Journal of Network and Innovative Computing
ISSN 2160-2174 Volume 1 (2013) pp. 65 - 73
© MIR Labs, www.mirlabs.net/jnic/index.html

Application of Fuzzy Sets for Isolating Selfish nodes by Trust Evaluation during Auto-configuration and Service Establishment in MANETs

Reshmi.T.R[1], Murugan.K[2]

[1]Ramanujan Computing Centre, Anna University,
Chennai, India.
reshmi.engg@gmail.com

[2] Ramanujan Computing Centre ,Anna University,
Chennai, India.
murugan@annauniv.edu

***Abstract*: Mobile Ad-hoc networks (MANETs) are infrastructure-less wireless networks. These networks are easily deployable and are used during disaster recovery, emergency situation and in areas with poor infrastructure. Each node in the MANET has to be assigned with an IP address to start communication and receive services. These IP addresses are configured using Stateless Auto-configuration or Stateful Auto-configuration. The Stateful Auto-configuration using a distributed dynamic server service is discussed in this paper. The current approach of server selection in Stateful Auto-configuration is based on factors like address buffer size, distance from the requesting node, link access to the node etc. The impacts of selfish nodes during the server selection are not addressed till now. Here in this paper we propose an algorithm using fuzzy sets to find the selfish nodes, which impose high threat to the performance of the MANET. The algorithm calculates the trust value of the nodes and thereby selects the servers which do not show selfish behaviors, and are with high trust value. The proposed technique has proven to improve the network throughput and, reduce the packet drops and network response time.**

Keywords: Fuzzy sets, IP address, MANETs, Stateful Auto-configuration, Selfish Nodes, Trust**.**

I. Introduction

The wireless networks are broadly divided as Infrastructure networks and Ad-hoc Networks. The Infrastructure networks have access points (AP) which act as centralized routing devices for communication between nodes. In Ad-hoc networks the node themselves act as nodes as well as routers and help in communication between nodes. The communication packets transmitted by the nodes, travel multi-hop to reach the destination device.

The routing protocols used by the Ad-hoc Networks are broadly classified as reactive protocols and pro-active protocols. Reactive protocols have a calculated routing table in each of the node and these route entries are used to route the packets between the nodes. Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV) are examples for reactive protocols. Pro-active protocols are routing protocols which do the route entries only when a communication is initiated. The nodes will not be processing any route updates until a communication is initiated. Ad-hoc On-Demand Distance Vector (AODV) and Dynamic source Routing (DSR) are examples of pro-active protocols.

The Ad-hoc networks with mobile nodes are called Mobile Ad-hoc networks (MANETs). These networks have dynamically changing topology as the nodes are mobile. So a frequent updation of the network topology has to be done. MANETs have a specialized protocol called Neighbor Host Discovery Protocol (NHDP) which performs the function of topology updation.

There are various communication technologies used in the wireless communications. These include Bluetooth, Wi-Fi, Wi-Max etc. All these technologies can be used in Ad-hoc wireless communications. All these communication require a unique identifier for each node. Medium Access Control (MAC) addresses and Internet Protocol (IP) addresses are used as identifiers in these networks. All these identifiers are to be assured to be unique before using it for communication. Here in this paper we focus on Ad-hoc a network which uses IP addresses as identifiers.

There are two versions of Internet protocols that are used in the networking devices. Internet protocol Version 4 (IPv4) is the first version of Internet Protocol (IP) which came in to the market. The IPv4 uses a 32 bit dotted address for its communication. The next version called Internet protocol Version 6 uses a 128 bit address, which are separated by double colons, for its communication. Both these version can be independently used in MANETs for its node identification and communication.

The IP addressing protocols are broadly classified as Stateless and Stateful Auto-configuration protocol. The node self-generates an IP address and does a duplicate check in Stateless Auto-configuration. These nodes will not have any knowledge about the already assigned IP addresses among the nodes in the network. The Stateful Auto-configuration have the centralized database of the IP addresses allocated to the nodes in the network and a set of free IP addresses which can be used to allocate to the newly entering nodes. Dynamic Host Configuration Protocol (DHCP) is an example of the Stateful IP addressing protocol. In MANETs a centralized DHCP server cannot be maintained because of the resource constrains and mobility of the nodes. So a dynamic distributed Stateful Auto-configuration is always preferred in MANET. To ensure the accurate implementation of the network, the addressing protocols try to achieve the following goals.

i. Unique IP addresses assignment: Each of the nodes in the network should be assigned with a unique identifier for its identification and communication. There should not be any conflict or ambiguity during communication.
ii. Recovering and allocating addresses during network merging and partitioning: A node maintains the same IP address reserved for it in the network until it stays in the same network. When there is network partitioning (i.e. a node leaves the network), the IP address will be released by the node. These addresses are to be managed and reused by the protocol. Whenever a network merges with an existing network, the IP addresses of these nodes have to be reconfigured to continue the communication.
iii. Availability of addresses: The addressing protocol should be scalable to support any number of nodes. The protocol should be able to provide an address without waiting for a reclaim of address. The nodes should be able to configure its address from a server which requires a multi-hop communication to reach it.
iv. Authenticate the rival for an IP address request: The protocol should be able to manage the address request from two nodes at the same time. The protocol should be able also be able to authenticate the identifiers provided for both the nodes.
v. Synchronization of address buffer: In Stateful Auto-configuration the nodes in the MANETs are provided with address buffer which is used to allocate to the newly entering nodes in the network. These address buffers has to be synchronized to avoid the address conflicts.

Selfish nodes are nodes which show least interest to participate in routing of packets which are intended to other nodes. These nodes have great impact in the performance of the Auto-configuration protocol. The proposed work focusses on isolating the selfish nodes during the functioning of the Auto-configuration protocol. A Mean Value Analysis(MVA) technique is used for evaluating the performance pattern of the nodes. Fuzzy rule sets are used to define the degree of membership when compared to other logic functions. Fuzzy sets can provide a precise description of the measured value like low, medium, high, very high etc. Here the fuzzy sets are used to evaluate the performance of the node and find the degree of trusted nature in its communication pattern.

The paper is divided into seven sections. Section II describes the literature review of the Auto-configuration protocol. Section III describes the basic functioning and mechanism of the Stateful dynamic IP addressing protocol. Section IV describes the algorithm, fuzzification and defuzzification of data sets to generate the trust levels of nodes. Section V contains the results obtained by applying the algorithm to isolate the selfish nodes in the MANET. Section VI discusses the conclusion.

II. Literature Reviews

The addressing protocols used for configuring an IP address in MANETS differs based on the versions of Internet protocols. The Stateful approach used in MANETs started off with a centralized approach and later on moved on to dynamic- distributed approaches to address the issues faced.

Chesire[1] initiated an IPv4 addressing protocol which gained good popularity in wired networks. The protocol allowed nodes to randomly select an address in the range of 169.254.1.0 to 169.254.254.255 and then check for its duplication. The idea was later on suggested for MANET application. A centralized Stateful Autoconfiguring protocol was introduced by Patchipulusu[2] as an outcome of his research. The protocol selected a centralized server which assigns IP addresses to the newly entering nodes. The centralized nature was a bottleneck to the functioning of the protocol.

Nasargi[3] developed a successful, distributed Stateful configuration protocol for IPv4 based MANETs and named it as “MANETconf”. When a node requests for IP address from a server node, it is assigned with the highest value IP address. These algorithms have to select big address range to provide scalability of nodes. An IPv4 based Stateless Auto-configuration protocol was proposed by Mukta et al [4]. The protocol selected an agent which does the address configuration to the nodes and also takes care of the address reclaim when a node departs a network. The protocol provides high scalability but does not support network partioning.

Thomson et al [5] is still appreciated for his proposed work, “Stateless IPv6 based Auto-configuring protocol” which eased the deployment of devices in large scale networks. The protocol allows the node to self-configure an address and check for duplication using an algorithm called Duplicate Address Detection (DAD). According to the algorithm, the node assigns an address and finds a neighbor using network advertisement. The neighbor receives the advertisement and reply with neighbor solicitation. The reply message contains the network prefix used and this help the node to reconfigure the address based on network prefix and then do the DAD in the network. The protocol induces a flooding of packets during the DAD process and hence the network performance is affected.

A Stateless Auto-configuration protocol specifically for both the Internet protocol (IP) versions was designed by Perkin [6]. The protocol allows the node to randomly select an address and initiate the Route Request (RREQ) packet flooding across the network. If any of the nodes already own the same address, the node reply with a Route Reply (RREP) packet. The protocol uses the flooding technique which often deteriorates the network performance. The protocol couldn't handle its functioning during network partitioning.

Mohnsin[7] proposed a Stateful Autoconfiguration protocol that can be used for both IPv4 and IPv6 based MANETs. Each of the configured nodes in MANET is assigned with a unique IP address and also a disjoint set of IP address which can be assigned to the newly entering nodes. The protocol maintenance was tedious and these types of protocols were prone to various types of attacks.

Park et al[8] proposed a distributed Autoconfiguration protocol for IPv6 based MANETs. The protocol performs a mechanism called strong duplicate detection, which checks for the dupli cation of address during the initial assignment. The protocol forms hierarchical addressing structures which ease the deployment and duplicate detection. The protocol provides full guarantee for the uniqueness of IP addresses of the nodes but doesn't support network merging and partitioning.

Weniger[9] proposed a hybrid configuring protocol called PACMAN, which assigned variable length addresses as identifiers for the nodes. It performs a weak duplicate detection [10] which checks duplication only when a packet communication is triggered by the node. So the node will not be aware of duplication during the initial assignment of address. The protocol uses complex algorithms to reduce the address conflicts. The complexity of the algorithmic computation is the main drawback of PACMAN. The same protocol has been tried in VANET to check its performance[17].

Mansi[11] proposed an IPv4 and IPv6 based dynamic distributed configuring protocol. The new node entered in to the network floods the address request message across the network. The nodes called as "allocator" reply to the message with an address offer. The requested node selects one of the offers and configures its IP addresses. The timers used in the protocol functioning makes it faster and less complex. But the flooding of packets and the timer functioning sometime induce network deterioration.

Dongkyun Kim et al. [12] proposed a stateless address Auto-configuration in mobile ad-hoc networks. The proposed work used a Passive Duplicate Address Detection (PDAD) method over proactive Ad-hoc routing protocols. The algorithm uses information like sequence number, location, and neighbor knowledge to achieve a good precision. The algorithm required shorter time to detect address conflict. The protocol was focused only on on-demand routing protocols.

Sanghyun Ahn et al. [13] described an address pool based address configuration mechanism in MANET. The protocol used node or router nodes which acted as the Internet gateway as the primary DHCP server for the network. The node contained the set of IP addresses allocated by the provider, and these addresses are allocated to the new nodes. Whenever a node request for an IP address and is assigned with a unique address, it is also provided with a part of its address pool, so that the node can act as a server and distribute IP addresses to the newly entering nodes. Whenever a node receives the IP address offer from many nodes, the requestor chooses the server arbitrarily and gains the unique IPv6 address. This solution does not consider the complexity and QoS issues caused by the protocol during the server selection and address pool allocation.

III. Dynamic Distributed Stateful Auto-configuration Protocol

The proposed protocol concentrates on the impact of the selfish nodes in addition to the common features of the address configuring protocol in MANETs.

A. Basic idea

The Stateful address configuration protocol in MANETs maintains an address buffer in each node which can be allocated to the newly entering nodes and also have the database of the already assigned IP addresses to the nodes. These types of protocols assure address uniqueness and are not prone to address conflicts. During the MANET initialization, the node which acts as the internet gateway to the network will be the allocated with an address buffer provided by the Internet Service Provider (ISP). These addresses are used for configuring the newly entering nodes in the MANET. So initially the Internet gateway (IGW) router which is the router to the internet will be the DHCP server to the network. In dynamic distributed IP addressing protocols, each node in the MANET is assumed to have a disjoint set of IP addresses derived from the previous allocating node. The allocating node keeps checking the IP addresses of the nodes. The address reclaiming is also done by the node that provides the IP address. So the protocol is assumed to provide unique IP address to the nodes in MANET as in the Dynamic Configuration and Distribution Protocol (DCDP) [14] designed for wired networks.

B. Auto-configuration of the new node

When a node enters the network, it starts multicasting *Router Solicitation* message. The IGW router responds back with the *Router Advertisement.* The requesting node analyses the *Router Advertisement* received to check the *Managed flag (M flag)* and Other Stateful configuration values (O flag). The message format of Router Advertisement is given in figure 1. If the node finds the M flag value set as 1, it unicasts a *DHCP request message* to the IGW router. The IGW router unicasts a *DHCP response* with an IP address from the set of pre-configured address buffer. Once the node is configured with an IP address, the node is also allocated with a disjoint subset of address buffer. Hence the node acts as a DHCP server for the newly entering nodes.

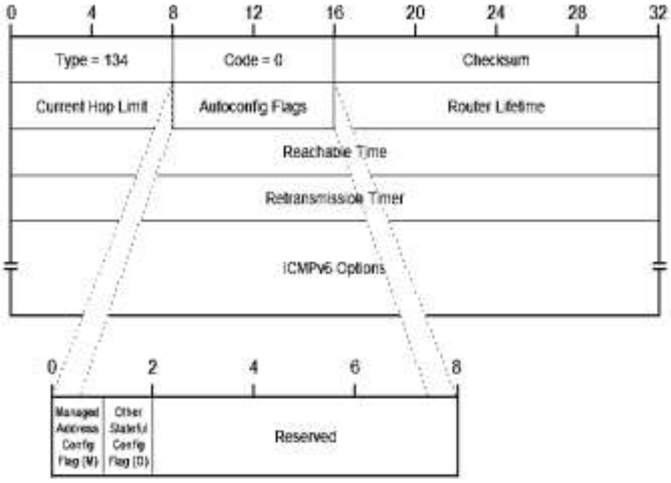


Figure 1. Router advertisement message format

When many preconfigured nodes are present in a network, a new node entering the network starts multicasting the *Router Solicitation*, and it will receive *Router Advertisement* from all the preconfigured nodes in the network. So the requesting node will select a server node and start sending the *DHCP request*. The working of the Dynamic Distributed Stateful Auto-configuration protocol is represented using a diagram given in figure 2.

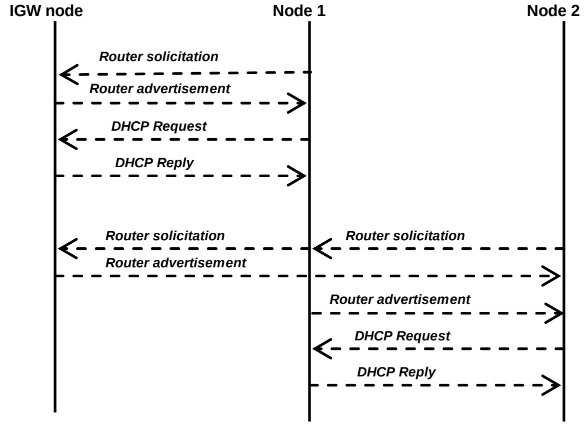


Figure 2. Working of Dynamic Distributed Stateful Auto-configuration protocol

C. Synchronization of address buffer

Each node in the network is assigned with a disjoint subset of addresses from the IGW node and is preserved in the address buffer. When a new node enters the network and finds a server for its address configuration, the server node offers an address from its address buffer. It also provides a part of its address buffer to the new node and synchronizes its database with the IGW. IGW contains the list of allocated address in the network, hence no address is duplicated in the network and uniqueness is assured. The IGW node is the authorized node to take care of database synchronization. The address buffer synchronization is done at regular intervals by the IGW node or by other nodes when there is an update in its address buffer. IGW node preserve the knowledge of the address set contained in the address buffer of each node. The information preserve help it to maintain the unique identification for each nodes.

D. Reclaiming the detached IP addresses

A node in the MANET may leave the network with explicit notification or without any notification. The IGW node checks the aliveness of the IP address at regular intervals. If the IGW node doesn’t receive the reply form the node for a time interval, it assumes that the node might have left the network so it reclaim the IP address and add it to the free set of IP address in the address buffer. These addresses are then reused for the addressing of new nodes. If the node explicitly notifies that the node is moving to another network then it releases its IP address and the IP address is added to the address buffer containing free set of IP addresses.

E. Support for network partitioning and merging

The network merging and partitioning are very common in MANETs because of the mobile nodes. During merging a group of nodes enter in to the MANET and require the address reconfiguration of all the nodes. In those cases, all these nodes release their IP addresses and receive IP addresses as like the new node entering the network. During partitioning of the MANET, the network with IGW node easily identifies the partitioning and updates the address buffer by collecting the set of free IP addresses. The nodes in the network which doesn’t have IGW node will listen for the aliveness message for a time interval, and then finds the new IGW node. The IGW node is selected based on the criteria like node performance, access to internet, address buffer size etc.

IV. Fuzzy system based selfish node detection in dynamic distributed Stateful Auto-configuration

Fuzzy systems are mathematical systems which use the analogous inputs provided as logical variables of data set with continuous values between 0 and 1. The fuzzy systems are widely used in variety of applications [16]. Fuzzy system can provide a clear idea of the range of membership of a function rather than the extremes like low or high. They can define membership like very low, low, medium, high, very high etc. These systems are equally beneficial like genetic algorithms and neural networks, the advantage is that it can be made much more human understandable. The application of fuzzy can make human task much mechanic.

A fuzzy based resource management [18] has applied fuzzysets in MANETs to ensure QoS. Here a fuzzy system is applied in dynamic distributed Stateful Auto-configuration to find the selfish nodes in the MANETs. Selfish nodes are those nodes which disagree to participate in forwarding the packets indented to other nodes. If selfish nodes are selected for forwarding the *DHCP request* or to serve *DHCP offer,* these nodes drop the service packets and delay the Auto-configuration of the node. So the selfish nodes are isolated based on the trust value calculated by the fuzzy systems. Trust value is derived as fuzzy sets which give precise insight of the nature of communication of the node. The algorithm calculates the node throughput and node capacity which are used as fuzzy sets to derive the degree of membership of the trust value. The nodes with low trust values are isolated as selfish nodes and are not chosen as the server nodes for configuring the addresses to the newly entering nodes. The architecture for the fuzzy system for isolating the selfish nodes in dynamic distributed Auto-configuration protocol is diagrammatically given in figure 3.

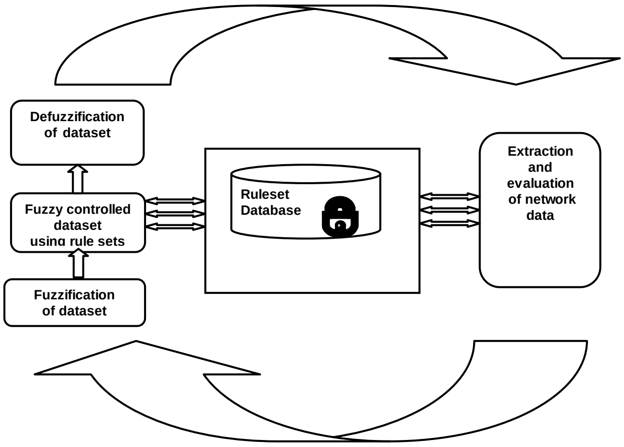

Defuzzification of dataset
Fuzzy controlled dataset using rule sets
Fuzzification of dataset
Ruleset Database
Extraction and evaluation of network data

Figure 3: Architecture of fuzzy system for the isolation of selfish nodes in MANETs.

The components of the fuzzy system used for the isolation of the selfish nodes in MANET and their functioning are listed below.

A. Fuzzification of dataset

The fuzzification process is the conversion of the analogous inputs in to the values ranging between 0 and 1. The fuzzification in the architecture converts the dataset extracted from the network traffic to the fuzzy set values. The algorithm used in fuzzy based selfish nodes isolation, finds the network throughput and network utilization. The dataset is then converted in to fuzzy values to calculate the node capacity and utilization.

B. Requirement analysis

The application of the MANET varies from defense purpose to the gaming environment. So based upon the requirement for the network, the ruleset generation for the isolation of selfish nodes varies. The network required producing high security and throughput should have much precise filter of the selfish nodes, in these cases the ruleset for calculating the trust value of the nodes must categorize the low and medium trust value nodes as selfish nodes. But in applications like gaming environment, the impact of selfish nodes is not high. So in those cases during trust calculation the ruleset can be generated in such a way that only the low trust value nodes are called selfish nodes.

C. Ruleset generation

Based on the application of the MANET and the requirement analysis of the network, the rulesets are formulated and generated. The ruleset generation is a secured mechanism which uses a authentication keys which are preserved by the moderator of the network. The ruleset generated is applied on the fuzzified dataset to generated fuzzy controlled dataset. These are resultant values which can be human understandable. An example of the ruleset generated is given in the table 1.

Table 1 : Sample of Fuzzy function configurations

```
#CAPACITY UTILISATION
attname=CAPACITY atttype=f
termset=LOW%MEDIAL%HIGH
LOW=RFuzzySet(0.0,0.39)
MEDIAL=TrapezoidFuzzySet(0.0,0.39,0.54,0.69)
HIGH=LFuzzySet(0.7,1.0)
Range=0-1
LOW=RFuzzySet(0.0,0.09)
MEDIAL=TrapezoidFuzzySet(0.0,0.09,0.15,0.19)
HIGH=LFuzzySet(0.2,0.49)
VERYHIGH=LFuzzySet(0.5,1.0)
Range=0-1
```

D. Fuzzy controlled dataset

The fuzzy controlled dataset relate the ruleset generated and the fuzzified dataset to obtain the degree of membership of the continuous values. Assume the fuzzy member function of capacity, *C (t)* consists of three fuzzy sets: *Low (L), Medial (M) and High (H).* The fuzzy membership function of *H (t)* and $T_L(t+1)$ consists of four different levels of fuzzy sets. *Low (L), Medial (M), High (H) and Very High (VH).* The fuzzified dataset is correlated with the interference relationship *R(t),* where

$$R(t)=U(t) \times C(t) \times TL(t+1) \qquad (1)$$

$$R(u,c,m) = U(h) \cap C(c) \cap T_L(m) \qquad (2)$$

The variables $u \in U$, $c \in C$ and $m \in T_L$.

For all the n rules we have the fuzzy interference relationship as given in equation

$$R(u,c,m) = \bigcup R(u,c,m) \qquad (3)$$

For each pair of given input U^* and C^*, the general total relationship *R*, the output can be calculated.

$$T_L^* = (U^* \times C^*) \circ R \qquad (4)$$

Then the maximal membership degree approach, the trust value U* ∈ [0, 1], can be calculated with the de-fuzzy methods. The rules in table 2 establish a mapping from *U x C* to T_L.

Table 2. Fuzzy Rules on Trust Level TL (t+1)

C(t)//U(t)	*L*	*M*	*H*	*VH*
L	*L*			
M	*L*	*M*		*H*
H	*L*	*M*	*H*	*VH*

E. Defuzzification of the dataset

The dataset generated by the fuzzy controller dataset is defuzzified to find the maximal degree of membership, which clearly concludes the trust value of the nodes. The membership of the trust level of a node decides whether the node is a selfish node or not. If the node is identified as the selfish node, then the node is isolated during the Auto-configuration process. So the address acquisition and service discovery delay of the newly entering node is reduced. The isolation of selfish nodes increases the network throughput and reduces network response time.

F. Extraction and evaluation of network data

The network traffic in MANET is extracted and evaluated to form the dataset input for the fuzzy system. The real traffic data is evaluated to find the network throughput and network utilization. The Mean value analysis (MVA) tool is used to analyze the traffic. The MVA tool is used to analyze traffic behaviors and performance in closed networks. Since MANET is such a type of closed network, MVA can be used for to analyze it. The algorithm followed by the MVA is given below.

Algorithm.1. Steps in Mean Value Analysis (MVA)

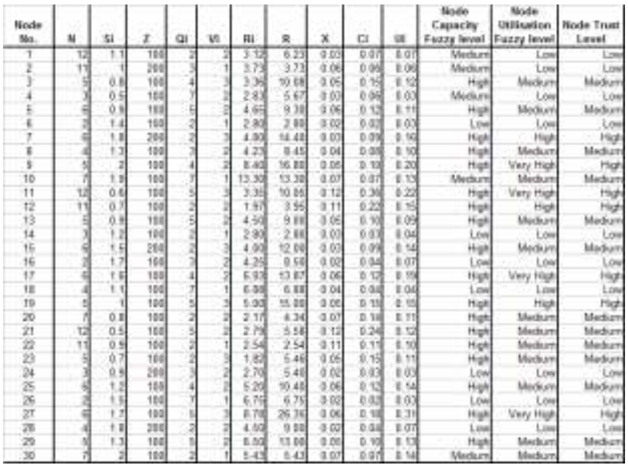
```
i. Initialize Network throughput, X=0
ii. For N Nodes, Communicated with nodes from
        i=1 to M Do
      Buffer size Q=Total Node(N)/Communicating
  nodes
iii. WHILE maximum of difference of the buffer
        value Q and product of network throughput,
        response time, no: of visits for each
        communication is greater than acceptable
        error Do
iv. For all nodes i=1 to N Do


v. Node Response time = Service time of node
        (1+ product of the ratio of total nodes
        excluding the node to the  total nodes in the
        network and buffer size)
vi. Network throughput = Ratio of total nodes in
        the network to the sum of buffer size and
        network response time
vii. Network Response time = Sum of the product of
        the node's response time and the number of
        visits by each node during communication
```

V. Numerical Results

The fuzzy system for the isolation of selfish nodes during the Auto-configuration of MANETs was tested using different datasets extracted from the network traffic. The experiments have be conducted in various scenarios and the results have be analyzed. The input datasets and output datasets have been collected for various scenarios like 30 nodes, 60 nodes, 90 nodes and 120 nodes. An example of the dataset used during the fuzzification, the fuzzy controlled data and the de-fuzzified values are shown in table 4.

Table 4. Dataset input and outputs in fuzzy system



Node No.	N	Si	Z	Qi	Vi	Ri	R	X	Ci	Ui	Node Capacity Fuzzy level	Node Utilisation Fuzzy level	Node Trust Level
1	12	1.1	100	2	2	3.12	6.23	0.03	0.07	0.01	Medium	Low	Low
2	11	1	200	3	1	3.73	3.73	0.06	0.09	0.06	Medium	Low	Low
3	5	0.8	100	4	3	3.36	10.08	0.05	0.15	0.12	High	Medium	Medium
4	3	0.5	100	7	2	2.83	5.67	0.03	0.09	0.03	Medium	Low	Low
5	6	0.9	100	6	2	4.69	9.38	0.06	0.13	0.11	High	Medium	Medium
6	3	1.4	100	2	1	2.90	2.90	0.02	0.03	0.03	Low	Low	Low
7	6	1.8	200	2	3	4.80	14.40	0.03	0.09	0.10	High	High	High
8	4	1.3	100	3	2	4.23	8.45	0.04	0.05	0.10	High	Medium	Medium
9	5	2	100	4	2	8.40	16.80	0.05	0.10	0.20	High	Very High	High
10	7	1.9	100	7	1	13.30	13.30	0.07	0.07	0.13	Medium	Medium	Medium
11	12	0.6	100	5	3	3.35	10.05	0.12	0.36	0.22	High	Very High	High
12	11	0.7	100	2	2	1.97	3.95	0.11	0.22	0.15	High	High	High
13	5	0.9	100	5	2	4.50	9.00	0.05	0.10	0.09	High	Medium	Medium
14	3	1.2	100	2	1	2.90	2.90	0.03	0.03	0.04	Low	Low	Low
15	6	1.5	200	2	3	4.00	12.00	0.03	0.09	0.14	High	Medium	Medium
16	3	1.7	100	3	2	4.25	8.50	0.02	0.04	0.07	Low	Low	Low
17	6	1.6	100	4	2	6.93	13.87	0.06	0.12	0.19	High	Very High	High
18	4	1.1	100	7	1	6.88	6.88	0.04	0.04	0.04	Low	Low	Low
19	5	1	100	5	3	5.00	15.00	0.05	0.15	0.15	High	High	High
20	7	0.8	100	2	2	2.17	4.34	0.07	0.14	0.11	High	Medium	Medium
21	12	0.5	100	5	2	2.79	5.58	0.12	0.24	0.12	High	Medium	Medium
22	11	0.5	100	2	1	2.54	2.54	0.11	0.11	0.10	High	Medium	Medium
23	5	0.7	100	2	3	1.82	5.46	0.05	0.15	0.11	High	Medium	Medium
24	3	0.9	200	3	2	2.70	5.40	0.02	0.03	0.03	Low	Low	Low
25	6	1.2	100	4	2	5.20	10.40	0.06	0.12	0.14	High	Medium	Medium
26	2	1.5	100	7	1	6.75	6.75	0.02	0.02	0.03	Low	Low	Low
27	6	1.7	100	5	3	8.78	26.35	0.06	0.18	0.31	High	Very High	High
28	4	1.8	200	2	2	4.50	9.00	0.02	0.04	0.07	Low	Low	Low
29	5	1.3	100	5	2	6.50	13.00	0.05	0.10	0.13	High	Medium	Medium
30	7	2	100	2	1	5.43	5.43	0.07	0.07	0.14	Medium	Medium	Medium

The table represents the dataset inputs and outputs to and from the fuzzy systems. The Node No. represents the identity of the node with numbers like Node1, Node 2….etc. The N represents the number of communicating nodes to each node. Si represents the service time required for each communication packet. Z represents the think time for the node to initiate the communication packet or to serve a communication packet. Qi represents the address buffer size. Vi represents the number of visits initiated by a communicating node to each nodes for a transfer of communication packets. The node response time is represented by Ri and network response time by R. X represents the network throughput and Ci and Ui represents the node's capacity and utilization respectively.

The dataset represented with Node No., N, Si, Z, Vi and Qi are given as the inputs to the fuzzy controller. The dataset represented with R, Ri, X, Ci and Ui are derived as the outputs. These fuzzy controller output are defuzzified to obtain the membership value of Node's capacity, Node utilization and Node's trust value. The dataset example given in table 4 is the dataset used in a scenario with 30 nodes. Experimentations have been carried out for scenarios with 60 nodes, 90 nodes and 120 nodes. The results have been analyzed and plotted in graphical representations.

The fuzzy systems calculated the trust value of each node using the trust level derived from the node's capacity and utilization values. The ruleset generated is used in to correlate the degree of membership of node's capacity and utilization. The nodes with minimum degree membership or called "low" value of node capacity and utilization are concluded as selfish nodes and are isolated from the Auto-configuration process. The number of selfish nodes detected in each scenario is plotted as a graph given in Figure 4.

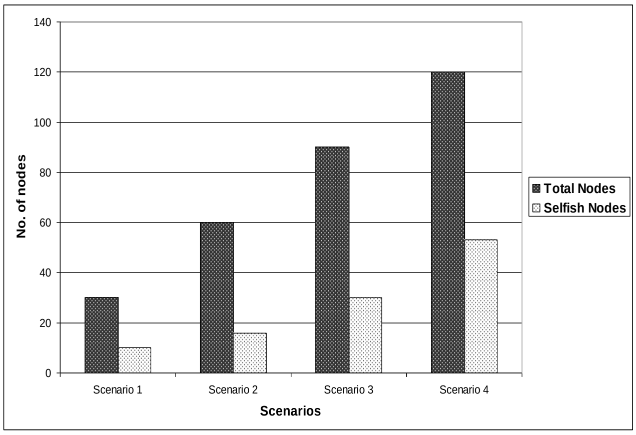


Figure 4. Selfish nodes isolated in each scenario

There is three degree of membership in trust values named low, medium and high. The nodes with low node capacity and node utilization are concluded as selfish nodes. All the other combinations of membership are concluded as medium or high trust level. But these nodes are not considered as selfish nodes. The trust value calculated and their degree of membership like low, medium and high has been analyzed. The degree of membership of each node in a scenario is analyzed and the total number of nodes in each membership category in each scenario has been plotted as a graph given in figure 5.

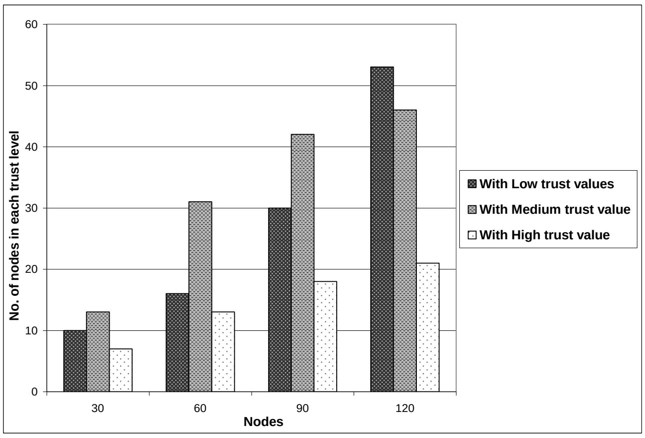


Figure 5. Degree of membership of MANET node’s trust value

Network throughput can be defined as the measure of the traffic flow through a network. Network throughput is constrained by various factors like the routing and switching protocols, capability of the networking devices and type of media for the communication. The networking throughput of a MANET is affected by poor routing, packet drops and due to resource constrains of the nodes. The dynamic distributed Stateful addressing protocol is integrated with the various routing protocols for configuring the new nodes. The network throughput of the MANET will be affected by the selfish nodes as it drop the routing and service packets. The network throughput of the MANET can be enhanced by isolating the selfish nodes from the network. The increased network throughput of a network is analyzed and the results are plotted in the figure 6.

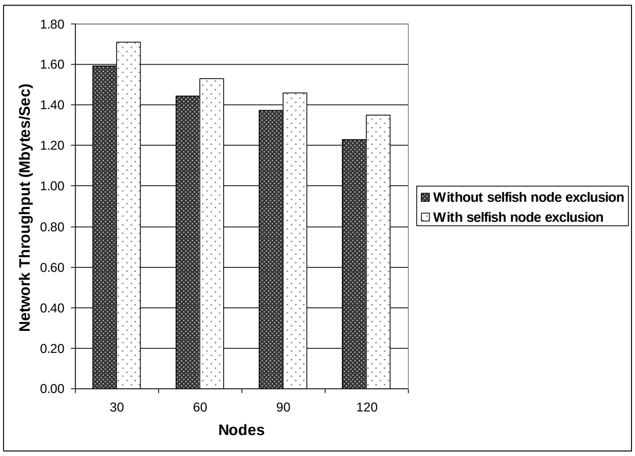


Figure 6.Network throughput before and after isolation of selfish nodes.

The Network throughput is expressed in terms of MBytes/Seconds. The values chosen for the input dataset is related to the real time traffic and hence the output values derived exactly matches the data values used for real time applications. Selfish nodes deteriorate the functioning of the routing protocols and other integrated service protocols. These nodes drop the routing packets or service packets intended to other nodes but are privileged by services offered by other nodes. The isolation of selfish nodes can reduce the packet drops during the functioning of the dynamic distributed Auto-configuration protocol an there by reduces the service acquisition delay. The packet drops caused by the selfish nodes are reduced by isolating those nodes. The packet drops caused by selfish nodes are only addressed in the algorithm. The packet drops before and after the isolation of the selfish nodes is analyzed and the results are plotted in figure 7.

Network Response time can be defined as the elapsed time between a communication request packet and a reply packet in a network. The network with minimum response time can execute a service faster when compared to the network with high response time. Network response time is expressed in milliseconds.

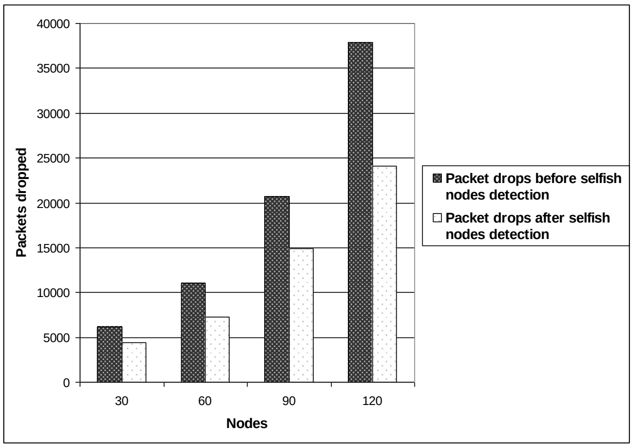


Figure 7. Packets dropped in a network before and after isolation of selfish nodes

There are four main factors affecting the MANET response time of a network. They are latency, network throughput, packets dropped and retransmissions. These factors are affected by the misbehaviors of the selfish nodes. So by isolating the selfish nodes in a network can reduce the factors affecting the network response. The analysis and results of the network response time before and after the isolation of selfish nodes is collected and plotted as graph in figure 8.

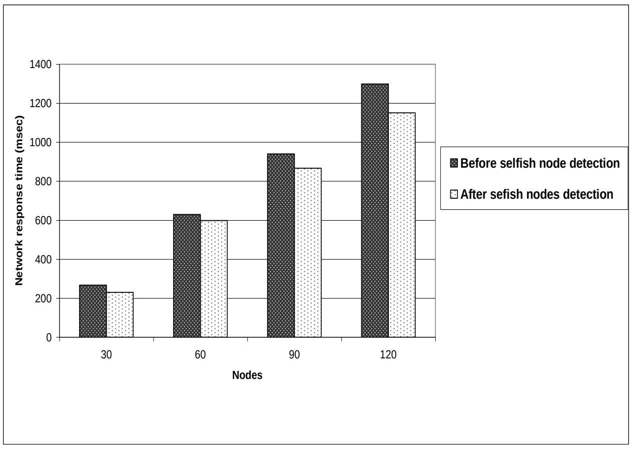


Figure 8. Comparison of network response time before and after isolation of selfish nodes

VII. Conclusion and Future Work

The network performance factors like the network throughput, network response time and packet drops are demonstrated using a fuzzy controlled system. It isolates selfish nodes during the function of the Dynamic Distributed Stateful Auto-configuration. The selfish nodes isolated by the fuzzy sets are based on ruleset used, that differs for each application of MANETs. If the MANET application is crucial, the ruleset generated must be too focused about the QoS and security of the network, but if the application is for entertainment the ruleset will not be too strict.

The fuzzy systems used in the proposed work ensure better identification of the selfish node because of its nature of identification using the continuous values between 0 and 1. The system is proved to enhance the various performance parameters in the network. The parameters like network throughput, network response time and packet drops are considered to compare the scenarios before and after isolating the selfish nodes. The systems have proved to improve the network throughput, and reduce the packet drops and network response time. The fuzzy based selfish node detection implemented in Dynamic Distributed Stateful Auto-configuration, can be extended and applied to various types of routing protocols to increase their performance during routing. The fuzzy system can also be extended to Stateless Auto-configuration during process of Duplicate Address Detection.

Acknowledgement

The authors are grateful to the Anna Centenary Research Fellowship(ACRF) grant for the support to carry out this research project. The proposed work is an enhancement of the paper published in World Congress on Information and Communication Technologies (WICT 2012) Proceedings [15].

References

[1] S. Cheshire, B. Aboba, and E. Guttman, “Dynamic Configuration of IPv4 Link-Local Addresses,” Internet Draft, July 2004.

[2] P. Patchipulusu, “Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks,” Master’s thesis, Texas A&M Univ, Aug. 2001.

[3] S. Nesargi and R. Prakash, MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network, IEEE INFOCOM, pp 1059 – 1068, June 2002.

[4] Matt W. Mutka, Hongbo Zhou, Lionel M. Ni, “Prophet address allocation for large scale MAolled NETs” , Ad Hoc Networks, Elsevier, 2003

[5] S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration,”, RFC 2462, Dec. 1998

[6] C. Perkins, J. Malinen, R. Wakikawa, E. Royer, and Y. Sun, “IP Address Autoconfiguration for Ad Hoc Networks,” Internet Draft, Nov. 2001.

[7] Mansoor Mohsin and Ravi Prakash, “IP Address Assignment in A Mobile Ad Hoc Network”, MILCOMM: Military Communication Conference Proceedings, pp. 1 – 6, 2002/

[8] Ilkyun Park, Namhi Kang, Ho Young Song,“Address Autoconfiguration for Hybrid Mobile Ad Hoc Networks”, Internet-Draft, MANET Autoconfiguration (AUTOCONF), 2007.

[9] K.Weniger, “PACMAN: Passive Auto-configuration for Mobile Ad Hoc Networks”, IEEE Journal on Selected areas in Communications, Vol. 23, No. 3, pp. 507 – 519, March 2005.

[10] N. Vaidya. ,Weak Duplicate Address Detection in Mobile Ad-hoc Networks, ACM MobiHoc, Lausanne, Switzerland,pp 206-216, June 2002.

[11] Mansi Ramakrishnan Thoppian and Ravi Prakash,” A Distributed Protocol for Dynamic Address Assignment in Mobile Ad Hoc Networks” IEEE Transactions On Mobile Computing, Vol. 5, No. 1, pp. 4 – 19, January 2006.

[12] Dongkyun Kim, Hong-Jong Jeong, C. K. Toh, and Sutaek Oh, “Passive Duplicate Address-Detection Schemes for On-Demand Routing Protocols in Mobile Ad Hoc Networks”, IEEE Transactions On Vehicular Technology, Vol. 58, No. 7, pp. 3558 – 3568, September 2009.

[13] Sanghyun Ahn, Yujin Lim “MANET Address Configuration using Address Pool”, Internet Draft, January 2011.

[14] K.Manousakis, A. McAuley, A. Misra and L.Wong, “Configuring an Entire Network with DCDP/DRCP”, Proceedings of 5th Advanced Telecommunications and Information Distribution Research Conference, College Park, March 2001.

[15] Reshmi.T.R, K.Murugan, “Trust based Dynamic Distributed IP addressing protocol for MANETs using Fuzzy rule set”, World Congress on Information and Communication Technologies (WICT 2012) Proceedings, pp – 931-936. November 2012.

[16] J. Bezdek, Fuzzy models – What are they, and why? IEEE Transactions on Neural Networks 1(1) (February 1993), 1–5.[17]

[17] Carlos J. Bernardos, Maria Calderon, Ignacio Soto, AnaBeatriz Solana, Kilian Weniger, "Building an IP-based community wireless mesh network: Assessment of PACMAN as an IP address autoconfiguration protocol", Elsevier, Journal on Computer Networks 54, pp. 291 – 303, August 2009.

[18] Yue-Bin Bai, Xuan Zhu, Xu Shao, Wen-Tao Yang , "FAST: Fuzzy Decision-Based Resource Admission Control Mechanism for MANETs", Mobile Networks Application, pp 758-770, July 2012.

Author Biographies

Reshmi.T.R received her Bachelor of Information Technology from SSM College of Engineering affiliated to Anna University and Master of Engineering in Computer Science and Engineering from Rajarajeswari Engineering college affiliated to Anna University, Chennai. She is currently pursuing research at Anna University. Her area of research is QoS and security issues in Mobile Ad-hoc networks

Murugan.K received his PhD degree under the Faculty of Information and Communication Engineering at Anna University, Chennai. He did his Master degree in Computer Science and Engineering, at National Institute of Technology (Formerly REC), Tiruchirapalli. He is currently working as Associate professor in Ramanujan Computing Centre, Anna University, Chennai, India. He is a life member of ISTE, IETE and CSI. His area of interest includes Mobile computing, MANETs and Wireless Sensor Networks