sciendo

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **23**, No 1
Sofia • 2023 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2023-0005

Performance of Optimized Security Overhead Using Clustering Technique Based on Fuzzy Logic for Mobile ad hoc Network

Amrendra Singh Yadav[1], *Avjeet Singh*[2], *Ankit Vidyarthi*[3], *Rabindra Kumar Barik*[4], *Dharmender Singh Kushwaha*[5]

[1]*IIITM Gwalior, India*
[2]*Sharda University, Greater Noida, India*
[3]*Jaypee Institute of Information Technology University Noida, India*
[4]*KIIT Deemed to be University, Bhubaneswar, India,*
[5]*MNNIT Allahabad, India*
E-mails: asy@iiitm.ac.in ankit.vidyarthi@jiit.ac.in avijeet.mnnit.cs@gmail.com rabindra.mnnit@gmail.com dsk@mnnit.ac.in

***Abstract*:** *MANET is an autonomous wireless network without any centralized authority, consisting of a dynamic topology with a multi-hop scenario. Clustering provides centralized authority within MANET and makes the network stable up to some extent. Security is one of the most challenging aspects, directly proportional to load and overhead over the network. The model being proposed uses a cluster-based technique and modified secure routing protocol, which minimizes the network's load and overhead, improving the network's security and performance. Two major factors are used as contribution level and stability factor for the choice of cluster head, which minimizes the method of re-selection for cluster head. The node addition using authentication and the Modified Secure Routing Protocol increases the security of the network. The Modified Secure Routing Protocol, based on limited and efficient use of the certificates with encryption and decryption of packets, minimizes the overhead and load over the network. Hence, it provides more efficiency and security.*

***Keywords*:** *Security; overhead; load; cluster; fuzzy logic; goodness factor; competence level; stability factor; mobility; contribution level*.

1. Introduction

Mobile Ad hoc NETwork (MANET) may be a self-managing, self-configuring, infrastructure-less wireless network composed of some mobile buyer pieces of appliances forming the non-permanent network. MANET is widely utilized in emergency relief and disaster, military operations, personal area networks, mobile conferences, and sensor dust. There are many factors, such as vitality, durability, heavyweight, bandwidth, authenticity, security, and many more, that affect the functioning as well as the performance of the network. MANET is an autonomous wireless network having a multi-hop layout and active topology. In MANET,

mobility and security are the two major parts. Hence, MANET is endangered by several attacks like man-in-the-middle attacks, spoofing, region attack, denial of service, wormhole attacks, etc., [1, 16]. Various key management schemes can be used to prevent and avoid attacks [2]. With security, due to dynamic topology, the inauguration is of key importance in system management and also one of the significant challenges, as well as the shortage of centralized authority and limited resources such as bandwidth, battery power or energy, etc., [15]. As we all know, security is related directly to the load and overhead over the network, which reduces the efficiency of the network [12].

The approach based on Clusters is used to prevent the network from these attacks and provide topological stability in the network. Here, the secure routing protocol being proposed increases security with less overhead and load over the network. The MANET is split into clusters (logical) that safeguard the network formation where the cluster head gets employed to update, originate, dispense, renovate, and repeal keys into its clusters and contribute to the route discovery and the anchored routing of packets [13]. Whenever the head of the cluster outstretches to its threshold, it rehabilitates the preceding subsequent cluster head for its cluster so that the dissemination does not get cut out. This work proposes a forecast on the election of a cluster head and implementing a secure routing protocol using only the most needed resources as resources in MANET are already very constrained. The remaining paper organization is as follows: Inside this paper, the assessment of the linked work that is used is briefly discussed in Section 2, the initiated work is described in Section 3, the analysis and validation of the initiated work are shown in Section 4 and the conclusion of our work is in Section 5.

2. Related works

As discussed above, the two major problems of MANET are the security and mobility of the network. A technique based on the cluster is used on the cluster to get control of this problem – the clusters are formed with the help of the cluster head. The cluster head works as a short-lived foot terminus at intervals in its neighborhood and communes with different cluster heads [17]. The main objective of cluster formation is to look after the network structure and then cut back the dispensation of a key organization over the network to minimize the versatility and expenses of the networks [11]. If a cluster head is undermined, the cluster is undermined going away, and the remainder of a network is shielded and stable [10]. Cluster heads can admit on a key for communicating firmly with the help of the cluster using the key agreement protocol of Diffie-Hellman. Electing the cluster head mobility [4] and residual energy [5] are the valued factors. The verification process of a node's stability factor and competent level is performed for these valued factors. The key management plan of action [6] embodies a disseminated arrangement that amalgamates both centralized and distributed key management to amalgamate the excellence or quality of the twain procedure.

In [6], MANET is split up into categories accommodating group leaders; similarly, at this place, the network is split up into multiple clusters with a cluster

head as a temporary centralized entity. A secure routing protocol approach is used, but it will increase the overhead and load over the network with security. The contribution level is the parameter used to select cluster head and node stability, where the contribution level of a node depends on node degree. Competent level and goodness function as in [7] using Fuzzy Logic [8, 14]. The concept of a weak node is taken from paper [9]. The node with a lesser node degree compared to others is called a weak node.

There are many algorithms for cluster head selection and cluster formation they have some drawbacks as lacking at some points as described below:

- Location based Clustering: Mobility factor, maximum number of nodes in a cluster, signal power information, etc., are not considered.
- Mobility based Clustering: Node degree, maximum number of nodes managed within a cluster are not considered.
- Neighbour based clustering: Stability factor, transmission range and many more factors have not been considered.
- Weighed based clustering: This technique does not consider reliability factor is lacking behind and calculation overhead is too high.

Based on literature survey, various problems have been encountered in clustering and secured routing protocols. Some of the main problems are as follows: in clustering, extra functionality of cluster head leads to power drainage and re-clustering takes place.

3. Proposed methodology

The MANET is split up into clusters and no other node is like to be left on the surface of the cluster. Every cluster has a cluster head that is selected right before the non-success of the antecedent one. Initially, all the nodes in a network have equal energy, and they are secure as authenticated nodes. Hence, initial cluster head selection will be made based on node degree. The Cluster head is re-selected when its energy level becomes less than its threshold value. The re-selection of cluster head will be done using the cluster head selection protocol based on two parameters – contribution level and stability factor [2, 3].

3.1. Cluster head selection protocol

The cluster head selection will be based on the parameters defined below using fuzzy logic. The cluster head selection depends upon the following two major parameters:

1. Contribution level of the node
2. Stability factor of the node

a) *Contribution level*. The Contribution level checks the participation of a node in the network's activity. It shows the behavior of the node towards the network. The contribution level of a node depends on various factors such as the degree of a node, competent level, and the goodness factor, which are described in brief below:

i. Node Degree. A node with a maximum degree of a node will be favored for the assortment process of the cluster head. Nodes are classified depending upon the node degree:

$$\text{Nt} = \begin{cases} \text{Reject if ND} = 0, \\ \text{Weak if } 0 < \text{ND} < 3, \\ \text{Considerable if } 3 \leq \text{ND} < 6, \\ \text{Strong if ND} \geq 6. \end{cases} \quad (1)$$

Node type are used to define some sets:

NDw, NDc, NDs are sets having nodes of type "weak", "considerable", and "strong", respectively. Preference can be defined in the following order:

$$\text{NDs} > \text{NDc} > \text{NDw}.$$

Based on the preferences shown above, a set will be selected for the next step for selecting cluster head based on fuzzy logic.

ii. Competent level. It is defined through energy level. Residual Energy E_i of normal node i can be defined as

$$E = \text{TE} - (E\text{c} + \Omega), \quad (2)$$

where: E is the node residual Energy; TE is the Total Energy of a node; Ω is in the ideal state; E_c is the energy which polished off due to noise and environmental factors.

iii. Goodness factor. The success factor is defined by the number of successfully forwarded packets without any dropping. The reliability of a node is shown by the success factor, which will help to define the goodness factor. Using fuzzy logic concept for selecting the parameter, the goodness factor can be formulated as: If the No of received packets ≠ 0, calculate Success factor,

$$\text{Sf} = (N_t - (N_d + N_r)) / N_t, \quad (3)$$

where, N_t is total transmitted packets; N_d is total discarded packets, N_r is total retransmitted packets.

Goodness factor, Competence level determines the membership degree of the relative elements in a set given, using fuzzy logic. It is defined in the next part of this section.

Nodes with high competence levels and goodness factors will participate in the upcoming selection process for cluster heads.

The contribution level of a node is a function depending on some factors like Node degree, Goodness factor, and Competence level,

$$\text{Ct}_i = f(\text{ND}, C_i, \text{GF}), \quad (4)$$

where: Ct_i is the i-th Contribution level; C_i is the i-th Competent level; GF is the Goodness factor; ND is the Node Degree.

The Contribution level of an individual node can be checked as, let us say, a node having a higher competence level but the node is a weak node, then this node will not be preferred first. Hence contribution level of this node will be below.

i. Stability factor. The stability factor is the measure for selecting a cluster head. The stability factor is an anti-proposal to cluster head reestablishment; therefore, we can save energy for cluster head formation in the future. In this way, we can reduce load over a network. Cluster head rotation leads to node detachment from the cluster head. Hence this method compromises the node security. The cluster head is chosen using the two deciding factors, neighbor node stability, and Self Stability.

ii. Self-Stability. This parameter represents the node stability with respect to the position previously. Let us take a situation where node I moves from the previous position (X_r, Y_r) to position (X_n, Y_n) with respect to time window t; then, the distance

covered can be obtained as:

(5) $$d_j^i = \sqrt{(X_n - X_r)^2 + (Y_n - Y_r)^2}.$$

To denote the Self-Stability (SS) of a node symbol *S* is used. Let *r* be the range, then it can be obtained as:

(6) $$\text{SS(t)}=\begin{cases} 1 \text{ if } D_i^t = r, \\ \frac{D_i}{r} \text{ if } D_i < r, \\ 0 \text{ else otherwise.} \end{cases}$$

To enhance stability, the value of *r* needs to be decreased from *r* to *r*/2 and *r*/4.

iii. Neighbour node stability. It is often represented that in terms of their self-stability, to what extent a node is being connected to its neighbor. Within the transmission range, nodes can exchange messages with other nodes present in the range. At each node, one-hop neighbors' connectivity information and signal stability are gathered and stored. Each node accumulates the information of the neighbor list that maintains an identifier for every neighbour.

(7) $$\text{NS}(t) = \alpha \times \frac{1}{\text{ND}} \rightarrow \sum_{i=1}^{\text{ND}} \text{S}(i) + (1-\alpha) \times \text{NS}(t-1).$$

Here, the aging factor is denoted by α ($0 < \alpha < 1$), and node degree is denoted by ND. With the change in the value of α, the stability of the neighbor node can be predicted. If there is an increment in α, it means an increment in the stability of the neighbor node; otherwise, a decrement in the stability.

The overall stability of a node in terms of the total mobility of a node can be represented with the help of the Stability Factor (SF). SF supports these two factors and is often calculated as

(8) $$\text{SF} = f(\text{NS}, \text{SS}) = \beta \times \text{SS} + (1-\beta) \times \text{NS}.$$

In a given set, μ_C (SF) is a membership function that can determine the degree of membership of the elements, using fuzzy logic and selecting the node for cluster head having maximum stability factor.

3.2. Proposed model for fuzzy-based cluster head election

Here we propose a model for selecting cluster heads based on the fuzzy logic technique. During the selection of a cluster head, three input functions such as stability factor, goodness factor, and competence level of a node are used. This information is converted in the form of fuzzy sets. The information about the degrees of membership is maintained in a fuzzy set.

The goodness factor, stability factor, and competence level of a fuzzy set are shown as

$$A = \{(e, \mu_A(e))\}, e \in E,$$
$$B = \{(g, \mu_B(g))\}, g \in G,$$
$$C = \{(s, \mu_C(s))\}, s \in S.$$

Here *S*, *G*, *E* are universal of divulging for Stability factor, Success factor, and Residual energy, respectively. They are obtained through SF, Sf, and E_i defined above; *s*, *g*, and *e* are the elements of *S*, *G*, and *E*, respectively; $\mu_C(s)$, $\mu_B(g)$, $\mu_A(e)$ are the membership functions, which represent the stability factor, success factor, and competence level respectively find the membership degree in a given set of the element.

The membership functions for stability factor, goodness factor for success factor, and competence level for residual energy are defined as follows:

$$(9)\ \mu_A(e) = \begin{cases} 1 \text{ if } e > \text{TH2} \\ (e - \text{TH1})/(\text{TH2} - \text{TH1}) \text{ if } \text{TH1} < e < \text{TH2}, \\ 0 \text{ if } e < \text{TH1}, \end{cases}$$

$$(10)\ \mu_B(g) = \begin{cases} 1 \text{ if } \text{TH2} \le g < 1 \\ (g - \text{TH1})/(\text{TH2} - \text{TH1}) \text{ if } \text{TH1} \le g < \text{TH2}, \\ 0 \text{ if } g < \text{TH1}, \end{cases}$$

$$(11)\ \mu_C(s) = \begin{cases} 1 \text{ if } \text{TH2} \le s < 1 \\ (s - \text{TH1})/(\text{TH2} - \text{TH1}) \text{ if } \text{TH1} \le s < \text{TH2}, \\ 0 \text{ if } s < \text{TH1}, \end{cases}$$

Here: TH1 is the required threshold to activate the system; TH2 is the required threshold, which indicates the level of activeness.

A membership function can describe the relationship between elements of *E*, *G*, and *M* (fuzzy relation), as $\mu_E \times S \times G$ (e, s, g), $e \in E$, $s \in S$ and $g \in G$.

Now after applying AND fuzzy operator, i.e., min (∧) on fuzzy relation,

$$(12)\quad \mu_A(e) \wedge \mu_B(g) \wedge \mu_C(s) = \min\left(\mu_A(e), \mu_B(g), \mu_C(s)\right) = \\ = \begin{cases} \mu_A(e) \text{ iff } \mu_B(g) \ge \mu_A(e) \le \mu_B(s)\, \mu_B(g), \\ \mu_B(g) \text{ iff } \mu_B(e) \ge \mu_A(g) \le \mu_B(s)\, \mu_C(s), \\ \mu_C(s) \text{ iff } \mu_B(e) \ge \mu_B(s) \le \mu_B(g). \end{cases}$$

3.2. Rule evaluation

Cluster Head selection protocol involves competence level, goodness factor, and stability factor.

Table 1. Input function

Input	Membership		
Residual energy	Less	Sufficient	Large
Stability factor	Low	Medium	High
Success factor	Less	Adequate	High

All these factors are based on fuzzy logic, which is depicted in Table 1, which shows the varying degree of input variables using the membership function. The probable output functions that may vary are shown in Table 2 and Table 3. For input functions, the order of precedence is:

Competence level > Stability factor> Goodness function.

Table 2. Output function

Output	Membership
Output memberships	R1, R2, R3, R4, …, R25, R27

For ranking of output memberships, precedence order is

R1 > R2 > R3 > R4 > … R24 > R25 > R27.

Proposed rule set. The given model defines all the possible combinations of the different membership functions for the three input variables. The output shows the 27 rules for the fuzzy interference shown in Table 3.

Table 3. Logical rulesets

Residual energy	Stability factor	Success factor	Output memberships
Less	Low	Less	R27
Less	Low	Adequate	R26
Less	Low	High	R25
Less	Medium	Less	R24
Less	Medium	Adequate	R22
Less	Medium	High	R21
Less	High	Less	R23
Less	High	Adequate	R20
Less	High	High	R19
Sufficient	Low	Less	R18
Sufficient	Low	Adequate	R16
Sufficient	Low	High	R15
Sufficient	Medium	Less	R14
Sufficient	Medium	Adequate	R8
Sufficient	Medium	High	R7
Sufficient	High	Less	R10
Sufficient	High	Adequate	R6
Sufficient	High	High	R5
Large	Low	Less	R17
Large	Low	Adequate	R13
Large	Low	High	R12
Large	Medium	Less	R11
Large	Medium	Adequate	R4
Large	Medium	High	R3
Large	High	Less	R9
Large	High	Adequate	R2
Large	High	High	R1

3.3. Proposed algorithm cluster head selection

The algorithm takes care of a proper and optimized cluster head selection algorithm. Let TH1 and TH2 be upper bound and lower bound as threshold value, ND[*k*] is node degree of *k*-th node, NDc, NDs and NDw are arrays representing the set of nodes having considerable, strong and weak node degree, respectively Algorithm 1.

Algorithm 1. Optimized Cluster Head Selection

Step 1. ***Input:*** Cluster Head Selection

Step 2. ***Output:*** Avoid Low Energy

Step 3. Procedure: Check the parameter of Cluster Head Selection

Step 4. Initialize $i \leftarrow 1$, $j \leftarrow 1$, $k \leftarrow 1$

For all *k*, where *k* is node in a cluster

For $i \leftarrow 1$ to n

a) **if** (TH1<=ND[*k*] <= TH2) then, set $ND_C[i] \leftarrow k$

b) **else If** (ND >= TH2) then, set $ND_S[i] \leftarrow k$

c) **else If** (ND <= TH1) then, set $ND_W[i] \leftarrow k$

d) (ND <= TH1) then, set $ND_W[i] \leftarrow k$

Step 5. Selecting set *S* for applying fuzzy logic on selected nodes only

a) If(ND_C[0] != Ø) then, For i←1 to n
$S[i] \leftarrow k$ for all $k \in$ NDc
b) elseIf (NDs[0] != Ø) then, For i←1 to n
$S[i] \leftarrow k$ for all $k \in$ NDc
c) else, For i←1to n
$S[i] \leftarrow k$ for all $k \in$ NDc

Step 6. Apply Fuzzy logic on S[ ] and store fuzzy output in X[ ]
Step 7. Based on X[ ], select node as Clusterhead, Ch using fuzzy rule set
Step 8. Finally, Ch is cluster head of that cluster
Step 9. End Procedure

3.4. Node addition using authentication

Whenever a new node is added to the cluster, it sends a request to the cluster head. This sent request possibly may be incarcerated by a malevolent node that also acts as a cluster head, or a malicious node can send the request to the cluster head to join the cluster. Therefore, before adding a new node, the cluster head, and new node both authenticate each other.

The authentication process is described below as follows.

3.4.1. Authentication of cluster head using other nodes

Initially, the cluster head works similarly as in [2], but more steps are also added. Cluster head selects a random secret number S such that ($1<S<N$) and two large prime numbers as p and q after that compute: $N = (p \times q)$ and $V=S^2 \bmod N$. Here, V and N are announced in the cluster publicly illustrated in Fig. 1.

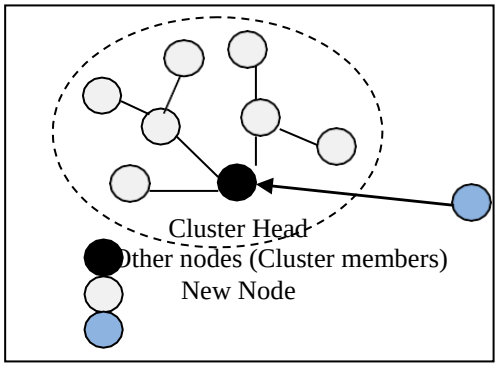


Fig. 1. A Cluster in MANET

When the cluster head receives a challenge to authenticate itself, it selects the random number R such that $1<R<N$ and calculates $X=R^2 \bmod N$. Then cluster head sends $\langle N, V, X \rangle$ to the new node. On receiving $\langle N, V, X \rangle$, a new node sends the challenge c to the cluster head. The cluster head then calculates the value of [$Y= (RS^c) \bmod N$] and forwards this value to the new node. Now, the node computes $X \times V^c$ and matches Y^2.

If it is matched, then it is proven that they are not acting maliciously, but we cannot rely on this calculation only, as most of the numbers are generated.

Calculations are done by the cluster head only that is being authenticated. So here, we use some additional approaches for fully authenticating the cluster head, that new node rechecks $\langle N, V \rangle$ from other nodes (members of that cluster).

For verification purposes, the new node selects i nodes from all the cluster members and sends them verification messages, including $\langle N, V \rangle$. On getting this all-selected node, check $\langle N, V \rangle$ and send a token T_{reply} to the new node which wants to be a member of that cluster. On receiving a positive response as $T_{\text{reply}} = 1$ from j nodes cluster head gets fully authenticated; otherwise, authentication fails, where $j<i$ and j is a threshold value such that at least j number of nodes send a positive reply.

After getting more than two times verification messages by the same node for different $\langle N, V \rangle$ within some time interval, that node's information is forwarded to the cluster head, where the cluster head blocks it. After that cluster head forwards the message to the other cluster heads to block it, and they do the same.

Let us consider two small prime numbers, p=2, q=3, and calculate N=6. Let secret key S be 5 and calculate V, as $V = S^2 \text{mod} N = 1$. Now select any random number 7 and calculate $Y = R^2 \text{mod} N = 1$. The cluster head sends $\langle 6, 1, 1 \rangle$ to the new node without sending the value of S and R. After receiving the value new node will send a challenge c=9. On receiving a challenge, the cluster head calculates $Y=RS^c$ mod. $N=7\times5^2$ mod6=1and sends it to a new node. After receiving Y the new node calculates $Y^2=1$ and $X\times V^C = 1$, and as soon as it gets matched new node sends $\langle N, V \rangle$ to other members for token verification. Like this, a new node verifies and authenticates the group leader.

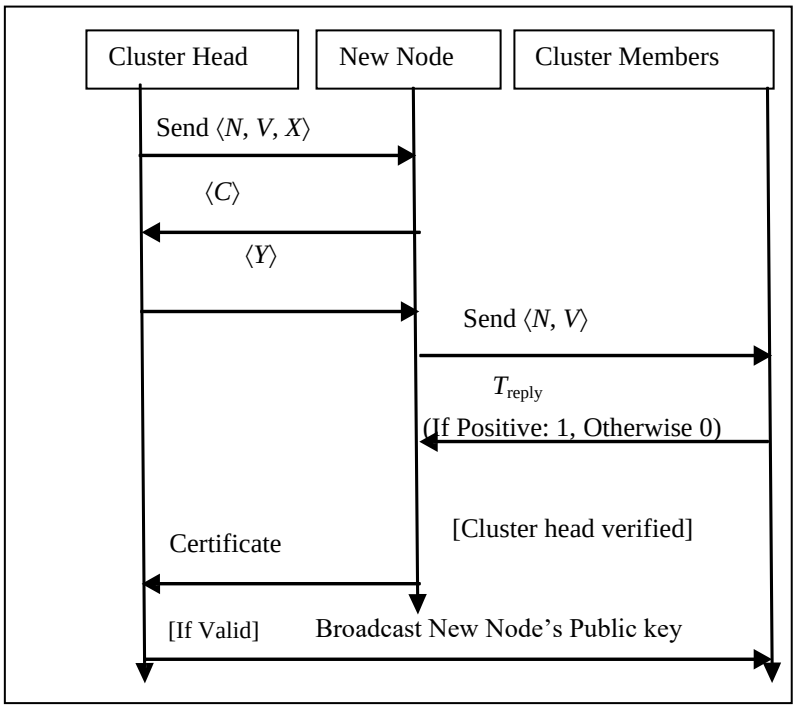


Fig. 2. Authentication process during new node addition mathematical verification of authentication of a group leader

3. 4. 2. Authentication of a new node

If the cluster head is successfully authenticated, the new node sends its certificate to the cluster head and supernode issued by a Trusted Third Party (TTP). With the help of a supernode, the cluster head verifies the node's certificate. A node_id is generated by the cluster head, the node_id and a key generated by function *f* are shared by the cluster head, and the node that is encrypted with the public key of the new node is sent by the cluster head.

The cluster head sends e_x (node_id, k) to all nodes where the e_x is the new node's public key. Then cluster head modifies the cluster key and list of cluster members, and this information is forwarded to the cluster members a illustrated in Fig. 2.

3.5. Modified secure routing protocol

The suggested Modified Secure Routing Protocol (MSRP), liaises nodes because the source nodes attach their digital signatures and of received Route REQuest (RREQ) message to RREQ message then rebroadcast RREQ message. When the neighbors of the source receive the RREQ, the decision is made according to the verification of the source signature, and the decision is taken accordingly. The sequence number of the destination [6] within the protocol is attached or included to form the routing in a loop-free manner and to check the freshness of the route control packet. There could be a situation where the source and destination nodes may or might not be present within the same group. Modified secure routing protocol uses the AODV protocol.

Security includes two stages:

Stage 1. Authorization of nodes is done with digital signatures.

Stage 2. Private and public keys for secure data transmission over the network.

RREQ packet contains the Digital Signature (DS) of the source node, predecessor node, and current node only, whereas the RREP packet contains the DS of the current node, predecessor node, and Destination node.

3.5.1. Route discovery

Route REQuest (RREQ) and Route REPly (RREP) packets are the two types of packets consisting of Route Discovery. In the proposed protocol, these packets are modified, with the original fields of RREQ & RREP packet digital signatures appended. These packets are then hashed for secure route discovery.

RREQ packet format is

PT	SA	SSEQ	DA	DSEQ	BID	HOP
PA	CA	DSs	DSp	DSc	Tp	Res

RREP packet format is

PT	SA	DA	DSEQ	HOP	LF	
PA	CA	DSc	DSP	DSD	Tp	Res

Here: PT is Packet Type; SA is Source IP Address; DA is Destination IP Address; PA is Previous Node IP Address; CA is Current Node IP Address; SSEQ is Source SEQuence number; DSEQ is Destination SEQuence number; BID is Broadcast ID;

HOP is Hop Count; DSs is Digital Signature of Source node; DSD is Digital Signature of a Destination node; DSP is Digital Signature of Predecessor node; DSc is Digital Signature of Current node; Tp is Timestamp (Used for calculating latency in route discovery); Res is Flag and Reserved Bytes.

Generally, the AODV protocol uses the DS of all nodes. DS of all nodes is appended in the RREQ and RREP packet, increasing the packet size and overhead over the network. In our proposed work, three digital signatures are only used for authentication purposes, which decreases the packet size and minimizes the overhead over the network. Each digital signature consists of 6 bytes, increasing the packet size of the normal RREQ and RREP packet of the AODV protocol used, shown in Fig. 3.

The Hash Function for verification can be calculated considering the values below:

$$Hx=H(S, \langle \text{Predecessor} \blacktriangleright \text{ Predecessor}\rangle, \langle \text{Predecessor}\rangle, \langle \text{HOP}\rangle).$$

New Hash Function can be calculated considering the values below for replacing the old one:

$$Hx = H(S, \langle \text{Predecessor}\rangle, \langle \text{Current}\rangle, \langle \text{HOP}\rangle).$$

3.5.2. Example

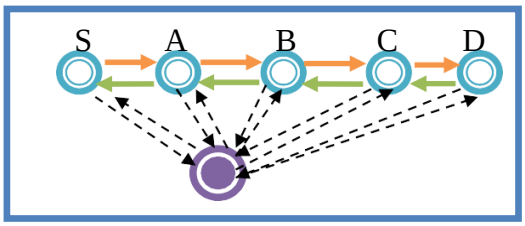


Fig. 3. Sub-network Route Discovery

1) *S* × RREQ (*S*, *D*, Seq, Hop, ⟨*S* ⟩, DSs, hS)

2) *A* × RREQ (*S*, *D*, Seq, Hop+1, ⟨*S*, *A*⟩, DSs, DSA, hA)

3) *B* × RREQ (*S*, *D*, Seq, Hop+2, ⟨*S*, *A*, *B*⟩, DSs, DSA, DSB, hB)

4) *C* × RREQ (*S*, *D*, Seq, Hop+3, ⟨*S*, *A*, *B*, *C*⟩, DSs, DSB, DSC, hC)

5) *D*→*C* RREP (*S*, *D*, Seq, Hop, LREQ, ⟨*S*, *A*, *B*, *C*, *D*⟩, DSs, DSD, hD)

6) *C* → *B* RREP (*S*, *D*, Seq, Hop–1, LREQ, ⟨*S*, *A*, *B*, *C*, *D*⟩, DSC, DSD, DSS, hB)

7) *B* → *A* RREP (*S*, *D*, Seq, Hop – 2, LREQ, ⟨*S*, *A*, *B*, *C*, *D*⟩, DSB, DSC, DSD, hB)

8) *A* → *S* RREP (*S*, *D*, Seq, Hop – 3, LREQ, ⟨*S*, *A*, *B*, *C*, *D*⟩, DSA, DSB, DSD, hA)

Notations

1) LRREQ → Lifetime
2) *H* → Hash function
3) *A* → * A broadcasts message.
4) Seq → Destination sequence number.
5) DSA → Digital Signature of node *A*.
6) *B* → *A*: *B* sends a message to *A*.
7) hA → Hash code appended by *A* to RREQ.

At every node, these are verified by their cluster head whether they are valid and authorized nodes or not, which maintains security by reducing the overhead over the network. As RREP and RREQ packets contain these certificates, the previous [6] Secure routing protocol increases the traffic over the network by sending more packets over the network as the number of certificates appended will be variable depending on the path and how long it follows the route discovery. Whereas, Modified Secure Routing Protocol [MSRP] reduces the traffic over the network, reducing the load and overhead due to the transmission of more information during every route discovery process for secure route setup. Therefore, overall overhead and load over the network decrease using this secure routing protocol.

3.5. Proposed algorithm modified secure routing protocol

Algorithms 2 and 3 take care of optimization in the modified secure routing protocol.

Algorithm 2. Routing Protocol
Step 1. ***Input:*** Size of Message, Bandwidth, Processing Power
Step 2. ***Output:*** Receiving Packets
Step 3. Procedure: Check the parameter of Secure Routing
Step 4. Initialize *S*← Source and *D*← Destination)
Step 5. *S* Check for a route (*S*, *D*)
Step 6. IF (route(*S*, *D*) exists) THEN select that route for sending a data packet
Step 7. ELSE do Route_Discovery ()
Step 8. Select_Route ()
Step 9. Route_Maintenance ()
10. End Procedure

4. Experimentations and explorations

NS2 simulator has been used to evaluate the performance of the network. Several measurement matrices have been collected from the simulation to evaluate the performance of the proposed model. For assessing the performance of the network, an NS2 simulator is used. The simulation region is a bounded area of 500×500 units. The layout used for simulation is a flat grid, whereas the number of nodes taken is 20.

4.1. Performance of result and its observations

The following section discusses the results and observations of the proposed protocol with the previous SPR, SAODV, and general AODV routing protocol regarding the packet delivery ratio and network load. The value of the SPR protocol is an approximate value and not guaranteed. The performance evaluation is shown below:

a) Packet Delivery Ratio (PDR)

The PDR is defined as the ratio of the number of delivered packets and the quantity of sent packets. The cluster's performance is proportional to the PDR value, or it can be stated as the performance of the cluster increases with the increase in PDR value illustrated in Table 4. It is the ratio of the data packets successfully delivered to the destination and can be defined as:

PDR (%) = ((No of received packets) / (No of packets sent)) × 100.

Table 4. PDR (%) vs pause time (s)

Pause time	AODV	MSRP	SAODV	SRP
8	99.25	96.2	94.23	95.44
16	99.56	96.85	95.96	96.23
24	99.15	97.46	96.25	96.78
32	99.46	97.68	96.49	97.59
40	99.62	98.56	96.98	97.89

Fig. 4 represents the graph of PDR w.r.t. the pause time. According to the graph below, the routing over the modified clustering algorithm and optimized Modified Secure Routing Protocol (MSRP) is more efficient than then SAODV and SRP.

The PDR of the overall protocol is higher than that of SAODV and SRP but lower than the General AODV protocol. This is because the overall protocol does not factor in the additional overhead from implementing security measures, assuming that no individual node will behave maliciously within the network. Like this, the network form is more reliable with higher performance.

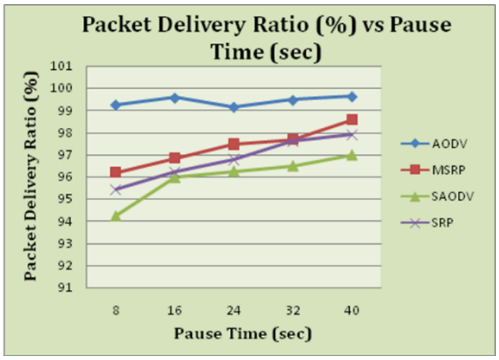


Fig. 4. PDR vs pause time

b) Network overhead

Network overhead is based on the number of packets send for route discovery, the packet size of RREQ/RREP, and granularity or time interval. It can be defined as shown in Table 5 and Fig. 5.

Network overhead = (No of packets sent×Packet size) / Time interval.

Table 5. Network overhead vs pause time

Pause time	MSRP	AODV	SRP (approximation)
8	408	264	864
16	2312	1948	2400
24	3332	2096	9334.5
32	6086	6168	13818
40	6664	5808	16023

Fig. 5 represents the graphical representation of SRP, MSRP, and AODV, between network overhead versus pause time. Modified Secure Routing Protocol (MSRP) consists of constant and less packet size compared to Secure Routing

protocol (SLR), due to which the overhead and load over the network will decrease, as illustrated in Fig. 5. Whereas, MSRP's network overhead is more than that of simple AODV due to the overhead involved during the implementation of security, which includes DS, Hash value, etc. Hence, the overall overhead over the network is less, which increases the performance over the network and utilizes the resources more efficiently, such as battery power and bandwidth.

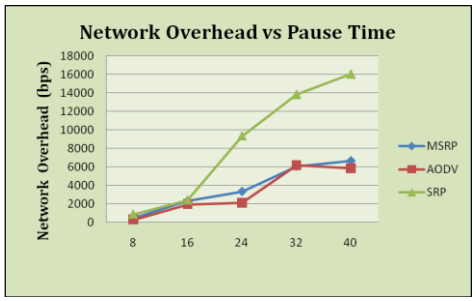


Fig. 5. Network overhead vs pause time

The total delay experienced by the packets from the generation of the packet at source till it is successfully delivered to its destination includes all the delays, such as a delay due to buffering during route discovery, queueing delay, retransmission delay, propagation time, and focusing on delay due to the verification process. It can be defined as:

For each packet send, calculate the send time and receive time and average them discussed in Table 6.

End to end delay (in s) = (Average receive time) – (Average send time).

Table 6. End to end delay (s) vs No of malicious node

No of malicious node	MSRP	SAODV	SRP (approximation)
2	3.3	4	5.33
4	4.3	6	6.43
6	3.9	6.2	6.95
8	4.7	6.8	7.99
10	5.2	7	8.54

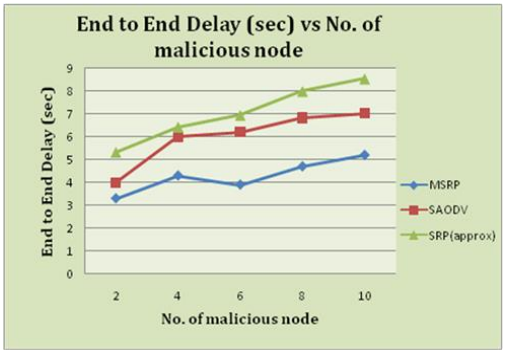


Fig. 6. End to end delay (s) vs No of Malicious nodes

Fig. 6 represents the graph of MSRP, SAODV, and SRP in presence of varying no of malicious nodes. It can be observed that in all three protocols, the end-to-end delay is very less than others (as SAODV and SRP) due to the clustering approach and fewer authentications with more security. Hence, the performance of the network increases.

5. Conclusion

The proposed technique minimizes cluster head selection and increases the efficiency of the network. Factors such as the goodness function provide trustworthiness and provide reliability to work better than other nodes. The higher the node degree lower will be the communication and authentication overhead over the network, but after some limit, it drains the resources. Hence, considering three levels of ranges for node degree optimum utilization of resources have been made, the competence level increases the efficiency and performance of the cluster head over the network. The mobility factor is included to increase the stability in the network, through which clustering cost reduces. The proposed protocol minimizes cluster head selection and increases the efficiency of the network.

Modified secure routing protocol uses only a limited number of certificates. It reduces the overhead of maintaining the security of the network. Hence, the overall performance and efficiency of the nodes over the network increase.

References

1. S e n, J. Security and Privacy Issues in Wireless Mesh Networks: A Survey. – Wireless Networks and Security: Issues, Challenges and Research Trends, 2013, pp. 189-272.
2. S h i v a n g i, S., A. K. D a n i e l. Fuzzy Logic Based Clusterhead Selection Protocol under Competence Level, Goodness Funciton and Mobility for Mobile ad hoc Network. – In: Proc. of Conference on IT in Business, Industry and Government (CSIBIG'14), 2014, pp. 1-6.
3. S h i v a n g i, S., A. K. D a n i e l. Cluster Head Selection Protocol under Node Degree, Competence Level and Goodness Factor for Mobile ad hoc Network Using AI Technique. – In: Proc. of 4th International Conference on Advanced Computing & Communication Technologies, 2014, pp. 415-420.
4. X u k a i, Z., B. R a m a m u r t h y. A Simple Group Diffie-Hellman Key Agreement Protocol without Member Serialization. – In: Proc. of 1st International Symposium, Computational and Information Science (CIS'04), Shanghai, China, 16-18 December 2004. Berlin, Heidelberg, Springer, 2005, pp. 725-731.
5. K a f h a l i, S. E., A. H a q i q. Effect of Mobility and Traffic Models on the Energy Consumption in MANET Routing Protocols. – arXiv preprint arXiv, 2013, pp. 1304-3259.
6. K u m a r, C. K., A. K. S. S a n g e r. Securing Mobile ad hoc Networks: Key Management and Routing. – arXiv preprint arXiv, 2012, pp. 1205-2432.
7. H o u s s e i n, H., S. A. S h a h r e s t a n i. Fuzzy Trust Approach for Wireless ad hoc Networks. – Communications of the IBIMA, Vol. **1**, 2008, pp. 212-218.
8. V i j a y a n, R., V. M a r e e s w a r i, K. R a m a k r i s h n a. Energy Based Trust Solution for Detecting Selfish Nodes in MANET Using Fuzzy Logic. – International Journal of Research and Reviews in Computer Science, Vol. **2**, 2011, No 3, pp. 647-652.
9. B r u s t, M. R., et al. Topology-Based Clusterhead Candidate Selection in Wireless ad hoc and Sensor Networks. – In: Proc. of 2nd International Conference on Communication Systems Software and Middleware, IEEE, 2007, pp. 1-8.

10. Y a n g, Y a-t a o, et al. A Feasible Key Management Scheme in Adhoc Network. – In: Proc. of 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'07), Vol. **1**, IEEE, 2007, pp. 300-303.
11. S i n g h, Y. A., et al. Increasing Efficiency of Sensor Nodes by Clustering in Section Based Hybrid Routing Protocol with Artificial Bee Colony. – Procedia Computer Science, Vol. **171**, 2020, pp. 887-896.
12. G u r u m o o r t h y, K. B., et al. A Novel Clustering Method for Fault Recovery and Routing in Mobile ad hoc Networks. – International Journal of Communication Systems, Vol. **34**, 2021, No 15, e4937.
13. M o h a m m e d, A. S., et al. FCO – Fuzzy Constraints Applied Cluster Optimization Technique for Wireless ad hoc Networks. – Computer Communications, Vol. **154**, 2020, pp. 501-508.
14. B o d d u, N., V. B o b a, R. V a t a m b e t i. A Novel Georouting Potency Based Optimum Spider Monkey Approach for Avoiding Congestion in Energy Efficient Mobile ad hoc Network. – Wireless Personal Communications, Vol. **127**, 2022, No 2, pp. 1157-1186.
15. F a t e m i d o k h t, H., M. K. R a f s a n j a n i. QMM-VANET: An Efficient Clustering Algorithm Based on QoS and Monitoring of Malicious Vehicles in Vehicular ad hoc Networks. – Journal of Systems and Software, Vol. **165**, 2020, pp. 3-16.
16. N a g e n d r a n a t h, M. V. S. S., A. R a m e s h B a b u. An Efficient Mobility Aware Stable and Secure Clustering Protocol for Mobile ADHOC Networks. – Peer-to-Peer Networking and Applications, Vol. **13**, 2020, pp. 1185-1192.

Received: 09.05.2022; Second Version: 17.10.2022; Third Verion: 27.02.2023; Accepted: 06.03.2023