpha * DTV_B^A + ß * IDTV_B^A$ such that α+ß = 1 …… (7),

where

- Case-1: when, $DTV_B^A < 0.5$, α = 0.5 and ß =0.5.
- Case-2: when, $DTV_B^A >= 0.5$, α =1 and ß =0.

b) Selection of primary and secondary cluster heads

Periodically, each mobile node broadcasts a HELLO packet to other nodes that lies within its transmission range to notify its presence and to discover its neighbors. Initially, before cluster formation, all the nodes may be in *un_decided* state. During cluster formation, when all nodes have discovered its neighbors, they exchange their weight values through HELLO packet. Therefore, the state of the node changes either as *cluster_head* or as *cluster_member*. A member node which lies within the transmission range of more than one cluster heads becomes a *gateway* node. The HELLO packet format is given in table-1.

Table-1
Hello packet format

Status of the node (0-undecided state/1-cluster head/ 2-cluster member)
Node ID
Weight value
Cluster Head's Neighbor Table
Cluster Head's Cluster Adjacency Table

In our proposed TWCBRP protocol, primary and secondary cluster heads are elected by computing the weight values of the nodes. Each node computes its own weight using the following weighting function which is based on [WCA], [SWDCBRP]:

$W_t(V) = (W1*LQ + W2*RS + W3*BW + W4*MV)$ …… (8),

where, *LQ* is the link quality, *RS* is the residual energy, *BW* is the available bandwidth and *MV* is the mobility of the mobile node. A node with highest weight among the other nodes in its transmission range is elected as a primary CH. Similarly; a node having a second highest weight is elected as a secondary CH. The following *ICF algorithm* is used for cluster formation in the network.

Algorithm-1: Initial Cluster Formation (ICF) algorithm

```
/*At system initiation, let us assume that, each node A in MANET holds undecided state and opinion values as,
b_B^A=0; d_B^A = 0; u_B^A=1; DTV_B^A=0; IDTV_B^A= 0;
Each node A maintains the weights of its one-hop neighbors and assume node A is invoking the algorithm*/
Input: Set of nodes in MANET
Output: Set of clusters
ICF( )
Begin
Do {
  Find a node B with highest weight in its CH set (ie., say B[i] where i=1 to N)
  If (B==A)
  {
       if (PCH does not exist in the cluster) {
            Node A elects itself as PCH;   }
         elseif (SCH does not exist in the cluster) {
           Node A elects itself as SCH;     }
  }
```

```
  elseif ( ($u_B^A$ >0.5) or ($b_B^A$ >=0.5) or ($b_B^A == d_B^A$) ) //A checks the opinion value of B {
      if (( B is a cluster member or undecided) && (PCH does not exist in this cluster)){
        B changes its status to PCH and accepts A as its member }
    elseif ( (B is a cluster member or undecided) && (SCH does not exist in this cluster) ) {
        B changes its status to SCH; A becomes member of this cluster; }
    elseif (B is a PCH of this cluster) {
        A sends induced Join_Cluster message to B;
       B sends an Accept_Join message to A; A becomes a member of this cluster; } }
 elseif ($d_B^A$ >=0.5)  {
  Remove B from CH set and continue the loop. }
} while ((PCH Not Exists) or (SCH Not Exists));
End;
```

The *initial cluster formation (ICF)* algorithm is described as follows. Each node computes its own weight value using eqn-8 and broadcasts to its 1-hop neighbors through hello packet. Similarly each node receives the weights of its one-hop neighbors and inserts them in its neighbor table and forms a CH set. If a node A, has no interactions with its neighbor nodes B, initially its belief (b_B^A), disbelief(d_B^A) and undecided opinion values (u_B^A) would be computed as 0, 0, 1 respectively using the eqns-2, 3, and 4. Each node A then finds a node B with highest weight in its CH set and checks its opinion values of it. If its u_B^A > threshold or its b_B^A ≥ threshold or its belief value (b_B^A) == disbelief value (d_B^A), then node B will either become primary CH or secondary CH based on the need. If its (d_B^A) ≥ threshold, then node B will be removed from A's CH set. The following table-2 describes the format of one-hop neighbor table (1NT):

Table-2
one-hop neighbor table

Node ID	Node Status	Cluster ID (CID)	Direct Trust value (DTV)	InDirect Trust Value (IDTV)	Final Trust Value (FTV)	Entry update time (in sec)

Each entry in one-hop neighbor table contains information about a 1-hop neighbor and also used to record the opinion about each 1-hop neighboring node. This table is used for cluster formation and route discovery. The following table-3 describes the format of two-hop neighbor table (2NT):

Table-3
Two-hop neighbor table

Node ID	Node Status	Next Hop Node	Entry update time (in sec)

By examining the *HELLO* packets received from its neighbors, a node gathers information about its 2-hop neighbors (ie., 2-cluster away nodes) and stores them in this table. This table is used during route discovery and data forwarding. The following table-4 describes the format of cluster adjacency table (CAT):

Table-4
Cluster Adjacency Table

Cluster ID (CID)	Gateway ID (GID)	Entry update time (in sec)

CAT table is used to keep information about its adjacent clusters. That is, a node records the ID of each of its adjacent CHs and the corresponding gateway node to reach it. This table is used during route discovery and data forwarding.

4.2 Cluster maintenance phase

Since, our MANET is vulnerable to attacks, the elected primary CH and secondary CH would become malicious or selfish and affect the network connectivity. In our TWCBRP protocol, at system initiation, cluster formation is done through *Initial Cluster Formation (ICF)* algorithm with two trust aware cluster heads namely primary and secondary cluster heads. The secondary cluster head after being elected keeps itself in promiscuous mode and overhear the transactions of PCH node. If forwarding ratio of PCH becomes lesser than dropping ratio, SCH triggers PCH node with a *LIFE_DOWN* message, to carry out the pending transactions of PCH by invoking *CH_Change* algorithm. Similarly, if forwarding ratio of SCH becomes lesser than dropping ratio, it sends a LIFE_DOWN message to all its one-hop neighbors and invokes the *CH_Change* algorithm to elect a new SCH node. The significance of *CH_Change* algorithm is that, it involves only the set of nodes that are within the cluster for local cluster heads updating and does not involve the entire nodes in the network for re-election process. Therefore, it minimizes updating overhead during topological change. The *CH_Change* algorithm is given below:

Algorithm-2: Cluster Head (CH) change algorithm

```
// Let us consider Node A as SCH and Node B as PCH
// Let us assume Node A is invoking the algorithm
Input: SCH node
Output: Change of cluster head
CH_Change ( )
Begin
//F-Forwarding ratio and D-Dropping ratio
If (node weight value of B < Th) or (F(B) < D(B)) then
//here Node B is PCH
{
  SCH sends a LIFE_DOWN message to PCH to relinquish the role of PCH and to process its
  pending transactions and invokes Elect ( ) function to elect a new SCH;
  PCH joins the cluster as a cluster member;
} else
    If (node weight value of A < Th) or (F(A) < D(A)) then
//here Node A is SCH
```

```
   {
     SCH sends a LIFE_DOWN message to all its member
nodes and invokes Elect ( ) function;
   }  }
End;
function Elect ( ) {
 Do    //here Node B is cluster members
 {
    Find a node B with highest weight in its neighbor
table (ie., say B[i] where i=1 to N)
    If ((node B is a cluster member or undecided) &&
(FTV_B^A>=0.5))  {
        Node B changes its status to SCH and sends a
HELLO message to its one-hop
        neighbors;   }
    elseif (FTV_B^A <0.5)  {
      Remove B from CH set and continue the loop.  }
  } while (SCH Not Exists);
}
```

a) Route discovery

Route discovery is a mechanism whereby a source node S wishing to send a packet to destination node D, it is done through intermediate nodes. Route discovery in TWCBRP is done through flooding RREQ packets only with cluster heads and gateway nodes. However, in order to isolate malicious nodes from participating in the network, their 1-hop neighbors will ignore all packets received from them, and will attempt to find a route that does not include intermediary misbehaving nodes. For that, each node will keep itself in promiscuous mode to record the transaction of its next hop node [18]. For every successful and unsuccessful transaction, it updates its direct trust value and final trust value respectively. Intra-cluster routing takes place when source node S and destination node D are located within the same cluster. This can be identified by PCH's 1-hop neighbor table. Inter-cluster routing takes place when the source node S and the destination node D are not located in the same cluster. Therefore, primary CH needs to involve gateway node for data and control packet transmission. A gateway node is a node that lies within the transmission range of both the clusters, and would become members of both clusters. Therefore, a powerful node should be appointed as a gateway node for maintaining network connectivity. In our proposed TWCBRP protocol, among the nodes that lies in the common region of more than one clusters, a node with highest weight and highest trust value (FTV) is elected as a gateway node in order to improve network connectivity. The elected gateway node will act as a "trust guarantor" for the cluster heads that lies within its transmission range.

b) Data forwarding mechanism in TWCBRP protocol

When source node S attempts to send a data packet to the destination node D, it first checks its 1-hop neighbor table (NT). If D is found, it sends the data packet directly. Otherwise, S checks its 2-hop neighbor table (NT). If D is found in its 2-hop neighbor table and can be reached through more than one-hop neighbors, it chooses the one with the most recent *EntryUpdateTime* as the intermediate node [18]. If D is not found in its 1-hop and 2-hop NTs, it checks its route cache (RC). Route cache is the storage space in each mobile node for storing recently discovered routes. If a route to D is made available in its route cache, S simply uses the route to send the data packet to destination D. Otherwise; it floods a route request (RREQ) packet to its neighbor nodes. An intermediate node (IM) after receiving the RREQ will decide how to process it based on its cluster status and the information available in the RREQ packet header. It is expressed as follows:

1. If IM is a cluster member or with undecided status, it simply drops the RREQ packet.
2. If IM is a cluster gateway (CGW), it checks whether it is listed as an entry in RREQ packet header. If no, it simply drops the packet. If yes, it unicasts the RREQ to the corresponding neighboring CH as recorded in RREQ.
3. If IM is a CH, it appends its CID in the *traversed cluster address list* and increases the NUM2 counter by 1. If D is found to be a 2-hop neighbor, IM unicasts the RREQ to D based on its 2-hop neighbor table.
4. Otherwise, for each neighboring cluster which is not listed in neighboring CH list, IM records the CID of neighboring CH and the corresponding gateway address to reach that cluster in RREQ, increment NUM1 counter by 1, and broadcasts to them.
5. If no such neighboring cluster is found, it drops RREQ.
6. Before recording any node's ID in RREQ packet, each node checks that the recorded entry does not have FTV_B^A <0.5.

The following table-5 shows the format of RREQ packet.

Table 5
Route Request (RREQ) packet

Packet Type	Num1	Num2	Identification Number
Destination address			
Gateway node address [1]			
Neighboring cluster head address [1]			
…….			
Gateway node address [Num1]			
Neighboring cluster head address [Num1]			
List of traversed cluster addresses [Num2]			

Here, in the above table, PT indicates whether the packet type is RREQ or RREP packet. List of gateway nodes are used by CHs to forward RREQ packets to its one-hop away CHs. List of neighboring CHs are used by gateway nodes to

forward the RREQ, and each CH appends its addresses in the traversed cluster address list field in the RREQ packet during route request propagation. The identification field is used to match the route request packet with the correspondent route reply packet. Num1 and Num2 indicates hop counts for neighbor cluster head and gateway pairs and targeted cluster address list respectively. The following table-6 shows the format of RREP packet.

Table 6
Route Reply (RREP) packet

Packet Type	Num1	Num2	Identification Number
List of traversed cluster addresses [Num1]			
List of CH addresses in calculated route [Num2]			

In the above table, PT indicates whether the packet type is RREQ or RREP. List of addresses in calculated route is used to reach the RREQ of source node. The identification number is copied from the RREQ packet in order to match with it.

The actual routing is done like the way that the traditional on-demand source routing protocol such as AODV does. That is, each intermediate node in the underlined data packet forwards it to the next specified address until the destination node is reached. However, the significance of TWCBRP protocol is that it does not allows malicious and selfish nodes (FTV_B^A <0.5) to forward neither RREQ nor RREP packets.

c) Node movement

Node movement in XYZ protocol is shown with the following algorithm.

Input: Node A in mobility
Output: Node A joins/leaves the cluster
Begin
If(node A is a leaving node from cluster) {
Find the status of Node A;
If (moving node A is a PCH or SCH) {
Invoke *CH_Change* algorithm; }
Else if (moving node A is a cluster member) {
No change takes place in the cluster structure; and no need of re-election. }
}
Else if (Node A is a joining node into the cluster) {
Node A sends a JOIN_REQUEST message to PCH node;
Upon the receipt of ACCEPT_JOIN message from its PCH node, it joins the cluster as
a member node. }
End;

4.3 Simulation Results

a) Simulation Model and Parameters

The Network Simulator (NS-2) is used to simulate the proposed architecture. In the simulation, mobile nodes are randomly deployed in 750 meter x 750 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized below:

Number of Nodes: 100 to 500; Node Speed: 5 m/s to 25 m/s; Area Size: 750 X 750 m; Mac: IEEE 802.11; Transmission Range: 20m; Simulation Time: 50 Sec; Traffic Source: CBR; Number of CBR connections: 10; Packet Size: 512; Rate: 50 kb; Initial Energy: 20 Joules; Transmission Power: 0.660; Receiving Power: 0.395.

b) Performance Metrics

The proposed TWCBRP is compared with the CBPMD protocol [16]. The performance is evaluated mainly, according to the following metrics. **Packet Delivery Ratio** is the ratio between the number of packets received and the number of packets sent. **Packet Drop** refers the average number of packets dropped during the transmission. **Delay** is the average end-to-end delay measured in seconds. **Energy Consumption** is the amount of energy consumed by the nodes to transmit the data packets to the receiver. **Throughput** is the average number of packets received per second.

c) Results

*A. **Based on Nodes:*** In our first experiment we vary the number of nodes as 100,200,300,400 and 500.

Table 7
Simulation Results

Nodes	Delay		Delivery Ratio		Energy		Throughput	
	CBPMD	TWCBRP	CBPMD	TWCBRP	CBPMD	TWCBRP	CBPMD	TWCBRP
100	7.558292	0.126717	0.72323	0.996462	12.57041	16.48706	5302	8730
200	10.11672	0.380857	0.777793	0.991782	15.30881	17.60048	5702	8689
300	16.45621	1.214569	0.549038	0.97466	14.53496	18.12165	4025	8539
400	13.61595	2.8902	0.141591	0.938591	11.88331	18.0135	1038	8223
500	12.85457	0.788641	0.182547	0.983449	13.84155	17.81934	3008	8616

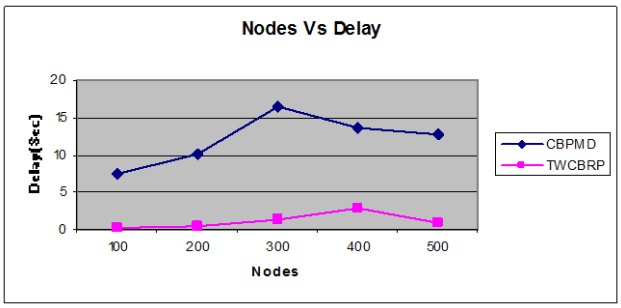


Figure 1: Nodes Vs Delay

Figure 7 shows the delay of TWCBRP and CBPMD techniques for different nodes scenario. We can see that, for nodes 100, the delay of TWCBRP is 98.32% lower than the existing CBPMD technique, for nodes 200 the delay of TWCBRP is 96.23% lower than the existing CBPMD technique, for nodes 300 the delay of TWCBRP is 92.61% lower than the existing CBPMD technique, for nodes 400 the delay of TWCBRP is 78.77% lower than the existing CBPMD technique, for nodes 500 the delay of TWCBRP is 93.86% lower than the existing CBPMD technique. In over all we can conclude that the delay of our proposed CBPMD approach has 92% of lower than CBPMD approach.

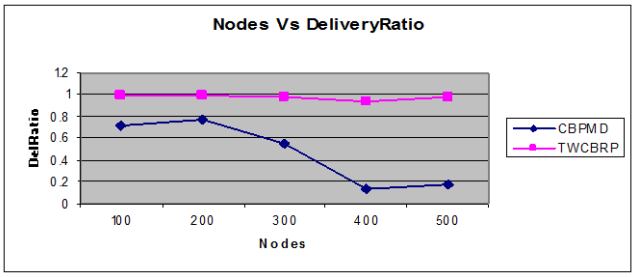


Figure 2: Nodes Vs Delivery Ratio

Figure 8 shows the delivery ratio of TWCBRP and CBPMD techniques for different nodes scenario. We can see that, for nodes 100, the delivery ratio of TWCBRP is 27.42% higher than the existing CBPMD technique, for nodes 200 the delivery ratio of TWCBRP is 21.57% higher than the existing CBPMD technique, for nodes 300 the delivery ratio of TWCBRP is 43.66% higher than the existing CBPMD technique, for nodes 400 the delivery ratio of TWCBRP is 84.91% higher than the existing CBPMD technique, for nodes 500 the delivery ratio of TWCBRP is 81.43% higher than the existing CBPMD technique. In over all we can conclude that the delivery ratio of CBPMD approach has 52% of higher than CBPMD approach.

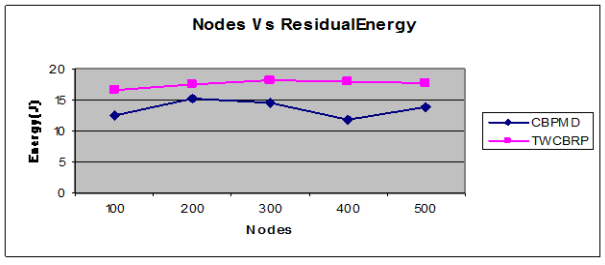


Figure 4: Nodes Vs Residual Energy

Figure 9 shows the residual energy of TWCBRP and CBPMD techniques for different nodes scenario. We can see that, for nodes 100, the residual energy of TWCBRP is 23.75% higher than the existing CBPMD technique, for nodes 200 the residual energy of TWCBRP is 13.02% higher than the existing CBPMD technique, for nodes 300 the residual energy of TWCBRP is 19.79% higher than the existing CBPMD technique, for nodes 400 the residual energy of TWCBRP is 34.03% higher than the existing CBPMD technique, for nodes 500 the residual energy of TWCBRP is 22.32% higher than the existing CBPMD technique. In over all we can conclude that the residual energy of CBPMD approach has 23% of higher than CBPMD approach.

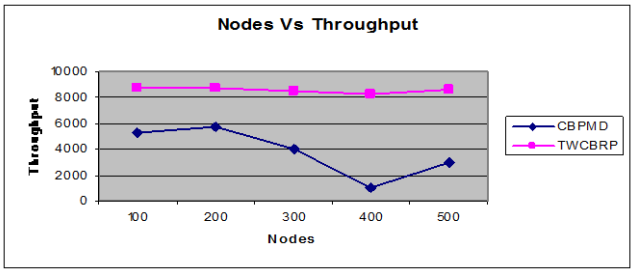


Figure 3: Nodes Vs Throughput

Figure 10 shows the throughput of TWCBRP and CBPMD techniques for different nodes scenario. We can see that, for nodes 100, the throughput of TWCBRP is 39.26% higher than the existing CBPMD technique, for nodes 200 the throughput of TWCBRP is 34.37% higher than the existing CBPMD technique, for nodes 300 the throughput of TWCBRP is 52.86% higher than the existing CBPMD technique, for nodes 400 the throughput of TWCBRP is 87.37% higher than the existing CBPMD technique, for nodes 500 the throughput of TWCBRP is 65.08% higher than the existing CBPMD technique. In over all we can conclude that the throughput of our proposed TWCBRP approach has 56% of higher than CBPMD approach.

5. Conclusion

In this paper, we have proposed a trust sensitive weighted dual cluster head based routing protocol which ensures secured routing and enhances connectivity in MANET. Since malicious and selfish nodes are isolated from the routing path, this guarantees secured and trusted path from source to destination. Moreover, with primary and secondary cluster heads, the stability of the routing path as well as the stability of the cluster structure is also guaranteed.

References

[1] Udhayavani, M., and M. Chandrasekaran. "Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: a trust-aware routing framework for wireless sensor networks." *Cluster Computing (Springer)* 22.5 (2019): 11919-11927.

[2] Priya, I. Leela, S. Lalitha, and P. Victer Paul. "ENERGY EFFICIENT ROUTING MODELS IN WIRELESS

SENSOR NETWORKS-A RECENT TREND SURVEY." *International Journal of Pure and Applied Mathematics* 118.16 (2018): 443-458.
[3] Ahmed, Adnan, et al. "A trust aware routing protocol for energy constrained wireless sensor network." *Telecommunication Systems* 61.1 (2016): 123-140.

[4] Revathi, S., and T. R. Rangaswamy. "Secure Route Discovery using Opinion Based Method in MANET." *International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.5, No.1, February 2015.*

[5] Aruna, S, and A. Subramani. "Weighted Double Cluster Head Based Approach for Enhancing Route Stability in MANETS." *Asian Journal of Information Technology* 13.11 (2014): 725-732.

[6] Paramasivan, B., and M. Kaliappan. "Secure and Fair Cluster Head Selection Protocol for Enhancing Security in Mobile Ad Hoc Networks", *The Scientific World Journal* (2014).
[7] Aruna, S, and Dr. A. Subramani. "Comparative Study of Weighted Clustering Algorithms for Mobile Ad Hoc Networks." *International Journal of Emerging Technology and Advanced Engineering* 4 (2014): 307-311.
[8] Jichkar, Mr Rahul A., and M. B. Chandak, "Application of Indirect Trust Computation in MANET", *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 3, Issue 3, March 2014.

[9] Venkanna, U., and R. Leela Velusamy. "TEA-CBRP: Distributed cluster head election in MANET by using AHP." *Peer-to-Peer Networking and Applications* (2014): 1-12.

[10] Maleknasab, Mehdi, Moazam Bidaki, and Ali Harounabadi. "Trust-based clustering in mobile ad hoc networks: Challenges and issues", *International Journal of Security and Its Applications* 7.5 (2013): 321-342.