DEFENDING AGAINST FALSE DATA ATTACKS USING CLUSTER BASED ROUTING IN A 3D GRID BASED MANET

B. Muneeswari*,
Assistant Professor,
Department of ECE,
SACS MAVMM Engineering College,
Madurai, TN, India.
Email: bmuneeswari04@gmail.com

M.S.K. Manikandan,
Associate Professor,
Department of ECE,
Thiagarajar College of Engineering,
Madurai, TN, India

*Corresponding Author: B.Muneeswari

Abstract **–** Quality of Service and Energy Efficiency are both required performances in the practical applications of mobile ad hoc networks. Due to the limited wireless link capabilities, paths with heavy load will reduce their energy rapidly and maximizes the possibility of path disconnection and packet drops. Hence optimal path is necessary to reduce the energy consumption in MANET. The Dual Cluster Head Election is developed based on node residual energy, distance and expected relative mobility. The dual cluster head selection considers the residual energy of nodes, average distance to neighbors and number of neighbor nodes. The existing multipath routing schemes distribute traffic amid multiple paths instead of routing all the traffic via single path. Two key issues arise in multipath routing are redundancy and quality. We address these issues in the proposed optimal routing paradigm where the best path is selected instead of routing among all available paths. We propose a hybrid approach that uses T2FLS (Type 2 Fuzzy Logic System) to identify a set of good paths and PSO (Particle Swarm Optimization) to identify a best path among the selected paths. Due to the lack of central monitoring system in MANET, insider attacks (False Data Injected Attack and False Route Attacks) may occur. To reveal this task, false data predicted on the source digital signature by upcoming cluster member. We compare the performance of our approach with those existing schemes and finally show that the proposed approach yields best performance with 0% packet loss rate.

Index Terms – 3D Grid MANET, PSO, T2FLS, False Data Attacks, Signencryption and Signdecryption

I. INTRODUCTION

The Mobile Ad hoc Network is an emerging research area where a set of mobile routers is connected. Recently, MANET is used in various applications include mobile networking, health monitoring system, emergency alert system, wireless communication in VANET. A node in MANET can joins with other nodes and moves randomly. Most commonly, this type of network does not follow any fixed/centralized infrastructure for mobile communication [1]. A mobile node in MANET does possess a few characteristics namely self-routing, autonomous and thus they do not require any special infrastructure. Routing protocols take the responsibility for establishing communication whenever required. It ensures routing policies like transmission, link connectivity, reliability, etc. Clustering is another opportunity to improve the network performance. It is an optimized reliability and stability achieved method wherein, a set of shorter distance nodes with high residual energy are interconnected to form a group [2]. Over the past few decades, many reasons are found for the inefficient clustering and routing namely limited battery capacity, node mobility, and node failure due to node energy depletion and data sharing. Node mobility is an essential type of metrics which causes failure of wireless links between nodes and thus it affects the number of reliable links in MANET [3]. A routing is promising using clustering approach wherein paths are noted among clusters rather than within nodes. It raises the network lifespan, reduces the rate of energy consumption and therefore reducing the extent of routing control overhead [4]. When rising network capacity, the routing overhead is reduced and it provides more efficacy to scalability. The cluster head in clustering takes accountable for numerous functions (routing table updates, novel routes detection and cluster maintenance). Among the previously existed multipath techniques, optimal path selection is a key topic in MANET. The multipath routing techniques with the subsequent issues are state below. Firstly, the overflow the route request to the entire network that gives large amount of communication overhead. Secondly, every node in network forwards route request data packets with the supreme energy. This leads to the obtain transmission of poorer energy for the receiver. In addition, numerous paths transfer data concurrently, although node disconnects multi paths are considered. Thus, the possibility for collisions may occur, which leads to higher packet loss rate as well as poor data transmission performance [5]. Routing protocols in ad hoc network is split into three types: table driven routing protocols (proactive), on-demand routing protocols (reactive) and hybrid. Proactive protocols: In this family of protocols, each node knows the address of every other node in the network. The examples of proactive protocols include: Fish-Eye State Routing (FSR), Cluster-Head Gateway Switch Routing (CGSR), Optimized Link State Routing (OLSR), and Destination Sequenced Distance Vector (DSDV). On the other hand, reactive protocols are also known as on-demand, this means that routes are elected as and whenever they required. The examples of reactive protocols include: Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Temporary Ordered Routing Algorithm (TORA) [6]. Aforementioned mentioned heuristics work well for small scale networks as the number of nodes in the MANET increases, the performance of these methods decreases, it may not able to provide good solution. Therefore, to find better solution in highly dense networks, meta-heuristic based approaches have been proposed to work efficiently in order to solve many optimization and combinatorial problems. In this research, a considerable amount of work has been done in the domain of meta-heuristics based routing either in one-hop and multi-hop routing. Particle Swarm Optimization (PSO) based routing approach is more beneficial in comparison to other meta-heuristics based approaches due to its robustness for effortless enumeration, control parameters, sensitivity toward fitness function and the ability of particles to share their information with other particles. The PSO based routing makes it more suitable for routing in large

scale networks. However, this meta-heuristic based solution suffers from large computational time in convergence when they work in huge multidimensional search space [7]. Thus the selection of the energy efficient schemes (either protocol or meta-heuristic) in MANET is an actually critical issue and it must be considered in all networks. MANETs does not have the user friendly environment due to its multi-hop communication and the lack centralized infrastructure. However, there is a possibility to attack the network by malicious/unauthorized users. To be finding this type of task in MANET is a complex and difficult. Besides that the malicious nodes can randomly join the network and cause various performance degradations, as interfering the routing information or listen to the communication over the network. In order to secure the MANET, the following attributes are required to be consider: data confidentiality, data integrity, authentication, availability and non-repudiation. However, the MANETs are vulnerable to different types of misbehaviour attacks. Mainly, there are two types of attacks in MANETs: active attacks and passive attacks. In active attacks, packets forwarded to unacceptable destinations into the network, changing contents of packets, removing packets and masquerading as other violate security criteria. Classification of misbehaviour attacks are shown in figure.1.

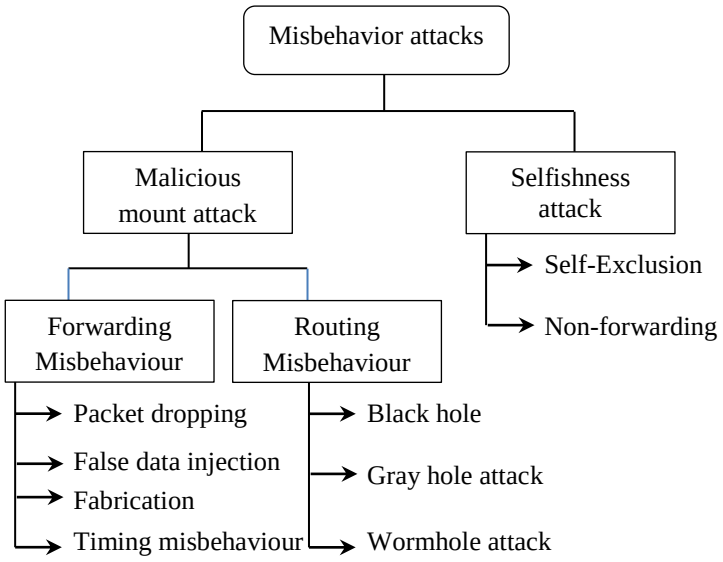

Figure.1. Classification of Misbehaviour Attack

These countermeasures are considered to eliminate or reduce the security attacks and vulnerabilities in the network [8]. The malicious nodes can inject false data to a trusted network. The insider attacker will be able to do different abnormal actions namely, drop, flood, listen and packet modification. Thus the any misbehaving action on trusted network can consume high network resources by continuously transmitting false messages [9].

This research intends to reduce energy consumption and prolong the network lifetime with assistance of meta-heuristics algorithm.

The major contributions of this paper are as follows:

The main aim of this proposed framework is to forward the packets through secured path with less hop-count.

i. To reduce the energy consumption rate, in this work, we proposed a new clustering approach named Dual Cluster Head Election (DCHe) rather than the single cluster head election.
ii. This scheme explores all the feasible paths from the source node to a destination node on the basis of their performance factors
iii. Among these feasible paths, the best optimal path is elected by the utilization of the newly formulated PSO algorithm. Thus the secure route is established by the newly derived T2FLS and PSO meta-heuristics algorithms.
iv. This scheme also protects and discovers the nodes from malicious attacks (false data injection attacks and false route attacks)
v. The results of the proposed framework are evaluated using throughput, delay, packet delivery ratio, energy consumption, and so on.

The organization of the rest of the article is organized as follows: the literature survey is discussed in section **2** where the related works of secure routing against some security attacks in MANETs are reviewed. The recent research problems under secure routing are explained in Section **3**. Section **4** describes the proposed system framework for protecting packets from internal attackers and providing a secured routing path. In section **5,** the simulation results of the proposed work with the comparison of previous approaches are available and finally, the conclusion of the research and outline of the future work is made in section **6**.

TABLE I. NOTATIONS DESCRIPTION

Notations	*Description*
T_{MN}	The total number of mobile nodes in a MANET
R	Population of PSO algorithm
k_{opt}	The number of optimal clusters in each round
T^n_{L-I}, T^n_{L-II}	Energy threshold for selecting cluster heads
p	Prime number
a, b	Integer element
$\mathbb{F}$.	Finite field
H_f	Hash function
D_m	Euclidean distance
$rm^t_{i,j}$	The relative mobility of the node n_j at instant t
$\varepsilon(t)$	Remaining energy
β_1, β_2	Weighting coefficients
$\alpha_1, \alpha_2, \alpha_3$	Random integers
F_1, F_2	Learning factors
μ, τ	Random numbers between 0 and 1
V	Particle velocity
X	Particle position
P_{ID}	Particle's best position
P_{GD}	Particles global best position
ω	Inertia weight
$f(i)$	Fitness function
TA	Trusted Authority
Pu_k	Public key
Pi_k	Private key
DS	Digital signature

II. RELATED WORKS

We have described several approaches of clustering, routing and security protocols developed for mobile ad hoc

networks. Many approaches have been presented to cope with the limitations of battery, mobility of nodes. In this section, we review the routing approaches in literature as two major categories: multi-path routing approaches versus optimal path routing (single path) approaches. In multipath routing, many paths are found and established between a pair of nodes (Source-Destination). In optimal path based routing approaches, only one path is found and established between a source-destination pair of nodes.

Naghma Khatoon et al., [10] have proposed mobility aware energy efficient clustering for MANETs. Energy efficiency and mobility awareness are two crucial optimization issues in MANER where in nodes move randomly at any direction. These problems are widely studied to maximize the lifetime of such ad hoc networks. This paper developed a clustering algorithm which is inspired by using particle swarm optimization algorithm by taking account of node mobility, degree and remaining energy. The cluster formation is considered by taking multi-objective fitness function using PSO. However, the basic PSO algorithm does not work well since it takes high processing time to form clusters.

In MANET, efficient routing has to be constructed on the basis of reducing control overheads, broadcasting hello messages, selecting secure and reliable nodes, and defining reliable route between source and destination node. In case of a highly dense network, the existing routing approach of ad hoc network generates high control overhead.

Gurpreet Singh et al., [11] introduced orientation based ACO (Ant Colony Optimization) for routing in mobile ad hoc networks. Recently, ACO is an important category of meta-heuristics algorithm which provides an efficient solution to many problems. An orientation factor is considered in ACO for routing between the source and the destination node. It is used to flood the search packets in the right direction. This scheme reduces network layer overheads because the end nodes selected randomly.

Irin et al., [12] have presented a novel method for selecting an optimal path selection between the nodes for packets transmission in mobile ad hoc network. Generally, routing protocol selects the route based on multiple objectives like distance between the nodes, hop count, trust values, received signal strength, residual energy, etc. The DBDP_AODV (distance based dual path ad hoc on demand distance vector) proposed which determined two routes between the source and destination. After the routes selection, optimal route is selected for routing. This type of routing improves the energy conservation rate but make easy to use of malicious users.

Many energy aware routing protocols have been presented by considering various issues such as topology control, transmission power control and adaptability but these algorithms have not considered the problem like early exhaustion of nodes battery, reliability and mobility constraints. Hence it increases node overall energy consumption of the routing path. The huge amount of energy consumption by the mobile nodes during transmission receives critical issue in routing. For example, kokilamani et al., [13] have presented an optimal path selection criterion called minimum energy threshold value. This paper considers the node energy level as an optimal path criterion. Each path is established depending on the energy threshold value. Thus, the nodes which are having minimum energy could select to complete the transmission successfully. A node energy level is an essential metric for routing, but other criterions are also required to improve the network performance in terms of delay, throughput, and lifetime of the node.

Mafirabadza et al., [14] have made an attempt to prolong the network lifetime and also reduce the delay by taking shortest path for data transmission. The proposed protocol is named as EPAAODV (Efficient Power Aware AODV). It is an extension of previous works known Ad hoc On-demand Distance Vector protocol (AODV) and power aware AODV (PAAODV). The major enhancement of this combined protocol is that it uses threshold residual energy of a battery(θ). Moreover, the combined protocol provides better performance than the individual techniques such as PAAODV and AODV, but still some of the issues (security, and quality of service) are unsolved.

Kumar et al., [15] have proposed an intelligent probabilistic strategy to broadcasting data packets among mobile nodes. This paper suggested retransmission probability based on its neighbourhood density, remaining energy of the node and available bandwidth. Further, the particle swarm optimization is presented for energy efficient and reliable routing. The PSO based probability forwarding scheme is beneficial than the existing protocols follows: 1). It is very easy to implement and efficient on global search, 2). Original probability is used rather than the blind flooding or fixed probability. The mobile nodes which are have high energy, less number of neighbours and available bandwidth, which increases the overall nodes lifetime in the network. However, the general PSO and fuzzy logic controller does not perform well in high dense networks.

Security is an essential concern for the basic functionality of MANET. Most of previously done studies based on security issue of node. For example, Dhananjay et al., [16] have proposed fuzzy based secure architecture (FBSA) for node classification and malicious activity detection using fuzzy detector. In order to detect and classify the malicious activities, three factors such as packet delivery ratio (PDR), packet forwarding (PF) and residual energy (RE) are used. Fuzzy rules are defined on the basis of requirement and analysis of malicious activity. The node malicious activity can be detected on the basis of conditions such as dropping of packet by neighboring node, destination node and forwarding node. The proposed approach is better than the existing approach but still the packet dropping rate is high.

Ramireddy Kondaiah et al., [17] presented an integrated algorithm for secure routing in MANET. An integration algorithm is entitled Fuzzy integrated Particle Swarm Optimization for secure routing. Various trust factors are considered to find the malicious nodes in a network. The trust value exploits the relationship between two nodes in a network. There are four trust computations are chosen for predicting the existence of malicious nodes are direct trust, indirect trust, recent trust, and historic trust. The model enhances the performance in terms of security but it is not suitable for large networks.

Bisen et al., [18] have proposed AB-SEP (Agent based Secure Enhanced Performance) approach in mobile ad hoc networks. This approach uses agent nodes which are selected through optimal node reliability. This factor is computed on the basis of node different characteristics such

as normalized distance value, energy level, mobility, degree of difference and optimal hello interval of node. The node malicious behavior detected using fuzzy based secure architecture (FBSA). This scheme reduces unnecessary broadcasting of hello messages and also minimizes end-to-end delay by using agent node.

Hrishabala et al., [19] presented a new approach namely energy efficient secure multipath AODV (EESM-AODV) which is an extension of AODV protocol. It is an adaptive approach which conjointly offers security by filtering route discovery process in routing protocol. The main issue of AODV protocol against mobile ad hoc network is to achieve efficiency in any type of network environment, but it does not verify the routing parameters included in protocol packets and no message integrity. Hence, an attacker can easily use/modify the messages and cause different security threats during routing

Brindha et al., [20] presented FSMR (Fuzzy Enhanced Secure Multicast Routing) which ensures better security in network and data. In order to measure the presence of misbehaving nodes, the FSMR approach is established from statistical data in normal and abnormal nodes. Certificateless based secure routing is developed and it authenticates data without the knowledge of certificate routing. Through the evaluation of the simulation results, the proposed system provide better data packet authentication with minimum energy consumption and this technique ensure nodes integrity, trustworthy and responsibility towards transferring packets.

Vamsi et al., [21] have proposed generalized trust model named generalized trust model (GTM) for cooperative routing. GTM is a self-adaptable, lightweight and effective protocol that efficiently utilized to identify and isolate malicious nodes in routing process. It is also a hybrid trust model that computes consolidated trust value of nodes. This GTM is integrated with three MANET routing protocols such as OLSR routing (proactive protocol), AODV routing (reactive protocol), and GPSR routing (geographic protocol). The energy consumption rate is high for these three MANET routing protocols.

III. Problem Definition

Srinivas aluvala et al., [22] have discussed node authentication for providing routing security in mobile ad hoc networks by implementing ones complement and cryptographic algorithm. It can be embedded in all the routing protocols to increase efficiency of the network. In this authentication scheme, each node on the network append ones compliment of its own IP address with public key secondly. The receiving node checks the packet authentication of its source by adding the appended ones complement and source IP address to it to get all ones but the encrypted data cannot be decrypted. At the same time, if a node fails authentication, a caution message is broadcasted over the network which indicates about the presence of a malicious nodes along with its IP address. The proposed key exchange protocol uses RSA algorithm to exchange the keys in the network. However, public keys are not efficient to provide security in the network.

Vallala et al., [23] presented multipath security aware routing protocol in MANET using trust enhanced cluster scheme (TECM) under lossless multimedia data transfer applications. The TECM algorithm considers multiple metrics input and computes trust value for each and every node in the network. The PSO algorithm is used for cluster formation. It works well against recent routing malicious attacks such as Byzantine, Sybil, Blackhole, Jellyfish, DoS, Wormhole attacks. However, the general PSO takes high computational time for routing data packets.

Deepa et al., [24] have presented a DE-AODV (Dynamic Energy Ad hoc on-Demand Distance Vector) which reduces packet delay, and energy consumption and thereby DE-AODV protocol selects the shortest route path from source to destination. The major problem which is not concern in this paper is network size. If the network size is increased then the performance of DE-AODV will become complicated and given high network overhead.

Saravanan et al., [25] have considered particle swarm optimization for optimal route selection using expected transmission count (ETX). The delivered rate of packets used to determine the optimal path. This method can easily find the total number of transmission and retransmission incidence on the link of optimal path. The system efficiency is increased by using the minimum hop count. However, energy consumption is a major concern in any type of wireless multi-hop networks. This problem is not focused in this paper and also overhead was not reduced.

In order to mitigate these issues, this research is developing a secure route based packet transmission algorithm, T2FLS & PSO by the combination of Type-2 Fuzzy Logic System and Particle Swarm Optimization for the optimal route selection against false data injection and route attacks.

III. Proposed Work

4.1 Overview

A dual cluster based routing algorithm is proposed in this paper for identifying the malicious node in 3D Grid based MANET. The main objective of the proposed method is to prolong the lifetime and prevent the mobile node from malicious activity by considering various performance metrics namely energy, mobility, distance, etc. Our proposed approach also used to solve security issues such as data confidentiality and data integrity in MANET. The proposed framework is illustrated as following blocks namely, cluster formation, cluster head selection, trusted authority, false data identification and finally evaluation of the proposed method performance. The detailed descriptions of these steps are given in the following subsections.

In MANET, there is "n" number of mobile nodes $n_i = \{n_1, n_2, n_3, \dots n_n\}$. In the proposed method, the initialization process is carried out to determine nearby nodes to send the packets.The mobile nodes deployed within a fixed area that are assigned with unique GIDs (Grid Identifiers). Each node in the network becomes aware of its neighboring nodes by broadcasting its IDs. The transmission among them started on wireless connections which are established only when nodes are within the communication range of each other. Let assume that the sender node as n_1 and one the neighbor node as n_2. Figure 1 represents 3D view of the network topology constructed with $x - y - z$ coordinates. Let find the following values for cluster formation and cluster head selection

4.2 Construction of Grid Structure

This paper creates a grid based network arranged in an N×M grid. A grid cell is divided into equal size in which the grids are formed with a unique identifier i.e. Grid Identifier (GID). This unique identifier is provided by its transmission range which is used to identify each grid cell. Each node in a grid can only communicate with its immediate neighbors based on the grid network topology (a node in the grid can communicate to its immediate vertical, horizontal and diagonal neighbors. Figure 2 shows the grid based network topology with N × M grids. To compute the grid size, the node location is used and the origin position of the grid defines(X_0, Y_0). The grid size is written by ρ which is determined based on the transmission range R$\left(\rho = \frac{R}{2\sqrt{2}}\right)$. If the nodes are deployed, then computes unique grid identifier which calculated by,

$$GID\ (x,y) = \left\{(x,y)|x = \left[\frac{X-X_0}{\rho}\right], Y = \left[\frac{Y-Y_0}{\rho}\right], (X_0,Y_0)\ \epsilon\ origin\ (0,0)(X_0 \le X) \wedge (Y_0 \le Y); \rho: Grid\ Size\right\} \quad (1)$$

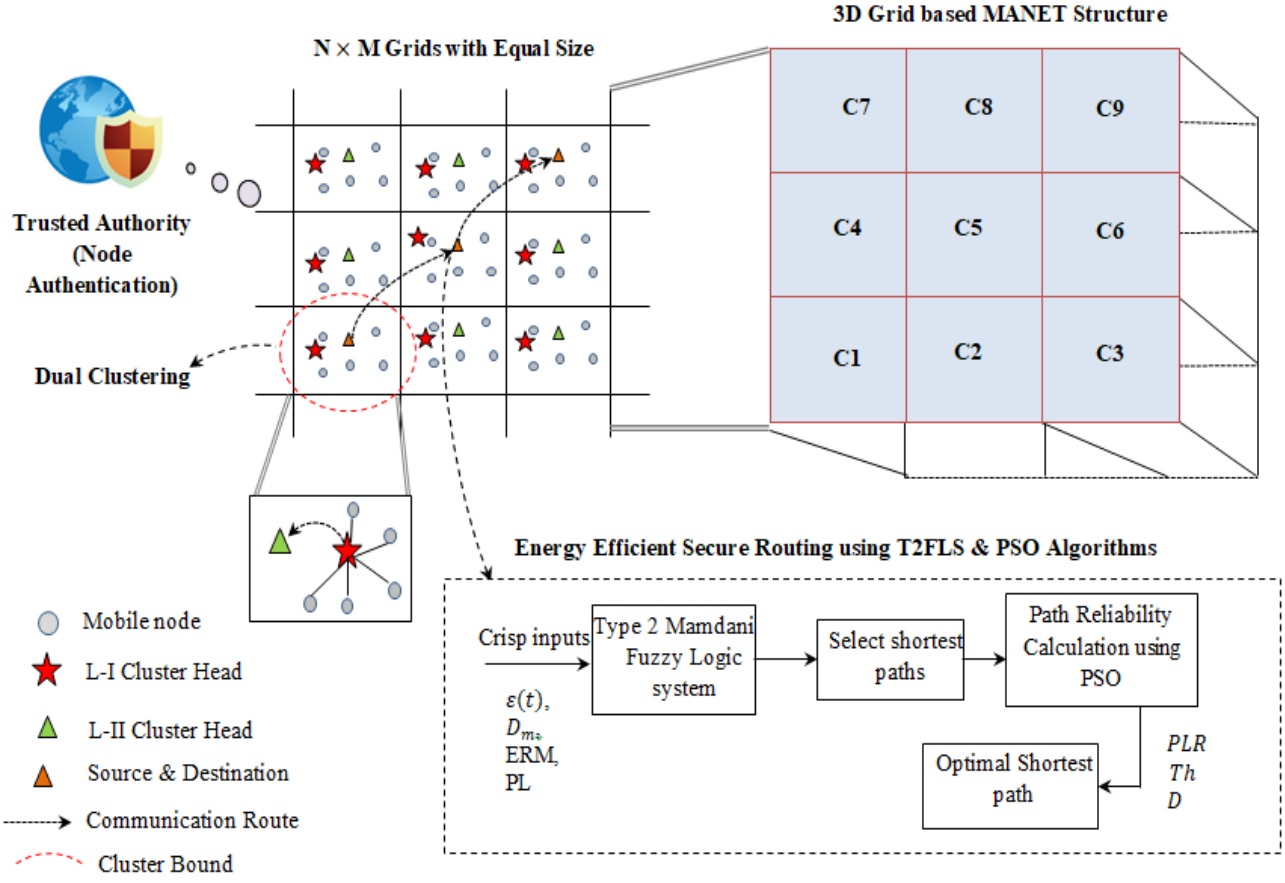

Figure 2.System Architecture

The link connectivity between mobile nodes to the neighbour mobile nodes derived using eqn. (1). If the node is positioned from any corner of the grid then that node also can communicate with its neighbour node.

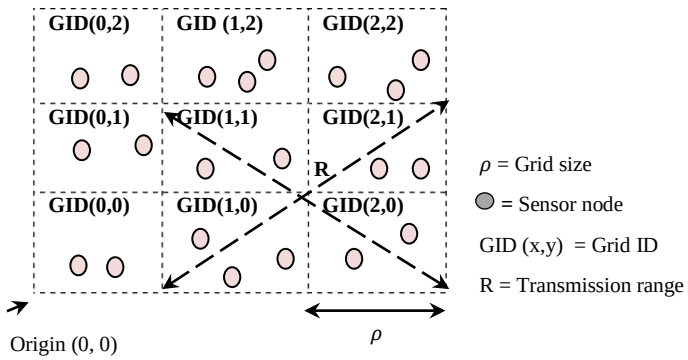

Figure 3.The Network Topology N× *M* Grid

4.3. Dual Clustering in MANET

In general clustering, each cluster head directly forward data to the destination node, which increases the cluster nodes energy consumption especially in large dense networks. To mitigate such issues, this paper puts forward a kind of dual clustering algorithm

4.3.1 Cluster Formation: This paper considered dual clustering algorithm where chose level-one cluster head (LI-CH) from all members of the node, who takes in control to obtain data which send from members of the node. Then sorting data fusion to level-two cluster heads (LII-CHs) which are selected among all non-head nodes who is in charge to forward the packet to the destination node i.e. cluster head responsibilities assigned to the two levels of cluster heads which are greatly reduce the cluster heads energy consumption and improve the survival time of the network. However, the influence factors of energy

consumption in the network and cluster heads distribution is the nodes energy, distance between the nodes to neighbor and the mobility. Among all node in cluster, cluster head should possess with enough energy for achieve send and receive data and transmit data back to the destination node. The nodes energy parameters introduced to make the lower energy nodes cannot attend cluster head election in the next round.

4.3.2 Cluster Heads (L-I & L-II) Election: Cluster heads selection is one of the important procedures in MANET; electing the incorrect CH may lead to an early diminish the network. If an attacker gets a hold of all CHs, then it takes total in-charge over network. To elect the CH, the following factors are considered.

i. Remaining Energy

The remaining energy is computed based on the difference between the initial energy and consumed energy. More generally, all the cluster heads (CHs) must maintain more residual energy when compared with other nodes that exist in the network. Let consider ε_i represents the initial energy of the mobile node. The remaining energy for a node at time t, $\varepsilon(t)$ is computed by,

$$\varepsilon(t) = (N_{TP} * x) + (N_{RP} * y) \quad (2)$$

Where,

N_{TP} =The total number of data packets transmitted

N_{RP} = The total number of data packets received

(x, y) = constants in the range between 0 and 1

ii. Expected Relative Mobility (ERM)

The node's mobility is defined on the basis of movement direction and speed. The relative mobility of the node n_j at instant t is defined by,

$$rm_{i,j}^{t} = \sqrt[2]{(v_i^t)^2 + (v_j^t)^2 - [2v_i^t v_j^t cos(\theta_i^t - \theta_j^t)]} \quad (3)$$

Where,

v_j^t = defines the node (n_j) speed

θ_j^t = defines the movement direction of the node (n_j)

Most commonly, the relative mobility is varied in different epochs. Thus, this would not identify the appropriate mobility parameter of the node. In node mobility, the expected relative mobility (ERM) is computed over different epochs. The ERM between two mobile nodes n_i and n_j by,

$$ERM_{(i,j)}^{T} = \frac{1}{k} \sum_{t=1}^{k} rm_{(i,j)}^{t} \quad (4)$$

Where, t denotes the time and K refers to the number of epochs. Therefore the node expected relative mobility policies are as follows

1) $ERM_{(i,j)}^{T} > 0$ means node move away from each other (high node energy consumption)
2) $ERM_{(i,j)}^{T} < 0$ means node move closer to each other (less node energy consumption)
3) $ERM_{(i,j)}^{T} = 0$ means nodes are stationary (average node energy consumption)

iii. Distance

Let the coordinates of $n_1$and n_2 be the$(x_1 - x_2)$, $(y_1 - y_2)$ and $(z_1 - z_2)$ respectively. The distance between two mobile nodes n_1 and n_2 for the packets transmission is computed as follows,

$$D_m = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2} \quad (5)$$

4.3.3 Threshold Computation: Normal distribution of cluster node position will increase the cluster head nodes in the high dense region. When the node density exceeds the average network density of 50%, node density is considered densely populated area and it will increase the node probability becomes cluster head. The remaining energy $\varepsilon(t)$, Expected Relative Mobility (ERM) and distance (D_m) are combined together to compute the fitness for the node. Therefore the LI cluster head election threshold computed by,

$$T_{L-I}^{n} = T^{n} \times \left[\alpha_1 \frac{N \times \varepsilon(t)_n}{\sum_{i=1}^{N} \varepsilon_i(t)_n} + \alpha_2 \frac{N \times ERM^T}{\sum_{i=1}^{N} ERM^T} + \alpha_3 \frac{N \times D_m}{\sum_{i=1}^{N} D_m}\right] \quad (6)$$

Where $\varepsilon(t)_n$the residual energy of the node is n is, $\sum_{i=1}^{N} \varepsilon_i(t)_n$ is the sum of the node residual energy. Here α_1, α_2, α_3 are random integers such that,

$$\alpha_1 + \alpha_2 + \alpha_3 = 1$$

The level-two (L-II) cluster head forward data fusion to the destination node which gathers from level-one cluster head. Therefore, the distance from node to destination should be preferred as well as consideration of the nodes around node mobility. In this way, it can reduce the network energy consumption. Thus the rewritten threshold formula can be follows:

$$T_{L-II}^{n} = T^{n} \times \left[\beta_1 \frac{N \times ERM^T}{\sum_{i=1}^{N} ERM^T} + \beta_2 \frac{N \times D_m}{\sum_{i=1}^{N} D_m}\right] \quad (7)$$

where β_1, $\beta_2$is weighting coefficient which satisfy

$$\beta_1 + \beta_2 = 1$$

To conclude that if node moves away from each other, then there will be a high chance of link modification or failure with their neighbor nodes. If node moves away from each other, the distance value of node will be higher. Hence, node will consume more energy that will result in poor quality of service so that value of fitness value must be high. Following policies are considered in this research:

i. When node mobility, distance and energy is high, then the value of fitness must be low
ii. When node mobility, distance, and energy is low, then the value of fitness must be high
iii. When node mobility, distance, and energy is medium, then the value of fitness must be medium

It is clear that a node which is less mobility, depleted less energy and less distance from neighbour is a best candidate to become a Level-I CH.

After the selection of L-I, L-II CHs have been selected; the source node broadcasts a message that contains all CHs ID. IF a node's CH ID matches its own ID, the node becomes a CH. Then, each CH broadcasts a hello message over the coverage area. Each ordinary node determines its cluster and sends a reply message to its CH. The denotation k_{opt} represents the optimal number of clusters i.e. the ideal number of CHs, it is computed by,

$$k_{opt} = \frac{\sqrt{T_{MN}}}{\sqrt{2\pi}} \sqrt{\frac{\varepsilon_{fa}}{\varepsilon_{amp}}} \frac{R}{d\ to\ Neighbor\ nodes} \quad (8)$$

Where, T_{MN} represents the number of mobile nodes, $\varepsilon_{fa}, \varepsilon_{amp}$ represents the energy consumption of amplifying radio and R stands for the length of an edge of the MANET. Therefore, the best radius of clusters R_{opt} to compute it, R_{opt} can be computed by eqn.(8)

$$R_{opt} = \sqrt{\frac{Area}{\pi * k_{opt}}}$$

Where, area denotes the coverage/population area of the network.

Procedure 1 for Dual Cluster Head Election

Input: A number of nodes in Grid based MANET
Output: Clustered MANET

Step 1: Begin
Step 2: for G =1 to n do /*'n' number of grids
Step 3: for MN =1 to m do //'m' number of mobile nodes
// L-I & L-II Cluster Heads Election
Step 4: for all nodes in the grids.
Computes
i. Residual Energy ($\varepsilon(t)$)
ii. Expected Relative Mobility (ERM)
iii. Distance (D_m)
// Find Threshold for LI-CH, LII-CHs
Step 5: Possibility = FindPossibility ($\varepsilon(t)$, ERM, D_m)
Step 6: if (y <$Possibility_{threshold(1)}$) // y = Output Value
$m_G(i)$ *elected as* $LI-CH$ // CH= LI-Cluster Head
else
$m_G(i)$ elected as CM //CM = Cluster Member
Step 7: if (y <$Possibility_{threshold(2)}$) // y = Output Value
$m_G(i)$ *elected as* $LI-CH$ // CH= L-II Cluster Head
else
$m_G(i)$ elected as CM //CM = Cluster Member
Step 8: for all cluster members
Step 9: Send Join_Request to nearest CHs
Step 10: end for
Step 11: end for
Step 12: end for
Step 13: end
Step 14: exit

4.4. Energy Efficient and Secure Routing using T2FLS & PSO

In this paper, the path is elected based on Type-2 Fuzzy Logic System. The difference between Type-1 and Type-2 model is that the Type-2 model is more accurate to handle the uncertainty. Many research results are available based on the multipath routing. As of now, there is a lack of research result with optimal path routing. The optimal path can be determined by PSO algorithm.

4.4.1. T2FLS for Multipath Selection

A type-2 fuzzy inference system includes four components:

- Fuzzifier: It translates inputs or crisp values to fuzzified values
- Type-2 Inference System: It combines the "IF-THEN" rules and provides an output of Type-2 fuzzy sets from an fuzzifier i.e. by crisp inputs
- Knowledge Base: It comprised set of fuzzy rules and membership functions
- Type Reducer/Defuzzifier: Type reducer is generates Type-1 fuzzy set, then which is converted by the defuzzifier to a numeric output

The Type-2FLS "IF-THEN" rules are characterized by "IF" and "THEN" statements in which consequent or antecedent sets are of type-2. The structure of the rules is defined by,

Rule l: IF x_1 is F_1 and x_2 is F_2 and …. x_n is F_p THEN y is G

There are 81 rules in our rule base the l^{th} rule has the above form, where $G = \{l = 1, \dots, 81\}$ are all considered to be "LOW", "HIGH" and "MEDIUM". To the best of our knowledge, the domains of four inputs and one output are all taken to be the unit interval [0, 1]. The input values of the fuzzifier are the remaining energy ($\varepsilon(t)$), the distance to the neighbor (D_m), expected relative mobility (ERM) and path length or hop count, respectively. In order to reduce the computational complexity, we divide all four inputs in to three levels that are the Low, High and Medium. All secondary membership functions (SMFs) are taken to be interval sets i.e. the proposed FLS are taken to be interval sets and the primary membership functions (PMFs) are triangular. Besides that the same membership functions for the four inputs.

TABLE II. FUZZY RULES

Rules	Input Variables				Output
	$\varepsilon(t)$	D_m	ERM	PL/HC	
1	High	High	Low	Low	Medium
2	High	High	High	High	Low
3	High	Medium	Medium	Medium	Medium
4	High	Low	Low	Low	High
5	High	Medium	High	Medium	Low
6	Medium	Low	Medium	Low	Medium
7	Medium	Low	Low	Low	Medium
8	Medium	High	High	High	High
9	Medium	Medium	Medium	High	Medium
10	Low	Low	Low	Medium	Medium
11	Low	High	High	Medium	Low
…	…	…	…	…	…
81	Low	Low	Low	Low	Medium

4.4.2. PSO for Optimal Path Selection:

The optimal path is defined as the determination of path with satisfies the routing policies. As previously said, it is difficult to find the optimal path among all the available paths. In order to avoid these conflicts while finding the reliable path, various optimization algorithms have proposed [26-27]. However, these cannot find out the global optimal solution. Thus the PSO algorithm is adopted in order to find

the reliability based global optimal path in this paper. The PSO algorithm is one of the evolutionary computing algorithms which work on the basis of Bird Flocking. A set of potential solutions in PSO are called particles that are randomly initialized. In PSO, each particle will have fitness value, which is evaluated through the optimized fitness function during each generation. Each particle identifies its best position P_{ID} and the global best position P_{GD} amid the whole part of the particles. Each particle will have velocities which direct the flying of the particle. At each generation, the velocity and the particle position will be updated. The position and the velocity update equations are given below.

$$V_{ID}(t+1) = \omega V_{ID}(t) + F_1\mu\left(P_{ID} - X_{ID}(t)\right) + F_2\tau\left(P_{GD} - X_{GD}(t)\right)$$

$$X_{ID}(t+1) = X_{ID}(t) + V_{ID}(t+1)$$

Where X is the particle position, V is the particle velocity, t is the time and ω is the inertia weight. μ and τ are random numbers between 0 and 1. F_1 and $F_2$are learning factors, P_{ID} is the particle's best position, and P_{GD} is the global best position. The major issue on using PSO is the determination of fitness function. Fitness function is closely related with the features of problem domain and it directly determines the performance of the optimal solution of the algorithm.

- *Update swarm:* The fitness function determine again and enhance the e^{pid} and e^{gid} qualities. On the off chance that the new measure is superior to anything, remove the old one by the current one. In addition, select the most optimal P_{ID} and P_{GD}
- *Condition to terminate:* Do until the generated solution is indeed suitable or most extreme steps are accomplished

PSO is proposed to extend or decreased the target perform and thereby considering the value of throughput, packet loss ratio and delay among multiple selected paths in every cycle. This paper going to define complete ways ranging from an origin (source node) to final (Destination) referred as the particles.

4.4.2.1 The Definition of Path Reliability Factors

In this section, various path reliability factors are computed for the number of available routing paths. Let assume that the proposed MANET environment have "N" number of shortest and energy efficient paths from source to the destination node. The optimal path is selected and it must possess maximum throughput, minimum packet loss ratio and minimum delay. Therefore, three factors are evaluated which are as follows:

A. Throughput: It is defined as the quantity of data packets being received or sent well from all cluster heads per unit of time. Thus the throughput x_i can be obtained as:

$$x_i = \sum_{i=0}^{n} n[D_{d^n d^{n-1}}(p)] \times \rho_d^n \quad (9)$$

where n is the number of mobile nodes connected to the destination node, ρ_d^n is the probability transmission of cluster head with the path ρ to the destination node

B. Packet Loss Ratio (PLR): It is computed by the number of packets lost per 100 of packets sent by node. It can be calculated by,

$$y_i = \frac{\frac{S_i(T)}{D_i(T)+S_i(T)}}{S_i(T-1)/D_i(T-1)+S_i(T-1)} \quad (10)$$

where $S_i(T)$ is the total number of packets transmitted in time T and $D_i(T)$ is the number of dropped packets at time T.

C. *Node Delay:* It is defined by the time duration which need for packet transmission over the network. It is calculated by,

$$z_i = \sum_{i=0}^{n} n_i \times T^{n_i} \quad (11)$$

where T^{n_i} represents the transmission time between the cluster heads to the destination node.

Based on the parameters mentioned above, the path reliability fitness value is computed by integrating the three parameters and thereby, the fitness value is computed by,

$$f(i) = x_i\,\alpha + y_i\,\beta + z_i\gamma \quad (12)$$

Therefore the fitness function $f(i)$can be computed using the result of throughput, packet loss ratio and node delay within the clusters. According to the fitness function defined above choose the path with the maximum value of $f(i)$ as an optimal path and it is the optimum result.

Procedure 2 for Particle Swarm Optimization

Step 1: Begin
Step 2: Generate random population R of P paths where $i \rightarrow$ particles
Step 3: For each individual i calculate fitness for P(i)
Step 4: Sort the paths P in descending order of their fitness
Step 5: Divide P into N paths
Step 6: For each path, find the best path and worst value path
Step 7: Improve the worst path by combine with the best path
Step 8: Repeat for certain iterations
Step 9: Again sort the paths P in descending order of their fitness
Step 10: Repeat step 5, otherwise eliminate the worst path

4.4. Certificateless Routing

The proposed framework contains of two elements namely source node and destination node. Three phases are presented in this framework using Elliptical Curves Cryptography as follows:

1: Key generation
2: Signencryption
3: Signdecryption

4.4.1 Key Generation

In key generation process, the authentication and encryption are important while message transmission in the network. Initially, the trusted authority generates and publishes all the public parameter of elliptic curves as well as each mobile node chooses his own private key and computes his related public key. The trusted authority

generates a prime number and then it sets two integer elements to satisfy the elliptic curve condition follows

$$4a^3 + 27b^2 \neq 0 \; mod \; p \;\; \text{when (a,b) < p} \qquad (13)$$

If the condition is satisfied, the elliptical curve is defined to satisfy the relation that follows

$$y^2 = x^3 + ax + b \bmod p \qquad (14)$$

The base point is then set of wireless links that are connecting the mobile nodes n_i to finite field $\mathbb{F}$. As a final point, the hash function is written using the condition

$$H_f : \{0,1\}^* \rightarrow \mathbb{z}_{\mathbb{p}} \qquad (15)$$

Then the parameters are published. In key generation process, trusted authority generates the parameter based on the procedure 3 for elliptical curve cryptography

Procedure 3 for Elliptic Curve

Step 1: $\boldsymbol{p}$ is a prime number
Step 2: Initialize the $(\boldsymbol{a}, \boldsymbol{b})$ two integer element and $(\boldsymbol{a}, \boldsymbol{b})$ < p that satisfies $\boldsymbol{4a^3 + 27\,b^2}$
Step 3: Elliptical curve defined over finite field $\mathbb{F}$ with "$\boldsymbol{n}$" order which satisfy equation $\boldsymbol{y^2 = x^3 + ax + b}$ mod p
Step 4: Set the base point $\boldsymbol{n_i}$ of $\mathbb{F}$
Step 5: Find the hash function $\boldsymbol{H_f}$: $\{\boldsymbol{0,1}\}^* \rightarrow \mathbb{z}_{\mathbb{p}}$
Step 6: TA distributes parameters
$\boldsymbol{TA} = \{\boldsymbol{p, H_f, n_i\, a, b, n}\}$
Step 7: $\{(\boldsymbol{Pu_k, Pi_k}) \rightarrow \boldsymbol{Source_{node}}\} \mapsto \boldsymbol{TA}$
$\boldsymbol{Pi_k}$: $\boldsymbol{X_L} \in [1, 2, \ldots(n-)]$
$\boldsymbol{Pu_k}$: $\boldsymbol{Y_L} = \boldsymbol{X_L n_i} = (\boldsymbol{Y_{L1}, Y_{L2}})$
Step 8: Computes $\{(\boldsymbol{Pu_k, Pi_k}) \rightarrow \boldsymbol{Destination_{node}}\}$
$\boldsymbol{Pi_k}$: $\boldsymbol{X_N} \in [1, 2, \ldots(n-1)]$
$\boldsymbol{Pu_k}$: $\boldsymbol{Y_N} = \boldsymbol{X_N n_i} = (\boldsymbol{Y_{N1}, Y_{N2}})$

Subsequently, public key $(\boldsymbol{Pu_k})$ and private key $(\boldsymbol{Pi_k})$ by trusted authority $\boldsymbol{TA}$ and then calculates public key and private key of destination node.

4.4.2 Signencryption

Signencryption is a cryptographic primitive approach which attains confidentiality and integrity through single logical step. Signencryption uses only one step rather than the signature then encryption approach since it needs two steps for integrity and confidentiality and thereby signencryption reduces the communication cost as well as minimizes the efficiency. The signencryption process is described in Procedure 4.

Procedure 4 for Signencryption

Step 1: Choose the random integer $\boldsymbol{v} \in \{\boldsymbol{1, n-1}\}$
Step 2: Find $\boldsymbol{S_K}$ from the TA $\mapsto$ t. $\boldsymbol{Y_L} \equiv (\boldsymbol{k_1, k_2})$
Step 3: Compute the session key for encryption as $\mathbb{p} = \boldsymbol{H_f}\,(\boldsymbol{x_{\mathbb{p}}} || \boldsymbol{Source\ node_{ID}} || \boldsymbol{y_{\mathbb{p}}} || \boldsymbol{Destination\ node_{ID}}$
Step 4: Calculate the cipher text $\boldsymbol{C_t} \leftarrow \boldsymbol{e_{k_1}(N)}$
Step 5: Find the master key $\boldsymbol{M_k} \leftarrow \boldsymbol{H_f(N, k_2)}$
Step 6: Calculate the digital signature $\boldsymbol{DS} = (\boldsymbol{t - MX_L})$ mod n
Step 7: Forward the signcrypted text $\boldsymbol{\delta(T)} \rightarrow (\boldsymbol{C_t}, \boldsymbol{M_k}, \boldsymbol{DS})$

The procedure 4 description: Firstly, choose the random integer between [1-(n-1)]. Next, determine the secret key from the trusted authority and generate the session key for encryption as $\mathbb{p}$ by taking source node identifier, destination node identifier. The cipher text $(\boldsymbol{C_t})$ is computed for forwarding to the destination node. Subsequently, the master key $(\boldsymbol{M_k})$ is determined. After the computation of master key, the digital signature $(\boldsymbol{DS})$ is computed. Finally the signcrypted text is forwarded

4.4.3 Signdecryption

The destination node obtains the signcrypted text from the source node and decrypts the text to extract plain text and verify the source node digital signature

Procedure 5 for Signdecryption

Step 1: Calculates the session key using $\boldsymbol{M_k, DS}$
$\boldsymbol{k'} = \boldsymbol{DS}.\boldsymbol{Y_N} + \boldsymbol{M_k}.\boldsymbol{X_L}.\boldsymbol{Y_M} = (\boldsymbol{k_1'}, \boldsymbol{k_2'})$
Step 2: Get the message from signcrypted text as follows
$\boldsymbol{N'} \rightarrow \boldsymbol{D_{k_1'}(C_t)}$
Step 3: Verifies $\boldsymbol{Source\ node_{ID}}$ authenticity based on the following equation
$\boldsymbol{M_k}' = \boldsymbol{H_f(N', k_2')}$

The procedure 5 description: Firstly, the session key is computed using digital signature and master key. Then, decrypt the message well from signcrypted text and finally verifies the authenticity based on the source node identifier.

4.6. False Data Attacks Detection & Prevention

False data attacks detection and prevention is a challenging task in wireless network. Typical wireless networks such as mobile ad hoc networks, and wireless sensor networks (WSN) are composed of multiple computing devices with constrained power and energy. In such cases, protecting authenticity and the data integrity from the source to the destination is a critical task since an adversary can inject false data into the network incurring node power consumption, redundant message forwarding, and thereby network performance is degrade. Unlike traditional cryptographic approaches, directly using Message Authentication Codes (MAC), we proposed Elliptic Curve with Digital Signature operations, which build an authentication among nodes. It is called en-route authentication (EA which helps mobile nodes on the routing path to remove or filter out false data in high success rate.

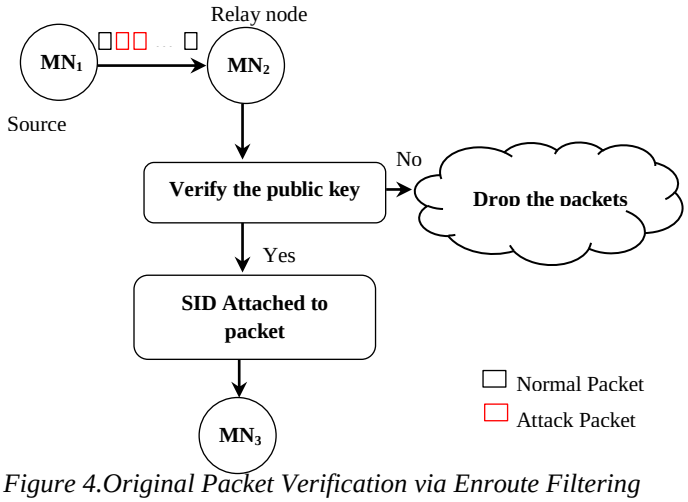

Figure 4.Original Packet Verification via Enroute Filtering

Figure 3 shows the enroute filtering operations while original packet verification. This proposed method can ensure data integrity as relay nodes will not be allowed to read data. Finally, the plain text will be re-encrypted by source private key as a source digital signature preserves the data confidentiality.

V. Experimental Evaluation

In this section, the performance analysis of the proposed technique is carried out in the NS3 simulation environment in consort with the performance metrics for the presented PSO-T2FLS based 3D Grid environment. In section 5.1, the simulation model is presented. In section 5.2, the performance metrics are considered and in section 5.3 the comparison assessment is performed amid PSOPB [15], DE-AODV [24], TECM [23], and FBSA [16]. The simulation values are shown in the following table III.

TABLE III SIMULATION PARAMETERS

Simulation Parameters	Value/Units
Network Size	650 × 500
Number of Nodes	150
Range	200 m
Packets Size	1000 Bytes
Initial Energy of Nodes	100 Joule
Transmission Energy	0.15 Joule
Simulation Time	33.0 Seconds
Energy of Elected Node (CH)	1.0 Joule
Propagation Model	Friis Propagation Loss Model & Constant Speed Propagation Delay Model
Mobility Model	Random Way Point Mobility Model
Speed of Nodes	20 Mbps

. *A. Simulation Model*

The NS-3 (version -3.25) simulator has been used for a study of the performance of the proposed system. In all the simulations, the network contains a fixed number of nodes which are moving in the fixed area. The number of nodes considered for simulation is 150. This paper used Random Waypoint (RWP) mobility model with pause time fixed to 0 second to have an effect on the relative speeds of the mobile nodes. The transmission range is set to 200m with a maximum speed of 20 m/s. The simulation includes 4 packets per second of size of 512 bytes generated.

This paper provides *secure communication in Battlefield Environment*. In battlefield or in border force any number of nodes may join or leave the network and there will be a continuous movement also. These two characteristics significantly reduce obtaining useful knowledge from the network.

B. Performance Metrics

The parameters that have been taken to analyse the network performance are energy consumption, packet delivery ratio, routing overhead rate, throughput, average end-to-end delay, network lifetime, packet loss ratio, and success rate

1). Energy Consumption

Energy consumption is estimated as the product of amount of energy consumed by single mobile node with respect to total number of mobile nodes in MANET. It is computed in terms of Joules (J). It is written as follows,

$$\varepsilon_c = \varepsilon_{MN} + T_{MN} \tag{16}$$

Energy consumption ε_c for routing is computed by product of energy consumed by single mobile node 'ε_{MN}' and total number of mobile nodes 'T_{MN}'

2) Packet Delivery Ratio (PDR)

PDR is measured as the ratio of number of data packets received to the number of data packets sent in MANET. It is estimate in terms of percentage (%) and it is written as below.

$$\text{PDR} = \frac{dp_s}{dp_r} * 100 \tag{17}$$

Where, PDR represents the packet delivery ratio whereas dp_s represents the number of data packets sent and dp_r represents the number of data packets received.

3) Routing Overhead Rate (ROR)

ROR is defined by the time taken to perform load balanced energy efficient path with respect to number of mobile nodes. It is computed in terms of milliseconds. It is formalized by,

$$\text{ROR} = \sum_{i=1}^{n} MN_i * T(MN_i) \tag{18}$$

Where, ROR is measured using mobile nodes MN_i and time for load balanced energy efficient routing respectively. If routing overhead is low, the method is said to be more efficient.

4). Throughput

It is defined as the number of bytes received successful and it is calculated by,

$$\text{Throughput} = \frac{Number\ of\ Bytes\ Received * 8}{Simulation\ Time * 1000} * kbps \tag{19}$$

It is estimated in terms of Kbps.

5). Average End-to-End Delay (AEED)

AEED is defined as the time duration of the data packet to be transmitted successfully across a MANET from source to the destination. It is estimated in terms of milliseconds (ms). It considers all possible delays such as buffering during the route discovery latency, transfer time, the propagation, queuing at the interface and it is computed by,

$$\text{AEED} = \frac{\sum_{i=0}^{n} packets\ received\ time - packet\ sent\ time}{n} \tag{20}$$

where n is the number of data packets transmitted successfully over the MANET, "i" represents the unique packet identifier.

6). Network Lifetime

In mobile ad hoc network, it is necessary to improve the network lifetime, which means to maximize the network survivability or to prolong the nodes battery lifetime. However, the lifetime of a node is effectively identified by its battery life. It is estimated in terms of milliseconds (ms). The major reason, while drainage of battery is due to

receiving and transmitting data among nodes and the processing elements.

7). Packet Loss Ratio (PLR)

Packets loss or corruption of packets indicates that the packets which have been sent by the sender but not received by the destination node. It is the ratio of packets not delivered to the destination node to those forwarded by the sources are computed by,

PLR (%) =

$$\frac{Number\ of\ packets\ sent - number\ of\ packets\ received}{Total\ packets\ sent} * 100 \quad (21)$$

8) Success Rate (SR)

Success rate is defined as the rate of packets that are correctly determined as a false during data transmission in the networks and thereby, rate of malicious activities rate is determined.

C. Comparative Analysis

In this section, the performance of the proposed system is evaluated along with the comparison of previous approaches have made in this section. The following metrics are evaluated to test the effectiveness of the proposed algorithm.

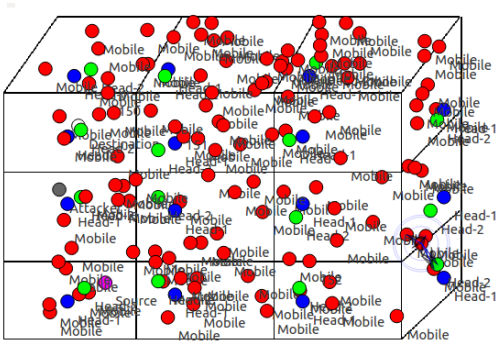

Figure 5.Node Visualization in Simulation

i. Energy consumption

This is defined as the average of energy consumed by all nodes of the network. As seen in figure 6, the proposed uses less energy per node as compared other routing approach.

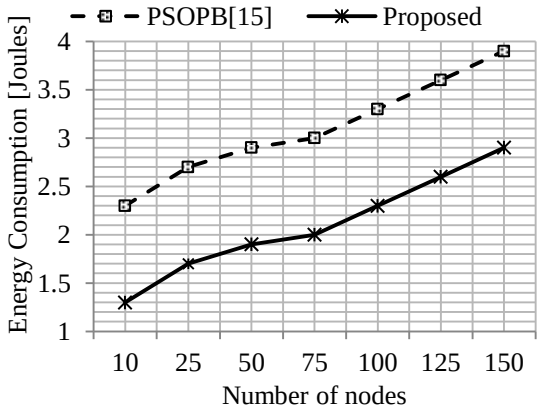

Figure 6.Energy Consumption

Figure 6 shows the performance of the proposed approach when comparison with the existing approach likes PSOPB [15]. From the obtained results, mainly the energy usage of proposed system gets better in contrast to that of existing approaches. The proposed method performs best at each and every point of number of nodes increases. As we increase the density of the node within a network, necessary updates increase and thus the performance degrades, particularly when network mobility is present.

ii. Packet Delivery Ratio:

The performance analysis PDR is demonstrated in figure by varying the number of nodes from 10-150 for a total of 150 nodes on the network.

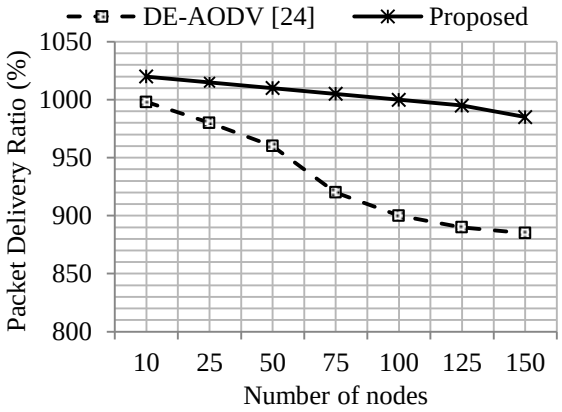

Figure 7.Packet Delivery Ratio

Figure 7 shows the packet delivery ratio performance of the proposed system when compared with the existing approach likes DE-AODV [24]. The performance of PDR is appealing in the proposed system. This is because that the proposed system selects reliable, shorter, stable and optimum path for data transfer. Thus the chances for path breakage due to node failure are very small. The proposed method keeps only one optimal path instead of multipaths based routing because the multipaths causes node failure (increases the packet drop rates). So the selected path is very much reliable and increases the packet delivery rate in battlefield communication

iii. Routing Overhead Rate

Within a network, each and every control messages such as RREQ, broadcasted and received is really known as routing overhead.

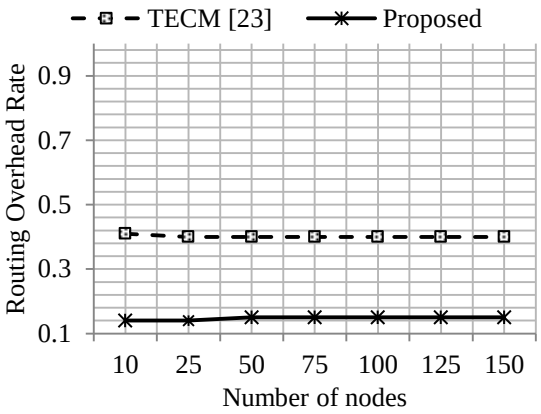

Figure 8.Routing Overhead Rate

Figure 8 illustrates the routing overhead of the proposed approach as well as existing approach (TECM [23]). The plot clearly shows that the proposed battlefield communication based MANET obtains very low overhead than the existing approach. The proposed approach uses

optimal path based on the PSO algorithm. It selects the best path for transmission using path reliability factors such as throughput, packet loss ratio, and delay.

iv. Throughput

It computes the network consistency in providing information to the destination. So the throughput can be defined as the number of packets incoming at the destination node in one millisecond.

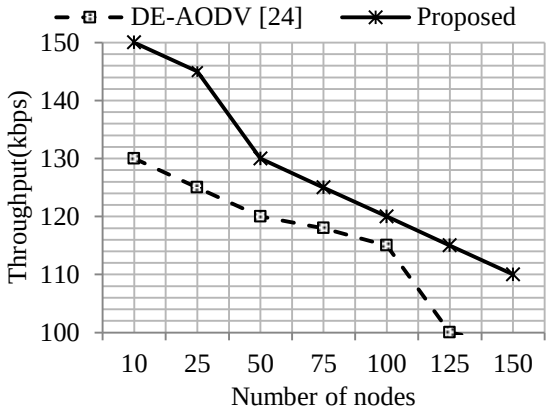

Figure 9.Throughput

Figure 9 shows the throughput performance in comparison with existing approach [DE-AODV [24]). Data throughput of proposed system is higher than the existing approach. The proposed system performs well with the average dense networks till the network size remains within 150 nodes.

v. Average End-to-End Delay

This metric is referred as the delay time taken to receive the data packet and retransmit packet to every node, which is known in terms of end-to-end delay.

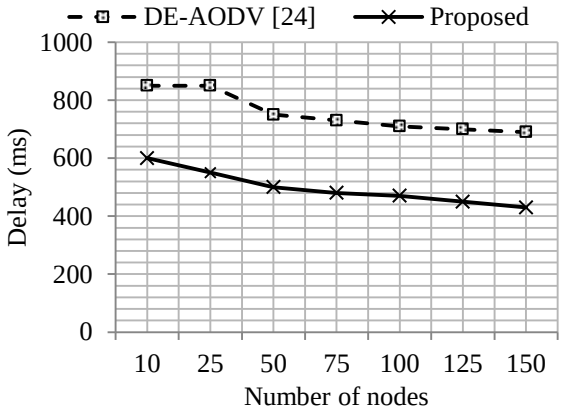

Figure 10.End-to-End Delay

Figure 10 shows the performance of average end-to-end delay for the proposed system when comparison with the existing approaches (DE-AODV [24]). In this paper, the proposed system chooses shortest path for routing. Thus, the proposed system produces better output when compared to the De-AODV approach.

vi. Network Lifetime

The network life time is the fundamental criterion in MANET. When conserving high energy, the network ensures to prolong the lifetime.

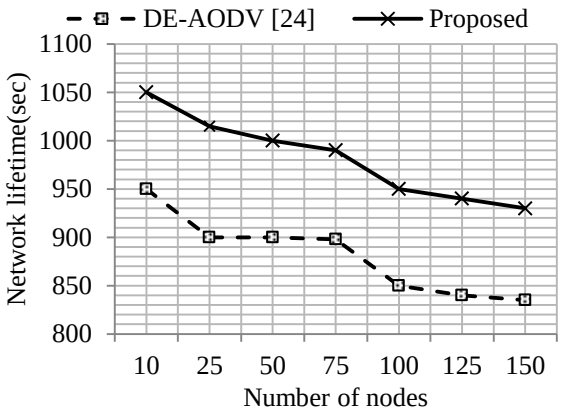

Figure 11.Network Lifetime (sec)

Figure 11 show that the network lifetime performance of proposed system when compared with existing approach likes DE-AODV method. This paper considers dual cluster heads for transmission which produce better results even when number of node increase.

vii. Packet Loss Rate

It affects the perceived quality of the network. Packet loss could be mainly due to unstable wireless links, congestion or overflowing in the network.

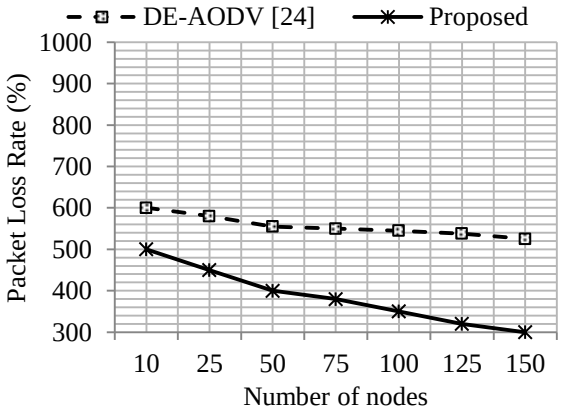

Figure 12.Packet Loss Rate

Figure 12 shows the performance of the proposed system in comparison with the existing approach [DE-AODV [24]] in terms of packet loss. In this paper, the proposed system uses digital signature based cryptographic operations which produce better output than the existing approach. Further, optimal path is selected for packets transmission.

viii. Success Rate

The number of malicious activities is occurred in highly dense networks. It must be evaluated when the mobile users under the highly dense environments.

Figure 13 shows comparison of previous detection approach like FBSA [16] with proposed approach. The proposed approach performs better in term of high success rate since it filter large number of malicious activities in the networks. FBSA weakly detects malicious nodes. The proposed 3D MANET has been gradually increased with success rate for number of nodes. The average success rate (%) for the

proposed approach in battle field communication has 95% and in FBSA, the success rate falls into 90%.

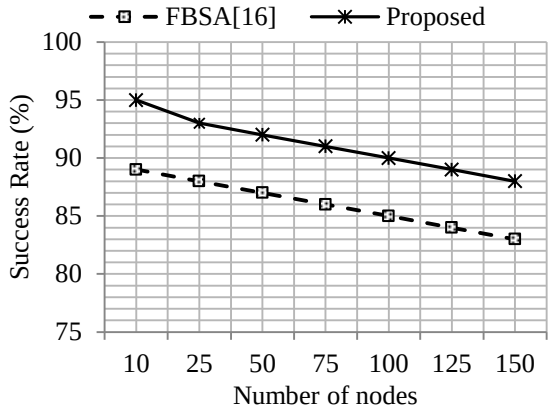

Figure 13.Success Rate

From the results, we conclude that the proposed approach outperforms than the previous approaches. It shows a clear and constant increase in the throughput because of removal of false data injection attacks. The simulated result shows a 25% enhancement over the previous approaches. Our proposed approach is validated in the battlefield communication based MANET where security and reliability is most wanted.

VI. Conclusion and Future work

In mobile ad hoc network, mobile nodes can easily compromised by the internal attackers. Network is often grouped because of the attackers which lead to network unavailability. In transmission, data packets are modified by attackers which intrude upon the security challenges in MANET. The major concerns in MANET are conservation of node energy and prolong the network lifetime. To overwhelm those issues, we proposed clustering scheme. In this research work, dual cluster head is selected which further reduce the energy consumption. To forward data packets, we develop Type-2 Fuzzy Logic System (T2FLS) and Particle Swarm Optimization to attain more efficiency among the mobile nodes in the network. The T2FLS mechanism determines the possible paths. After that, optimal route is selected among multiple paths using PSO. To protect data from attackers, we invoked certificateless key generation and signencryption concepts which improve the node authenticity. Therefore we can prevent the mobile node from false data injected and route attacks. Based on the simulation results, the proposed framework outperforms than the existing schemes in terms of energy consumption, packet delivery ratio, routing overhead rate, throughput, average end-to-end delay, network lifetime. In future, it is decided to select the hybrid crypto method to further achieve the better performance in data encryption and decryption process.

References

[1] G. Venkata Swaroop, G. Murugaboopathi, “Secure and Reliable Communication Scheme for MANET using ECMS Cluster Head based Certificate Revocation”, Springer-Cluster Computing, PP. 1-13, 2017

[2] K.B. Gurumoorthy, A. Nirmal Kumar, “Mutual Constraint based GA Suggested Routing Algorithm for Improving QoS in Clustered in MANETs”, Wireless Personal Communications, PP. 1-17, 2017

[3] V. Bhanumathi, R. Dhanasekaran, “Efficient Data Transfer in Mobile Ad hoc Network using OPSM for Disaster Response Applications”, Journal of Applied Research and Technology, Volume 13, PP. 392-401, 2015

[4] T. Maragatham, S. Karthik, R.M. Bhavadharini, “TCACWCA: Transmission and Collusion Aware Clustering with Enhanced eight Clustering Algorithm for Mobile Ad hoc Networks”, Springer-Cluster Computing, PP. 1-14, 2018

[5] Sumit Kumar, Shabana Mehfuz, “Intelligent Probabilistic Broadcasting in Mobile Ad Hoc Network: A PSO Approach”, Journal of Reliable Intelligent Environments, Volume 2, PP. 107-115, 2016

[6] Chrispen Mafirabadza, Pallavi Khatri, “Efficient Power Aware AODV Routing Protocol”, Springer-Wireless Personal Communications”, PP. 1-11, 2017

[7] Rashmi Chaudhry, Shashikala Tapaswi, Neetesh Kumar, “Forwarding Zone Enabled PSO Routing with Network Lifetime Maximization in MANET”, Applied Intelligence, PP. 1-28, 2018

[8] Houda Moudni, Mohammed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, “Secure Routing Protocols for Mobile Ad Hoc Networks”, IEEE International Conference on Information Technology for Organizations Development (IT4OD), 2016

[9] Babak Emami Abarghouei, Ali Farokhtala, Mojtaba Alizadeh, “DNACK: False Data Detection Based on Negative Acknowledgement and Digital Signature on Mobile Ad Hoc Network”, Springer Wireless Personnel Communications, Volume 83, PP. 1-15, 2015

[10] Naghma Khatoon, Amritanjali, “Mobility Aware Energy Efficient Clustering for MANET: A Bio-Inspired Approach with Particle Swarm Optimization”, Wireless Communications and Mobile Computing, Volume 2017, PP. 1-12

[11] Gunpreet Singh, Neeraj Kumar, Anil Kumar Verma, “OANTALG: An Orientation based Ant Colony Algorithm for Mobile Ad Hoc Networks”, Wireless Personal Communications, PP. 1-26, 2014

[12] P.E. Irin Dorathy, M. Chnadrasekaran, “Distance based Dual Path Ad Hoc On Demand Distance Vector Routing Protocols for Mobile Ad Hoc Networks”, International Conference on Advanced Computing and Communication Systems, Coimbatore, India, 2015

[13] M. Kokilamani, E. Karthikeyan, “An Optimal Path Selection Criterion in Multipath Routing using Energy”, Springer-CSIT, 2017

[14] Chrispen Mafirabadza, Pallavi Khatri, Efficient Power Aware AODV Routing Protocol for MANET”, Wireless Personal Communications, 2017

[15] Sumit kumar, Shabana Mehfuz, “Intelligent Probabilistic Broadcasting in Mobile Ad Hoc Network: A PSO Approach”, Journal of Reliable and Intelligent Environments, Volume 2, PP. 107-15, 2016

[16] Dhananjay Bisen, Sanjeev Sharma, “Fuzzy based Detection of Malicious Activity for Security

Assessment of MANET", National Academic Science Letters, PP. 1-6

[17] Ramireddy Kondaiah, Bachala Sathyanarayana, "Trust Factor and Fuzzy Firefly Integrated Particle Swarm Optimization based Intrusion Detection and Prevention for Secure Routing of MANET", International Journal of Computer Networks and Communications (IJCNC), Volume 10, No. 1, PP. 13-33, 2018

[18] Dhananjay Bisen & Sanjeev Sharma (2017): An enhanced performance through agent-based secure approach for mobile ad hoc networks, International Journal of Electronics, DOI: 10.1080/00207217.2017.1355019

[19] Hrishabha Raj Jain, Sanjay Kumar Sharma, "Improved Energy Efficient Secure Multipath AODV Routing Protocol for MANET", IEEE International Conference on Advances in Engineering and technology Research (ICAETR-2014), 2014

[20] V. Brindha, T.Karthikeyan, P. Manimegalai, "Fuzzy enhanced secure multicast routing for improving authentication in MANET", Cluster computing, 2017

[21] Raghu Vamsi, Krishna Kant, "Generalized Trust Model for Cooperative Routing in MANETs", Wireless Personal Communications, 2017

[22] Srinivas Aluvala, K. Raja Sekhar, Deepika Vodnala, "A Novel technique for Node Authentication in Mobile Ad Hoc Networks", Volume 8, PP. 680-682, 2016

[23] Vallala Sowmya Devi, Nagarathna P Hegde, "Multipath Security Aware Routing Protocol for MANET based on Trust Enhanced Cluster Mechanism for Lossless Multimedia Data Transfer", Wireless Personnel Communications, 2018

[24] J. Deep, J. Sutha, "A New Energy based Power Aware Routing Method for MANETs", Cluster Computing, 2017

[25] N. Saravanan, A. Subramani, P. Balamurugan, "Optimal Route Selection in MANET based on Particle Swarm Optimization Utilizing Expected Transmission Count", Cluster Computing, 2017

[26] Sapna Gambhir, Paul Tomar, "Optimal Path Selection Routing Protocol in MANETs", International Journal of Scientific & Engineering Research Volume 3, Issue 7, 2012

[27] M. Nagaratna, Cheerla Manasa, "Optimized Path Selection on Multicriteria in MANET", International Journal of Advanced Trends in Computer Science and Engineering, Volume 2, Issue 6, PP. 38-41