electronics

Article

A Trust-Based Secure Neuro Fuzzy Clustering Technique for Mobile Ad Hoc Networks

Alagan Ramasamy Rajeswari [1], Wen-Cheng Lai [2,3], C. Kavitha [4,*], Prabhu Kavin Balasubramanian [5,*] and S. R. Srividhya [4]

[1] Department of Computer Science and Engineering, Rohini College of Engineering and Technology, Kanayakumari 629401, Tamil Nadu, India
[2] Bachelor Program in Industrial Projects, National Yunlin University of Science and Technology, Douliu 640301, Taiwan
[3] Department Electronic Engineering, National Yunlin University of Science and Technology, Douliu 640301, Taiwan
[4] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai 600119, Tamil Nadu, India
[5] Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur 603203, Tamil Nadu, India
* Correspondence: kavitha.cse@sathyabama.ac.in (C.K.); prabhukb@srmist.edu.in (P.K.B.)

Abstract: A MANET consists of a group of mobile nodes. In a MANET, scalability and mobility have a greater influence on routing performance. The clustering technique plays a vital role in enhancing the routing mechanism and improving the network lifetime of a large-scale network like a MANET. The clustering process will degrade network performance if the malicious node is chosen as the Cluster Leader (CL). Thus, the secure clustering process in a MANET is a very challenging task. To overcome this problem, the following key factors like Trust Value (TV), Residual Energy Level (REL), and Mobility (M) of the node are used as decision-making parameters to elect a Cluster Leader (CL). In this work, we have proposed a soft computing-based neuro-fuzzy model, ANFIS-based Energy-Efficient Secure Clustering Model (ANFIS-EESC), with a primary objective of forming energy-aware stable trust-based clustering in a MANET. Moreover, we have proposed two working novel algorithms: Weight-Based Trust Estimation (WBTE) algorithm and the Fuzzy-Based Clustering (FBC) algorithm. The primary objective of the WBTE algorithm is to measure the trustworthiness of the nodes and to mitigate the malicious nodes. Fuzzy-Based Clustering (FBC) algorithm is a fuzzy logic-based cluster formation algorithm. In our proposed work, each non-CL in the system applies the cluster density of CL and mobility for each CL node using the Mamdani Fuzzy Inference system, and makes the decision to join as a member with a CL that holds maximum value. Simulation results show that the proposed work enhances the network performance by electing a more stable trust-aware and energy-aware node as Cluster leader (CL). We compare the performance parameters of the proposed work, such as packet delivery rate, energy consumption, detection rate, and reaffiliation, with the existing work, Weighted Clustering Algorithm (WCA). The network lifetime is 39% greater in the proposed ANFIS-EESC model than in the other existing work, WCA. Moreover, ANFIS-EESC shows an enhancement of 22% to 32% in packet delivery ratio and 32% and 39% in throughput. From the above analysis, it has been proved that the proposed work gives a better performance in terms of reliability and stability when compared to the existing work, WCA.

Keywords: MANETs; clustering; cluster leader; security; trust; residual energy level; mobility; ANFIS; fuzzy logic

Citation: Rajeswari, A.R.; Lai, W.-C.; Kavitha, C.; Balasubramanian, P.K.; Srividhya, S.R. A Trust-Based Secure Neuro Fuzzy Clustering Technique for Mobile Ad Hoc Networks. *Electronics* **2023**, *12*, 274. https://doi.org/10.3390/electronics12020274

Academic Editors: Danilo Pelusi, Rajesh Kumar Dhanaraj and Christos J. Bouras

Received: 21 November 2022
Revised: 25 December 2022
Accepted: 1 January 2023
Published: 5 January 2023

1. Introduction

MANETs (Mobile Ad Hoc Networks) have a wide range of advantages due to their user-friendly characteristics and were developed in 1997 for military applications. The two main issues in MANET applications are energy and security. The nodes in MANET communicate with each other using radio waves. The nodes will forward the packets across the infrastructure-less network. Thus, the nodes will act as both host and router. Moreover, each node carries out the following activities, such as packet delivery, topology identification, and determination [1].

A MANET is a network consisting of a collection of mobile nodes capable of communicating via wireless links. All nodes in the network are randomly movable over different time periods.

MANETs has been used in various applications due to its self-configured characteristics [2,3]. In the past, more research works were carried out on the characteristics, features, and architecture of MANETs, but in recent years, enhancing secure data transmission has been considered a major security challenge and research area. A MANET is configured as an independent, self-functioning, and multi-hop network [4]. As a result of the wireless and distributed nature of the system, designers are challenged to ensure its security. In recent years, MANET security issues have been a complex threat, and intrusion detection mechanisms have been developed in response. As a result, researchers have focused on specific security areas, such as intrusion detection, trust infrastructure, and routing protocols. The uncertainty and dynamic nature of the MANET environment may lead to frequent changes in topology and resources. Thus, the trust-based clustering mechanism plays a vital role in enhancing secure routing in a MANET. Small groups, namely clusters, are formed by dividing the nodes, and one among the nodes in the cluster is chosen as a Cluster Leader.

The Cluster Leader (CL) is responsible for coordinating and controlling all other nodes within the cluster. In a MANET, the mechanism of clustering has the following advantages, namely:

1. The network scalability and routing performance are improved.
2. Routing control overhead is decreased. Thus, energy consumption is minimised.

Cluster Leader (CL) election in a MANET is a major and important task. CL will be more vulnerable to various attacks by misbehaving nodes. The selfish nodes and malicious nodes are two classes of misbehaving nodes. Due to the energy constraint, the selfish nodes will purposefully drop packets, while the malicious nodes will perform black hole attacks and grey hole attacks. In this way, if a malicious node is elected as a CL, network performance will deteriorate, resulting in a shorter network lifetime. It is, therefore, crucial to elect a trustworthy node as CL during the CL election process. The topology may be subject to rapid changes in a dynamic network due to the nodes' dynamic nature. Due to the open nature of the MANET, the provision of security is a major challenging issue. Moreover, the best cryptographically secure solution for a MANET, namely an IBC-based routing protocol [5], has been described. However, the cryptographic-based work is time-consuming. Thus, the trust-based security management system provides a solution to overcome the security issues in MANET. In this proposed work, the decision-making parameters, namely Trust Value (TV), Residual Energy (RE), and Mobility (M) of the node, are considered to elect a CL. The Trust Value (TV) is chosen as a parameter to elect a more secure and trusted node as a CL, while Mobility is considered in the CL selection process to select a more stable node as a CL, which will enhance the stability of the cluster. In this work, ANFIS-Based clustering is proposed. By using the fuzzy logic rule, CL can be elected more accurately. In a Fuzzy Inference System (FIS), uncertain data are given as input to generate more flexible and cost-efficient solutions.

A neural network acts as a solution to most complex issues in the event of making an exact decision in case of uncertain conditions.

The following are significant contributions made by this paper:

- A novel method is proposed to elect a stable, energy-aware, and trust-aware node as a Cluster Leader (CL) by considering the following decision-making parameters: TV, RE, and Mobility of nodes.
- The objective of the new Weight-Based Trust Estimation (WBTE) is to measure the trustworthiness of each network node.

The rest of the paper follows after these points. A survey of related works is presented in Section 2. The details of our proposed work are explained in Section 3. Section 3.2 describes the proposed ANFIS-Based Energy Efficient Secure Clustering Model. Section 3.2.1 explains in detail about the design of the Weight-Based Trust Estimation (WBTE) algorithm. Section 3.2.2 explains in detail about the design of Fuzzy-Based Clustering. The fuzzy rules used in this proposed model are explained. We present the simulation results in Section 4. A conclusion is provided in Section 5.

2. Related Works

This section describes in detail the various research works carried out in areas such as clustering, fuzzy-based clustering, trust-based routing, and energy-aware routing protocols. Many researchers have proposed numerous cluster-based routing algorithms [6–10]. In [11], a trust-based model is developed to rectify and address the collision problem on the receiver side.

A recommendation-based model for trust management is proposed [12]. In this model, issues related to dishonest recommendations are discussed. A cluster-based filtering technique is proposed to remove dishonest recommendations. In [13], the need for competence in selecting a trustworthy node as a head is explained. In this proposed work, a VCG-based mechanism is employed to make the nodes participate frequently in the head election procedure, and incentives are assigned to the trustworthy node. It is possible to eliminate a malicious node with FAP trust [14].

There are multiple factors that determine a node's trust. Fuzzy Analytic Hierarchy theory assigns weights to decision factors based on entropy. The semi-ring theory is used in [15] as a basis for a trust model. Direct observation and recommendation contribute to estimating a node's trustworthiness. Reference [16] presents Cluster-Based Routing Protocol (CBRP) for dividing nodes into clusters, where clusters can be disjoint or overlapped. Using a Cluster-Based Trust Aware Routing Protocol (CBTRP), packets are protected from intermediary malicious nodes [17]. Compared to existing work, this protocol performs better at identifying malicious nodes. A node's trustworthiness is determined by observing the beliefs, disbeliefs, and uncertainties of its neighbours. There are numerous studies on wireless and sensor networks in the literature [18–22]. Additionally, trust management schemes for the internet of things [23] and traffic management and service configuration [24] are being investigated in wireless networks.

Every node uses the Mamdani fuzzy logic system (FLS) to determine the probability of forwarding its Route Requests (RREQs) during the DFES-AODV [25] route discovery phase. The soft computing algorithm developed in [26] was designed to counter sleep deprivation attacks. ANFIS detects normal and abnormal activities in MANETs using subtractive clustering. Using a neuro-fuzzy classifier, MANET activity is detected. A fuzzy logic algorithm is proposed in (CHEF) [27] for the election of cluster heads.

A CL is selected in CHEF using two parameters, proximity distance and energy. Fuzzy logic has been used in the selection of cluster heads. Nodes with high energy and locality are given the opportunity to be cluster heads in CHEF. CHEF has been enhanced with F-MCHEL [28]. In order to elect the cluster head, fuzzy rules were applied based on proximity distance and energy level.

The node with the highest residual energy level among the cluster head is selected as a Master Cluster Head (MCH). The role of MCH is to transmit the aggregate data to the static base station. Their mechanism enhances the network stability when compared with CHEF. In [29], authors have proposed fuzzy-based unequal clustering. In [30], a novel Secondary Cluster Head (SCH) election algorithm is proposed by considering parameters such as

a node's mobility and the distance between nodes and the base station. Using the circle criterion, Reference [31] analyses the stability of Takagi–Sugeno fuzzy control systems.

On the basis of a multi-dimensional fuzzy and Markov SCGM (1, 1) model, a model [32] is proposed for estimating the level of trust in a MANET node. In [33], a fuzzy logic that modified the AODV routing protocol to enhance the reliability of MANETs was developed. FMAR evaluates the routes by considering fuzzy logic weighted multi-criteria. The main drawback of FMAR is that it does not evaluate the stability of all routes. Fault tolerance is very low with FMAR. A trust-based secure routing mechanism in support of OLSR [34] is proposed and implemented. In their work, the trust level of a node is estimated by both the firsthand and secondhand recommendation methods. In [35], the density Viewpoint-based Weighted Kernel Fuzzy Clustering (VWKFC) algorithm is proposed. VWKFC makes the selection of initialized cluster centers and viewpoints more reasonable, obtains better clustering results, and achieves higher convergence speed.

In [36], fuzzy C-Means clustering with interval knowledge granules (IKG-FCM) and triangular knowledge granules (TKG-FCM) is proposed. Experiments on synthetic and real-world datasets demonstrate that IKG-FCM and TKG-FCM consistently achieve better clustering performance with less of a time cost, especially on imbalanced data, compared with state-of-the-art algorithms.

In spite of the availability of such related works, security-based clustering and routing techniques in MANET remain major challenges to achieve. Most of the related works focus in electing the energy-aware node as a cluster leader. However, in ad hoc architecture like a MANET, security-based routing is considered a major issue and needs to be addressed. Hence, in a MANET, there is a need for energy-efficient and secure-based clustering techniques to improve network performance and reliability.

3. Proposed Work

A secure and energy-aware clustering (ANFIS-EESC) model is developed in this proposed method. This model comprises two novel algorithms, namely the Weight-Based Trust Estimation (WBTE) algorithm and the Fuzzy-Based Clustering (FBC) algorithm. The primary objective of the WBTE algorithm is to measure the trustworthiness of the nodes and to mitigate the malicious nodes. Fuzzy-Based Clustering (FBC) algorithm is a fuzzy logic-based cluster formation algorithm.

The primary objective of this proposed work is to improve the network performance by electing a more stable and trustworthy node as CL. Thus, in our work, we have considered the following parameters—Mobility (M), Trust Value (TV), and Residual Energy Level (REL)—as metrics in the CL election process. Therefore, we have used ANFIS-based modeling in our work for choosing the CL among the available nodes in the network. Thus, three inputs to the proposed model are M, TV, and REL and the output from the model is either 0 or 1, where 0 indicates the possibility of the node acting as a CL, and 1 indicates that the node cannot act as a CL.

3.1. Cluster Formation

In this work, an energy-efficient and secure clustering mechanism is carried out with the objective of enhancing the network performance. The Cluster Leader (CL) is elected by considering the following four parameters: Mobility, Residual Energy Level, Cluster Density, and Trust Value of nodes. Once the clusters are formed, the Fuzzy Inference System (FIS)-based clustering process is adopted by the member nodes in electing the suitable trustworthy CL. The proposed work has four inputs, 27 rules, and one output. In the following section, we have discussed the fuzzy input parameters in detail.

3.1.1. Mobility

In a MANET, where the nodes are dynamic in nature, cluster members and cluster leaders will be moving in and out of the transmission range. To enhance the stability of the cluster, a node with low mobility is elected as the Cluster Leader (CL). Frequent re-election

of a cluster leader will be reduced if a more stable node is chosen as a CL for a cluster. The primary objective of electing a suitable, efficient CL is to enhance the network lifetime. The relative mobility, $M_X^{rel}(Y)$, at node X with respect to node Y is measured using Equations (1) and (2) (Basu et al.) [37].

$$M_X^{rel}Y = 10log_{10}\frac{RP_{Y\to X}^{new}}{RP_{Y\to X}^{old}} \tag{1}$$

For node X, there will be 'N' number of one-hop neighbours, then M_X is estimated using the relative mobility metric $M_X^{rel}(Y)$, where Y is a neighbour of X. The node with lower relative mobility (M_X) will be elected as a cluster leader.

$$M_X = var_0\left\{M_X^{rel}(j)\right\}_{j=1}^{N} \tag{2}$$

where var_0 indicates the variance with respect to zero.

3.1.2. Residual Energy Level

In this proposed work, an energy-efficient clustering process is carried out with the aim of improving the network lifetime. Hence, a node's energy level is considered one of the major parameters in the clustering process. For any node 'n' to act as CL, REL should be more than the threshold energy shown by Equation (3). Thus, the estimated REL plays a vital role in the cluster formation process.

$$\mathrm{REL(n)} > \mathrm{E_{thres}} \tag{3}$$

where

REL(n) is the Residual Energy Level of the node n.

$\mathrm{E_{thres}}$ is the threshold energy.

The threshold energy ($\mathrm{E_{thres}}$) is measured using Equation (4).

$$E_{thres} = \frac{\sum_{i=1}^{N}\mathrm{N_{REL}}}{\mathrm{N_{Network}}} \tag{4}$$

where

$\mathrm{N_{REL}}$ is the Residual Energy Level and

$\mathrm{N_{Network}}$ is the number of nodes in the network.

3.1.3. Cluster Density

Cluster density is defined as the maximum number of nodes grouped to form a cluster at a given instance of time.

In a dynamic environment like a MANET, where the nodes often move in and out from the transmission range of the cluster leader, it becomes highly complicated to establish and maintain a perfect cluster density balanced system. Thus, in this proposed work, we have used the Density Balancing Factor (DBF) to estimate the density of the cluster leader. The estimation of DBF (Damla et al.) [38] is given in Equation (5) as follows:

$$DBF = \frac{N}{\sum_i (x_i - \mu)^2} \tag{5}$$

DBF is the Density Balancing Factor.

N is the number of Cluster Leaders.

x_i is the cardinality of the node i.

$$\mu = \frac{(N - n_c)}{n_c}$$

μ is the variance.

n_c is the cardinality of cluster C.

This work considers a MANET environment in which nodes are featured with the capacity to move with different mobility in a different direction. The input to FIS is the Residual Energy Level, Trust Value, and Mobility. Thus, three parameters are computed periodically for every node.

3.2. ANFIS-Based, Energy-Efficient Secure Clustering Model

ANFIS is defined as an integrated system of both Artificial Neural Networks (ANN) and FIS. Thus, ANFIS includes the learning capabilities of neural networks and the reasoning capabilities of FIS. In this work, an ANFIS model is proposed using the first-order TS and consists of three inputs, four rules, and one output. The model consists of three inputs, namely REL, TV, and Mobility, and a single output denoted as Chance, defined as the possibility of the node being elected as CL or not. REL, TV, and Mobility are non-linear input parameters. The notations REL_{less}, REL_{more} for Residual Energy Level, TV_{less}, TV_{more} for Trust Value, and M_{less}, M_{more} for Mobility denote the linguistic values.

The proposed ANFIS-based, Energy-Efficient Secure Clustering Model (ANFIS-EESC) is a multilayer structure with five layers, labeled as Layer 1 to Layer 5. Thus, each layer is assigned a specific function and each layer contains a number of nodes performing similar functions. Typically, there are two types of nodes: fixed and adaptive. Fixed nodes are represented by a circle, whereas adaptive nodes are characterized by a square. The output from the nodes of the previous layer acts as an input for the next layer. Figure 1 depicts the structure of the ANFIS-EESC model. In this proposed study, the ANFIS-EESC model is based on three inputs, four rules, and one output. The first-order TS FIS model is utilized in this model. The main advantage of using Sugeno is the computational efficiency and its ability to generate fuzzy rules from the given input parameters.

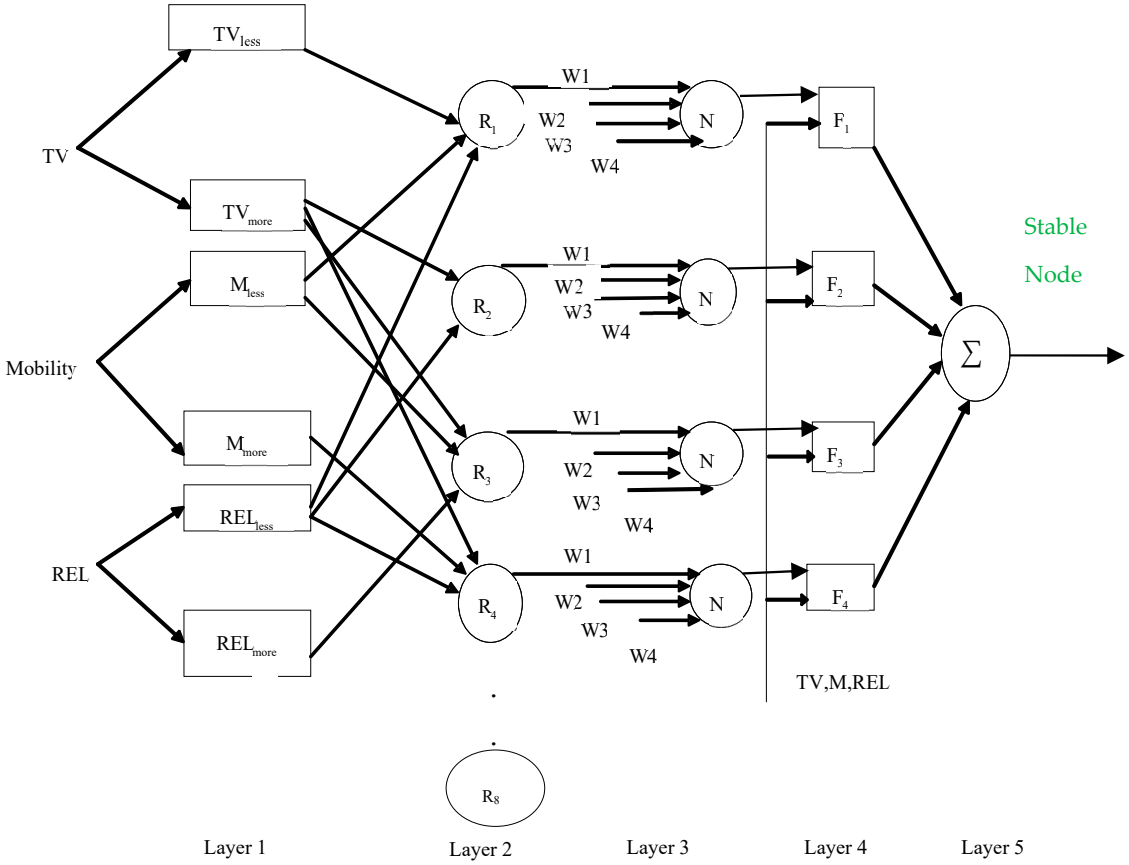

Figure 1. ANFIS-Based, Energy-Efficient Secure Clustering Model.

Layer 1 or a Fuzzification layer: Every node in this layer is denoted as a square node and is defined as an adaptive node. The nodes in this layer indicate the antecedent parts of fuzzy logic rules. Mobility, Trust Value, and Residual Energy Level are input to this layer. The degree of membership functions of inputs is determined by this layer of outputs. The following equations illustrate the Layer 1 outputs for a variety of nodes:

$$O^1_{T_{less}} = \mu_{T_{less}}(TV) \tag{6}$$

$$O^1_{T_{more}} = \mu_{\text{More}}(TV) \tag{7}$$

$$O^1_{M_{less}} = \mu_{M_{less}}(MB) \tag{8}$$

$$O^1_{M_{more}} = \mu_{M_{more}}(MB\Big) \tag{9}$$

$$O^1_{R_{less}} = \mu_{R_{less}}(RE) \tag{10}$$

$$O^1_{R_{more}} = \mu_{R_{more}}(RE) \tag{11}$$

As an illustration, the output of the node is represented by $O^1_{T_{less}}$ Layer 1. $\mu_{T_{less}}(TV)$ indicates the input membership function value.

Layer 2: Each node in this layer is defined as a fixed node denoted as a circle node. Layer 2 is represented as a rule layer labeled as Ri. In this layer, the incoming inputs are multiplied, and the product server is output. The output is represented as ω

$$\omega \mathrm{i} = \mu_{\mathrm{T_i}}(\mathrm{TV}) \times \mu_{\mathrm{M_i}}(\mathrm{M}) \times \mu_{\mathrm{R_i}}(\mathrm{REL}), \text{ where } \mathrm{I} = 1,\ 2 \tag{12}$$

Layer 3: This layer is the normalization layer denoted as N. Every node in this layer is a fixed node represented as a circle node. In Layer 3, each node receives inputs from the previous rule layer and estimates the normalized firing strength for a rule.

$$\omega = \frac{\omega_{\mathrm{x}}}{\sum_{\mathrm{x}=1}^{4} \omega_{\mathrm{x}}} \tag{13}$$

where x = 1 . . . 4.

Layer 4: Layer 4 is termed as the defuzzification layer and denoted by Fx, X =1...4. The nodes in this layer are adaptive and represented as a square node. The function of the node belonging to this layer is given as shown below:

$$O^4_x = \omega\ (\mathrm{a_i TV} + \mathrm{b_i M} + \mathrm{c_i REL} + \mathrm{d_i}) \tag{14}$$

where ω represents the output from Layer 3, the normalized firing strength, and $\mathrm{a_i}$, $\mathrm{b_i}$, $\mathrm{c_i}$, $\mathrm{d_i}$ denote the consequent parameters of the fuzzy if-then rules.

Layer 5: Layer 5 is defined as an output layer. This layer consists of a single fixed node denoted by a circle node and is indicated by $\sum$. The output of this layer is the summation of incoming signals. The nodes in this layer calculate the overall output as given by Equation (18).

$$O^5 = \frac{\sum_{i=1}^{4} \omega_i f_i}{\sum_{i=1}^{4} \omega_i} \tag{15}$$

The hybrid learning algorithm is described as adjusting the parameters. It includes two steps, namely forward pass and backward pass. During the forward pass, the consequent parameters are identified by Least Square Error and are adjusted. In the backward pass, errors are propagated backwards and premise parameters are adjusted by the gradient method. The ANFIS classifier has two modes of operation: training and testing. In the training mode of the classifier, the features of the nodes, namely, trust value and energy level, are trained by the classifier, which generates a trained pattern. In the testing mode of the classifier, the trust value of each node is tested with a trained pattern of this classifier. The

ANFIS generates a single output, either with 0 indicating the normal node or 1 indicating the malicious node.

The fuzzy-based "if-then" rules are described as follows:

Rule 1: if Mobility is M_{less} and REL is REL_{less} and TV is TV_{less}
Then $f_1 = a_1\ M_{less} + b_1\ REL_{less} + C_1\ TV_{less} + e_1$.
Rule 2: if Mobility is M_{more} and REL is REL_{less} and TV is TV_{less}
Then $f_2 = a_2\ M_{more} + b_1\ REL_{Less} + C_1\ TV_{less} + e_2$.
Rule 3: if Mobility is M_{more} and REL is REL_{more} and TV is TV_{less}
Then $f_3 = a_3\ M_{more} + b_3\ REL_{more} + C_3\ TV_{less} + e_3$.
Rule 4: if Mobility is M_{more} and REL is REL_{more} and TV is TV_{less}
Then $f_4 = a_4\ M_{more} + b_4\ REL_{more} + C_4\ TV_{less} + e_4$.
Rule 5: if Mobility is M_{less} and REL is REL_{more} and TV is TV_{More}
Then $f_5 = a_5\ M_{less} + b_5\ REL_{more} + C_5\ TV_{More} + e_5$.
Rule 6: if Mobility is M_{less} and REL is REL_{less} and TV is TV_{More}
Then $f_6 = a_6\ M_{less} + b_6\ REL_{less} + C_6\ TV_{More} + e_6$.
Rule 7: if Mobility is M_{More} and REL is REL_{less} and TV is TV_{less}
Then $f_7 = a_7\ M_{More} + b_7\ REL_{less} + C_7\ TV_{less} + e_7$.
Rule 8: if Mobility is M_{less} and REL is REL_{less} and TV is TV_{More}
Then $f_8 = a_8\ M_{less} + b_8\ REL_{less} + C_8\ TV_{More} + e_8$

where a_i, b_i, c_i and e_i for i=1 to 4 indicate linear consequent parameter. f_x indicates output for x = 1 to 4.

3.2.1. Design of Weight-Based Trust Estimation (WBTE) Algorithm

In this work, we have proposed and implemented a novel Weight-Based Trust Estimation (WBTE) algorithm to estimate the trust of the node by assigning the weights to the node using the weighted means technique. Consider a node, say X, calculates the trust on another neighboring node, say Y. In this scenario, the X will query its entire one-hop neighbour about the node Y. This one-hop neighboring node is termed Reputation Manager (RM) and assumes that there are m numbers of RM. Each RM will evaluate the trust of node Y and submit a report to node X. On receiving the trust values from its RM, X will estimate the final trust value of Y using the weighted means technique. Depending on the final trust value, the decision is made whether the node is trustworthy or malicious. Thus, the final trust value of a node is determined using Equation (6). The main flow of the WBTE algorithm is shown in Algorithm 1.

$$Trust\_Value_{Final} = \frac{Trust\_Value_{X,Y} + \sum_{k=1}^{m} W_K X Trust\ \_Value_{RM_{K,Y}}}{m+1} \tag{16}$$

$$Trust\_Value_{AVG} = \frac{\sum_{k=1}^{m} Trust\_Value}{m} \tag{17}$$

$$W_K = \frac{Trust\ \_Value_{RM_{K,Y}}}{Trust\_Value_{AVG}} \tag{18}$$

where

$Trust\_Value_{Final}$ is the final trust value.

$Trust\_Value_{AVG}$ is the average of the reputation manager trust value on Y.

W_K is the weight assigned for the trust value obtained from the Reputation Manager k.

$Trust\_Value_{X,Y}$ is the self-estimated trust of node X on Y for all nodes $n \varepsilon N$ and $Trust\ \_Value_{RM_{K,Y}}$ is the trust of reputation manager RM on Y and

K is the number of the Reputation Manager.

Algorithm 1 Weight-Based Trust Estimation (WBTE) Algorithm

Input: set of nodes N
Output: set of trustworthy nodes (Trust_node)
For each i ∈ N
    Initialise $\text{Trust\_Value}_{\text{Final}}$ to zero.
    Estimate $Trust\_Value_{Final}$ using Equation (6)
    Measure the average of RM trust value as $Trust\_Value_{AVG}$ (7)
    If $Trust\_Value_{Final} > Trust\_Value_{AVG}$ then
        Node i is the normal node
        Add i to Trust_node.
        Return Trust_node.
    Else
        Node is a malicious node
    End if
    End for.

3.2.2. Fuzzy-Based Clustering

Using factors such as Trust Value, Mobility, and Residual Energy Level, the CL is determined by the fuzzy-based clustering algorithm. Thus, the node with the maximum residual energy level, maximum trust value, and a low mobility will be given a chance to act as a CL. In this work, the members choose the CL based on the following factors: Residual Energy Level, Mobility, and Cluster Density of CL. In order to handle this uncertainty condition, a fuzzy inference system (FIS) is employed in our proposed work. The three input variables for the FIS are the Residual Energy Level, Mobility, and Density of CL. One output parameter is the CL_Choice, the probability that a member selects a CL. The main flow of the proposed FBC algorithm is described in Algorithm 2.

Algorithm 2 Fuzzy-Based Clustering (FBC) Algorithm

Input : set of trustworthy nodes
Output : cluster with CL
Find the neighbour of each node
Call the WBTM Algorithm
Estimate the Mobility
Estimate the REL.
Estimate the Cluster Density
For each i ε N
    Choose the node with minimum Mobility, maximum REL, minimum Cluster Density and
        maximum trust value as the CL_Choice.
    node_role (i) = CL_Choice
    Else
        Add i to the cluster member list
    if node_role = member
        CL = Fuzzylogic (Cluster Density, Residual Energy Level, Mobility, Trust Value)
        Join with CL As Cluster Member (CM)
    End if.
End for

The fuzzy input variables, namely, Residual Energy Level, Mobility, Cluster Density, and their corresponding linguistics variables, are given below:

Residual Energy Level—(High, Medium, Low)
Mobility—(High, Medium, Low)
Cluster Density—(High, Medium, Low)

In this work, for the boundary variables, namely, High and Low, the trapezoidal membership function is utilized, and for Medium, the triangular membership function is used. CL_Choice acts as a fuzzy output variable. Three linguistics variables for the output

variable are High, Medium, and Low. The High and Low boundary variables use the trapezoidal membership function; for the intermediate variable, Medium, the triangular membership function is used.

The CL_Choice calculation is done by considering the fuzzy IF-THEN rules. Based upon the three fuzzy inputs variables, 27 fuzzy mapping rules are constructed, as shown in Table 1. In this work, the simplicity Mamdani Inference System is used, and the Center of Area (COA) method given in Equation (19) is used for the defuzzification of the CL_Choice.

$$COA = \frac{\int \mu_A(x) x dx}{\int \mu_A(x) dx} \tag{19}$$

Table 1. Fuzzy "if-then"rules (CL_Choice).

Mobility (M)	Residual Energy Level (REL)	Cluster Density (CD)	CL_Choice
Low	Low	Low	Low
Low	Low	Medium	Low
Low	Low	High	Low
Medium	Low	Low	Low
Medium	Low	Medium	Low
Medium	Low	High	Low
High	Low	Low	Low
High	Low	Medium	Low
High	Low	High	Low
Low	Medium	Low	Medium
Low	Medium	Medium	Medium
Low	Medium	High	Low
Medium	Medium	Low	Medium
Medium	Medium	Medium	Medium
Medium	Medium	High	Low
High	Medium	Low	Low
High	Medium	Medium	Low
High	Medium	High	Low
Low	High	Low	High
Low	High	Medium	Medium
Low	High	High	Low
Medium	High	Low	High
Medium	High	Medium	Medium
Medium	High	High	Low
High	High	Low	Low
High	High	Medium	Low
High	High	High	Low

Fuzzy IF-THEN rules for nodes in the network to join the CL are given in Table 1. Fuzzy iF . . . then rules corresponding to Table 1 are given below:

Fuzzy_Rule_1: IF (Mobility = = Low) and (REL = = High) and (CD = = Low) THEN CL_Choice is High.
Fuzzy_Rule_2: IF (Mobility = = Low) and (REL = = High and (CD = = Medium) THEN CL_Choice is Medium.
Fuzzy_Rule_3: IF (Mobility = = Medium) and (REL = = High) and (CD = = Low) THEN CL_Choice is High.
Fuzzy_Rule_4: IF (Mobility = = Low) and (REL = = Medium) and (CD = = Low) THEN CL_Choice is Medium.

Table 2 depicts the maximum and minimum values for the fuzzy input variables for the computation of CL_Choice. Table 3 illustrates the fuzzy input variables and their range.

Table 2. Minimum and maximum values for Fuzzy Input Variables.

Variable Name	Min. Value	Max. Value
Mobility	5 m/s	30 m/s
Residual Energy Level	0	2
Cluster Density	0	2

Table 3. Input Ranges Corresponding to Fuzzy Variables.

S. No.	Input Values	Fuzzy Variable
1	Cluster Density	
	0.0–0.35	Low
	0.35–0.55	Medium
	0.55–1	High
2	Residual Energy Level	
	0.00–0.35	Low
	0.025–0.5	Medium
	0.35–1	High
3	Mobility	
	5–10 m/s	Low
	10–20 m/s	Medium
	20–30 m/s	High

4. Results and Discussion

The proposed ANFIS-Based, Energy-Efficient Secure Clustering (ANFIS-EESC) mechanism has been implemented using the NS2. In the experiment, 100 nodes are deployed over an area of (500 × 500) m^2, and the initial energy for each node is assumed as 1 J. The simulation parameters used in our proposed work are given in Table 4.

Table 4. Simulation parameters.

Area	500 × 500 m^2
Number of nodes	100
Initial Energy	0.5 J
Transmission Range	250 m
Radio Propagation model	Two-Ray Model
Packet Size	512 Bytes

Figure 2 shows the malicious node detection rate for five experiments with different sets of nodes. From Figure 2, it is inferred that ANFIS-EESC gives a better detection rate when compared to WCA [39,40]. This is because the proposed Weight-Based Trust Estimation algorithm will mitigate the malicious nodes from the network.

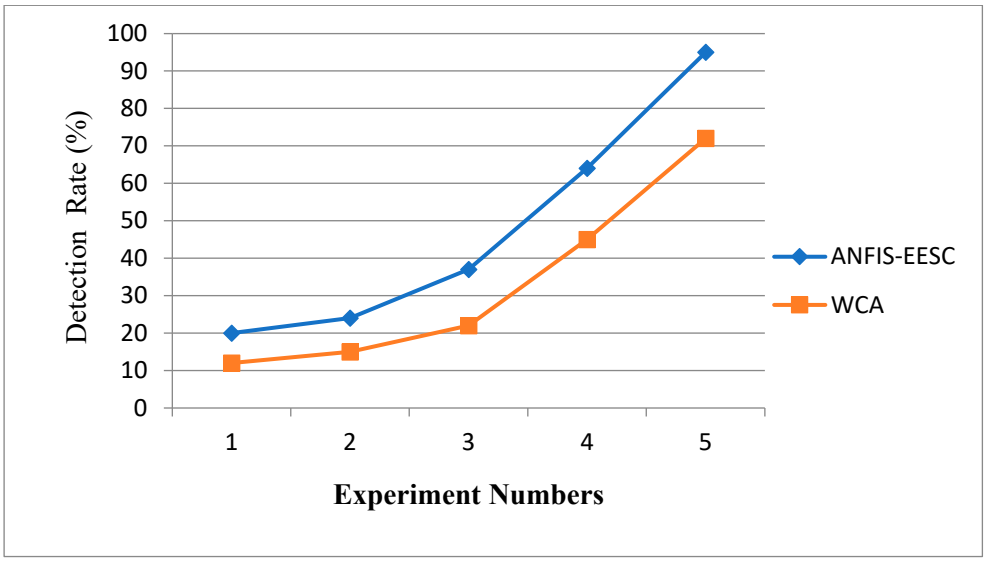

Figure 2. Detection accuracy rate.

Figure 3 shows the Packet Delivery Rate obtained in this work. From Figure 3, it is clear that the ANFIS-EESC shows better performance results than the other algorithms. This is because, in the proposed work for ANFIS-EESC, both energy-efficient and trust-based clustering is performed and the malicious nodes are identified very effectively, which leads to the transmission of more packets. In the proposed work, packet propagation is carried via the secure route. Hence, in this proposed model, the network performance is enhanced.

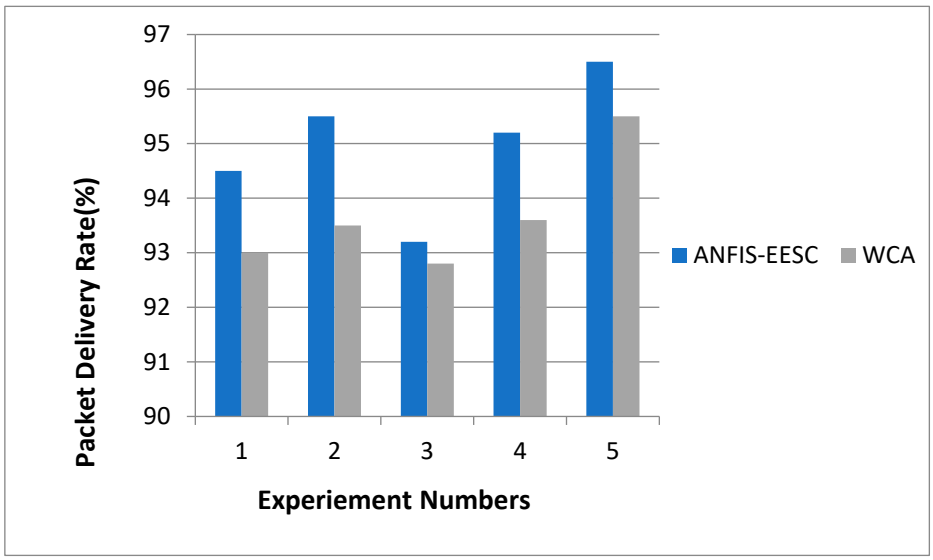

Figure 3. Packet delivery rate analysis.

Figure 4 illustrates the energy consumed in the network with varying numbers of malicious nodes. It is evident from Figure 4, the ANFIS-EESC algorithm consumes less energy when compared to WCA. This is due to the fact that the clustering reduces the number of nodes needed for routing and, therefore, consumes less energy.

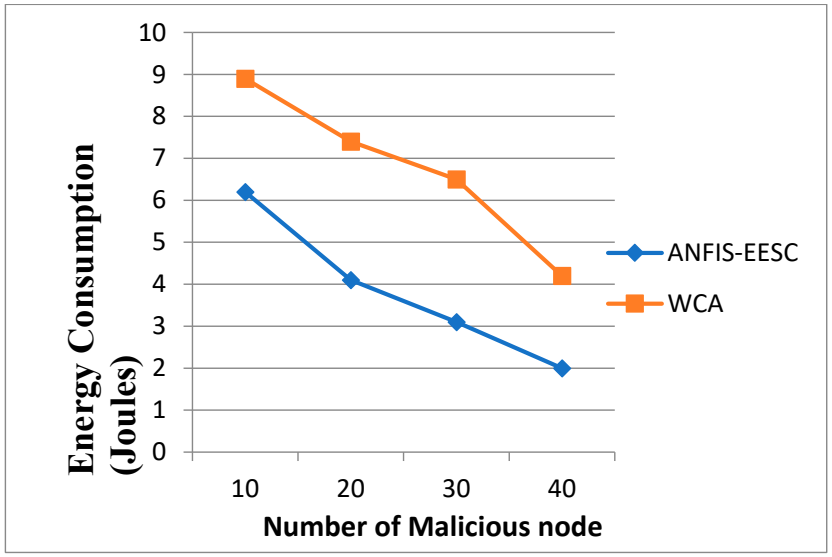

Figure 4. Energy consumption.

Figure 5 shows the performance of the proposed work ANFIS-EESC in terms of packet delivery rate concerning the mobility of the cluster leader. Figure 5 shows that the packet transmission rate is improved in ANFIS-EESC compared to WCA. This is because in the proposed work, a more stable node with low mobility is selected as CL. Thus, the packet drop caused due to the mobility of the CL is reduced.

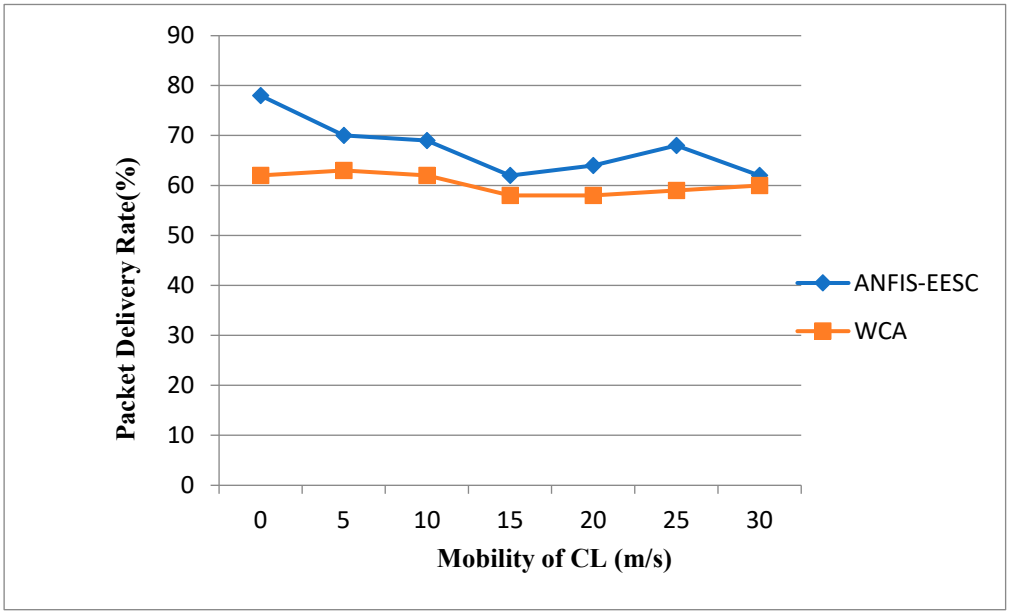

Figure 5. Packet delivery rate with respect to Mobility of CL.

Figure 6 shows the number of malicious nodes vs. detection time. Figure 6 shows that the detection time taken by the ANFIS-EESC to identify the malicious node from the network is less when compared to the existing work. This is because, in the proposed model, a novel WBTE algorithm is proposed with an objective to mitigate the malicious nodes in the network.

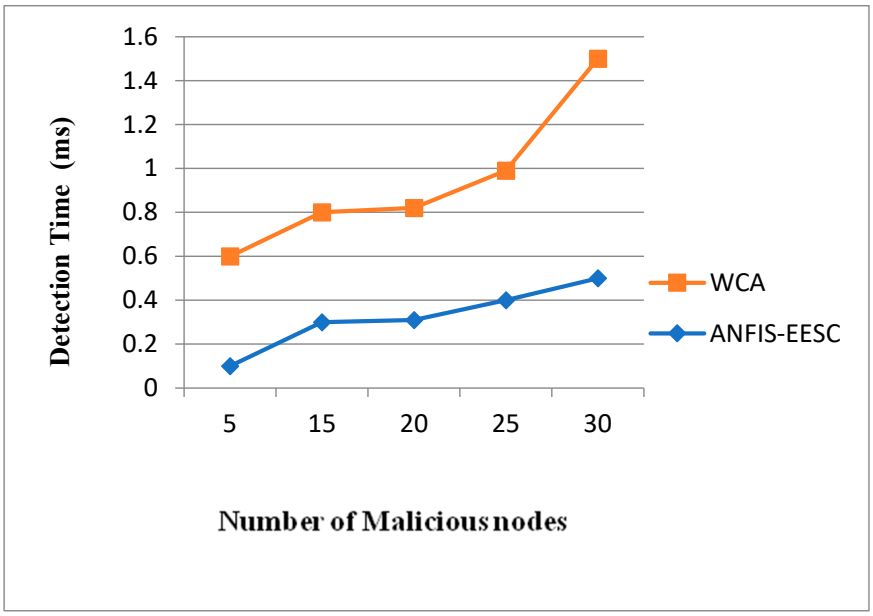

Figure 6. Detection time.

Table 5 shows the increase in the throughput of the ANFIS-EESC compared to WCA. In ANFIS-EESC, the malicious nodes are detected as the Cluster Leader and are elected based on the residual energy and trust value of nodes in the network. In this proposed model, the most trustworthy and energy-efficient node is elected as the CL. Moreover, the data propagation takes place through these CL. Thus, the packet loss in the network due to the malicious node is reduced.

Table 5. Performance comparison based on throughput.

Experiments	Throughput (%)	
	WCA	ANFIS-EESC
1	45	82
2	37	85
3	32	86
4	24	86
5	17	81

5. Conclusions

In this paper, we have proposed a novel soft computing-based secure clustering model, namely ANFIS-Based, Energy-Efficient Secure Clustering (ANFIS-EESC), that considers a neuro-fuzzy approach to form clusters and selects energy-efficient and secure cluster leaders. The main goal of our approach is to enhance the performance of the network and also to enhance the secure transmission of data in the network by electing energy-aware and trustworthy nodes as a CL. Moreover, this work also acts as a detection schema to eliminate the malicious node from the network. This work considers the following three factors—Residual Energy Level, Mobility, and Trust Value of nodes—during the cluster leader election process. In this work, two novel algorithms are proposed: Weight-Based Trust Estimation (WBTE) algorithm and Fuzzy-Based Clustering (FBC) algorithm. WBTE is proposed to calculate the trustworthiness of a node. Thus, only a trustworthy node will be allowed to act as CL. The simulation results show that the proposed system is more efficient than other existing work, WCA, in terms of network lifetime, and detection accuracy and detection time.

In the current era, novel network technologies such as the Internet of Things, 4G, 5G, Software Defined Networking, and cloud computing are gaining more attention and importance from researchers. Thus, energy-aware and secure cluster-based techniques are required to enhance network performance and quality of service (Qos). Hence, in this ANFIS-EESC model, a trust-based and energy-aware clustering technique is proposed.

Author Contributions: A.R.R. and C.K.: research concept and methodology, writing—original draft preparation. P.K.B.: review and editing; S.R.S.: investigation; W.-C.L.: validation and funding acquisition; review and editing. All authors contributed to the article and approved the submitted version. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by the National Yunlin University of Science and Technology, Douliu.

Data Availability Statement: The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chlamtac, I.; Conti, M.; Liu, J.J.N. Mobile ad hoc networking: Imperatives and challenges. *Ad Hoc Netw.* **2003**, *1*, 13–64. [CrossRef]
2. Murthy, C.S.R.; Manoj, B.S. *Adhocwirelessnetworks: Architecturesand Protocols, Portable Documents*; Prentice Hall: Hoboken, NJ, USA, 2004.
3. Perkins, C.E. Ad hoc networking: An introduction. *Ad Hoc Netw.* **2001**, *40*, 20–22.
4. Marti, S.; Giuli, T.J.; Lai, K.; Baker, M. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6–11 August 2000; ACM: New York, NY, USA, 2000; pp. 255–265.
5. Zhao, S.; Aggarwal, A.; Frost, R.; Bai, X. A survey of applications of identity-based cryptography in mobile ad-hoc networks. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 380–400. [CrossRef]
6. Kulothungan, K.; Ganapathy, S.; Indra Gandhi, S.; Yogesh, P. Intelligent secured fault tolerant routing in wireless sensor networks using clustering approach. *Int. J. Soft Comput.* **2011**, *6*, 210–215. [CrossRef]
7. Ganapathy, S.; Kulothungan, K.; Muthuraj Kumar, S.; Vijayalakshmi, M. Intelligent feature selection and classification techniques for intrusion detection in networks: A survey. *EURASIP J. Wirel. Commun. Netw.* **2013**, *271*, 1–16. [CrossRef]
8. Jerusha, S.; Kulothungan, K.; Kannan, A. Location aware cluster based routing in wireless sensor networks. *Int. J. Comput. Commun. Technol.* **2012**, *3*, 1–6. [CrossRef]
9. Liu, Y.; Xiong, N.; Zhao, Y.; Vasilakos, A.V.; Gao, J.; Jia, Y. Multi-layer clustering routing algorithm for wireless vehicular sensor networks. *IET Commun.* **2010**, *4*, 810–816. [CrossRef]
10. Gerla, M.; Tzu-ChiehTsai, J. Multicluster, mobile, multimedia radio network. *Wirel. Netw.* **1995**, *1*, 255–265. [CrossRef]
11. Pirzada, A.A.; McDonald, C. Establishing trust in pure ad-hoc networks. In Proceedings of the 27th Australasian Conference on Computer Science, Dunedin, New Zealand, 1 January 2004; pp. 47–54.
12. AntesarShabut, M.; KeshavDahal, P.; SanatBista, K.; IrfanAwan, U. Recommendation Based Trust Model with an Effective Defence Scheme for MANETs. *IEEE Trans. Mob. Comput.* **2015**, *14*, 2101–2115.
13. Mohammed, N.; Otrok, H.; Wang, L.Y.; Debbai, M.; Bhattacharya, P. Mechanism design based secure leader elevation model for intrusion detection in MANETs. *IEEE Trans. Dependable Secur. Comput.* **2011**, *8*, 89–103. [CrossRef]
14. Xia, H.; Jia, Z.; Li, X.; Ju, L.; Sha, E.H.M. Trust prediction and trust- based source routing in mobile adhoc networks. *Ad Hoc Netw.* **2013**, *11*, 2096–2114. [CrossRef]
15. Theodorakopoulos, G.; Baras, J.S. On trust models and trust evaluation metrics for ad hoc networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 318–328. [CrossRef]
16. Chiang, C.C.; Wu, H.K.; Liu, W.; Gerla, M. Routing in clustered multihop, mobile wireless networks with fading channel. In Proceedings of the IEEE International Conference on Networks, Houston, TX, USA, 12 June 1997; pp. 197–211.
17. Safa, H.; Artail, H.; Tabet, D. A cluster-based trust-aware routing protocol for mobile ad hoc networks. *Wirel. Netw.* **2010**, *16*, 969–984. [CrossRef]
18. Vasilakos, A.V.; Zhang, Y.; Spyropoulos, T. (Eds.) *Delay Tolerant Networks: Protocols and Applications*; CRC Press: Boca Raton, FL, USA, 2011.
19. Duarte, P.B.; Fadlullah, Z.M.; Vasilakos, A.V.; Kato, N. On the partially overlapped channel assignment on wireless mesh network backbone: A game theoretic approach. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 119–127. [CrossRef]
20. Attar, A.; Tang, H.; Vasilakos, A.V.; Yu, F.R.; Leung, V. A survey of security challenges in cognitive radio networks: Solutions and future research directions. *Proc. IEEE* **2012**, *100*, 3172–3186. [CrossRef]
21. Fadlullah, Z.M.; Taleb, T.; Vasilakos, A.V.; Guizani, M.; Kato, N. DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis. *IEEE/ACM Trans. Netw. (TON)* **2010**, *18*, 1234–1247. [CrossRef]

22. Zhang, Z.; Wang, H.; Vasilakos, A.V.; Fang, H. ECG cryptography and authentication inbody area networks. *IEEE Trans. Inf. Technol. Biomed.* **2012**, *16*, 1070–1078. [CrossRef]
23. Yan, Z.; Zhang, P.; Vasilakos, A.V. A survey on trust management for internet of things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134. [CrossRef]
24. Demestichas, P.P.; Stavroulaki, V.A.G.; Papadopoulou, L.M.; Vasilakos, A.V.; Theologou, M.E. Service configuration and traffic distribution in composite radio environments. *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.* **2004**, *34*, 69–81. [CrossRef]
25. Chettibi, S.; Chikhi, S. Dynamic fuzzy logic and reinforcement learning for adaptive energy efficient routing in mobile ad-hoc networks. *Appl. Soft Comput.* **2016**, *38*, 321–328. [CrossRef]
26. Chaudhary, A.; Tiwari, V.N.; Kumar, A. A Cooperative Intrusion Detection System for Sleep Deprivation Attack Using Neuro-Fuzzy Classifier in Mobile Ad Hoc Networks. In *Computer Intelligence in Data Mining*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 2, pp. 345–353.
27. Kim, J.M.; Park, S.H.; Han, Y.J.; Chung, T.M. CHEF: Cluster head election mechanism using fuzzy logic in wireless sensor networks. In Proceedings of the IEEE 10th International Conference on Advanced Communication Technology, Gangwon, Republic of Korea, 17–20 February 2008; pp. 654–659.
28. Sharma, T.; Kumar, B. F-MCHEL: Fuzzy based master cluster head election Leach protocol in wireless sensor network. *Int. J. Comput. Sci. Telecommun.* **2012**, *3*, 8–13.
29. Logambigai, R.; Kannan, A. Fuzzy logic based unequal clustering for wireless sensor networks. *Wirel. Netw.* **2016**, *22*, 945–957. [CrossRef]
30. Nayak, P.; Devulapalli, A. A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime. *IEEE Sens. J.* **2016**, *16*, 137–144. [CrossRef]
31. Ban, X.; Gao, X.Z.; Huang, X.; Vasilakos, A.V. Stability analysis of the simplest Takagi–Sugeno fuzzy control system using circle criterion. *Inf. Sci.* **2007**, *177*, 4387–4409. [CrossRef]
32. Zhang, F.; Jia, Z.; Xia, H.; Li, X.; Sha, E. Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM (1, 1) model. *Comput. Commun.* **2012**, *35*, 589–596. [CrossRef]
33. Su, B.L.; Wang, M.S.; Huang, Y.M. Fuzzy logic weighted multi-criteria of dynamic route lifetime for reliable multicast routing in ad hoc networks. *Expert Syst. Appl.* **2008**, *35*, 476–484. [CrossRef]
34. Tan, S.; Li, X.; Dong, Q. Trust based routing mechanism for securing OSLR-based MANET. *Ad Hoc Netw.* **2015**, *30*, 84–98. [CrossRef]
35. Tang, Y.; Pan, Z.; Pedrycz, W.; Ren, F.; Song, X. Viewpoint-Based Kernel Fuzzy Clustering With Weight Information Granules. *IEEE Trans. Emerg. Top. Comput. Intell.* **2022**, 1–16. [CrossRef]
36. Hu, X.; Tang, Y.; Pedrycz, W.; Di, K.; Jiang, J.; Jiang, Y. Fuzzy Clustering with Knowledge Extraction and Granulation. *IEEE Trans. Fuzzy Syst.* **2022**, 1–15. [CrossRef]
37. Basu, P.; Khan, N.; Little, T.D.C. A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks. In Proceedings of the IEEE ICDCS Workshop on Wireless Networks and Mobile Computing, Mesa, AZ, USA, 16–19 April 2001; pp. 413–418.
38. Turgut, D.; Turgut, B.; Elmasri, R. Optimizing Clustering Algorithm in Mobile Ad hoc Networks Using Simulated Annealing. *Wirel. Commun. Netw.* **2003**, *3*, 1492–1497.
39. Chatterjee, M.; Das, S.K.; Turgut, D. WCA: A weighted clustering algorithm for mobile Ad Hoc networks. *J. Clust. Comput.* **2002**, *5*, 193–204. [CrossRef]
40. Kavitha, C.; Mani, V.; Srividhya, S.R.; Khalaf, O.I.; Tavera Romero, C.A. Early-Stage Alzheimer's Disease Prediction Using Machine Learning Models. *Front. Public Health* **2022**, *10*, 853294. [CrossRef] [PubMed]