Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 2 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# A Novel Approach to Detect Malicious User Node by Cognition in Heterogeneous Wireless Networks

By G. Sunilkumar, Thriveni J, K. R. Venugopal & L. M. Patnaik
*Bangalore University, India*

*Abstract-* Cognitive Networks are characterized by their intelligence and adaptability. Securing layered heterogeneous network architectures has always posed a major challenge to researchers. In this paper, the Observe, Orient, Decide and Act (OODA) loop is adopted to achieve cognition. Intelligence is incorporated by the use of discrete time dynamic neural networks. The use of dynamic neural networks is considered, to monitor the instantaneous changes that occur in heterogeneous network environments when compared to static neural networks. Malicious user node identification is achieved by monitoring the service request rates generated to the cognitive servers. The results and the experimental study presented in this paper prove the improved efficiency in terms of malicious node detection and malicious transaction classification when compared to the existing systems.

*Keywords: cognitive networks, network security, OODA, dynamic neural networks, malicious node detection.*

*GJCST-E Classification : C.2.1*

# A Novel Approach to Detect Malicious User Node by Cognition in Heterogeneous Wireless Networks

G. Sunilkumar [α] , Thriveni J [σ] , K. R. Venugopal [ρ] & L. M. Patnaik [ω]

*Abstract-* Cognitive Networks are characterized by their intelligence and adaptability. Securing layered heterogeneous network architectures has always posed a major challenge to researchers. In this paper, the Observe, Orient, Decide and Act (OODA) loop is adopted to achieve cognition. Intelligence is incorporated by the use of discrete time dynamic neural networks. The use of dynamic neural networks is considered, to monitor the instantaneous changes that occur in heterogeneous network environments when compared to static neural networks. Malicious user node identification is achieved by monitoring the service request rates generated to the cognitive servers. The results and the experimental study presented in this paper prove the improved efficiency in terms of malicious node detection and malicious transaction classification when compared to the existing systems.

*Keywords: cognitive networks, network security, OODA, dynamic neural networks, malicious node detection.*

## I. Introduction

Now a day's Provisioning of security in networks has become challenge to researchers. The mechanisms currently employed are lack of adaptability to the unknown dynamic network conditions. The layered architecture adopted by the current network deployments lacking intelligent communication, lead to reduced network performance and unaware circumstances that arise at each level of the network architecture lead to reduced network performance. The amendments in the layered architecture are carried out post occurrences of problems or malicious activities. The need for secure intelligent and adaptable mechanisms is mandatory. Such mechanisms can be realized based on cognition loop or the OODA loop [1] [2]. Where the network conditions are observed, orientations and adoptions are achieved by intelligence, decisive actions are formulated and these decisions are applied to the network at the acting stage of the OODA loop. Such intelligent and adaptable networks are known as "Cognitive Networks" [3].

The cognitive network approach to secure networks from malicious user nodes or malicious activity is comparatively new and unique. Machine leaning techniques like fuzzy logic, self-organizing maps, neural networks can be used to incorporate intelligence into cognitive systems [4]. In this paper we introduce a discrete time dynamic neural network methodology to incorporate intelligence [5] [6]. Adoption of Cognition is based on the network metrics, parameters and patterns [7]. The cognitive network facilitates output in the form of certain actions that can be implemented for modifying the reconfigurable network policies, network components or network elements.

### a) *Difference between cognitive radio and cognitive network*

#### i. *Cognitive radio (CR)*

The Cognitive radio [1] (CR) is defined as "a radio that is aware of its environment or surroundings and adapts it intelligently". The cognition itself is an elusive quality which appears to be cognitive or intelligent prior to implementation is often dismissed as merely "adaptive" afterwards. A number of factors motivate CRs. CR is a transceiver system that is solely designed for using the best available wireless channel or resource in vicinity. Such kind of radio automatically detects the available bandwidth or spectrum resources and then it changes its transmission or reception parameters for permitting more synchronized wireless communication in a provided spectrum band even at the same location.

The need for cognition is driven by the complexity of the radio systems themselves. The existence of software defined radio (SDRs) capable of implementing a near endless number of different waveforms with different modulation schemes, power levels, error control codes, carrier frequencies, etc., means that controlling the radio becomes a problem of combinatorial optimization. Such problems are often computationally hard and lend themselves to solutions based on meta heuristic optimization methods based on simple search guided by higher level strategy. The application of such meta heuristic, which often appear to learn and innovate in turn, characteristic of work in artificial intelligence.

#### ii. *Cognitive Networks*

In order to achieve the seamless adaptation of radio link parameters, opportunistic use of underutilized spectrum, to get the higher flexibility in modulation and

*Author α σ ρ : Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. e-mail : sunil777g@gmail.com*
*Author ω : Indian Institute of Science, Bangalore, India.*

waveform Selection, the scientific or research society has seen an extraordinary progress in system or network development by implementing cognitive techniques. Cognitive Network is the best solution to attain the above mentioned requirements.

Cognitive Network [3] can be defined as an intelligent network encompassing the cognitive process which can perform a goal of achieving current network circumstances, planning, taking certain decision, acting on those perceived conditions, extracting or learning from the consequences of its previous or current actions, all while following end-to-end goals. The important component of cognitive network is its Cognition Loop that senses the circumstances, plans the actions to be taken and even according to input from sensors and network policies. It decides which solution or decision might be most effective for achieving end-to-end purpose. These characteristics facilitates the network systems to learn from the past about the situations, plans, decisions, actions and then using experiences for improving the decision in future.

### *b) Objectives*

In this paper, we have considered the use of cognition engines to identify the malicious users that are present within a heterogeneous network offering services. Malicious activity inducted through network transactions can be identified by monitoring the service request rates of the user's nodes [8] [9] [10]. In order to analyze effectively, instantaneously and to adapt the diverse network service rates, we introduce the discrete time dynamic neural network cognition engine. Access control mechanisms are critical in provisioning of network security. The proposed cognition mechanism considers the Physical Architecture Description Layer (PADL) structure for access control [11].

### *c) Organization*

This paper organization is as follows. Section two explains about literature survey. The background is discussed in the section three. The proposed system model is explained in section four. The Performance Evaluation and conclusions are discussed in the subsequent sections.

## II. Literature Survey

R.W. Thomas et al [3] provides the definition and introduction of "Cognitive Networks". In this research work, Software Adaptable Networks is considered to achieve cognition in networks. This paper also discusses a case study to demonstrate the concepts of cognitive networks based on the OODA Loop. The case study is targeted to maximize the time taken to connect between a source node and one or more destination nodes. The case study considers both multicast and unicast communication models. A network of learning automata is considered for the realization of the cognition layer. Finite Action Learning Automata is used to achieve cognition and the case study is compared with a non-cognition model Directional Reception Incremental Protocol [12]. The Finite Action Learning Automata achieves a $11\%$ performance improvement in solution finding. The major drawback of the algorithm proposed in this paper is that it is not applicable for link failures which occur in the real world scenario.

R S Komali et al [7] discuss about the effects of local and global information acquisition in cognitive networks. In this paper the cost of acquiring information, processing and network overheads arising from information accumulation is clearly discussed. The authors propose a Local $\delta$ Improvement Algorithm and compare it with the $\delta$ Improvement Algorithm [13] [14] and prove its efficiency. The authors of this paper conclude that utilizing both global and local information to achieve cognition, degrades system performance and an optimum global and local knowledge can be utilize to achieve cognition without effecting network performance. The major drawback is that there is no clear conclusion drawn as to the information global or local ratio to be considered to achieve cognition.

Daojing He et al [8] have proposed a trust based node misbehavior detection scheme for medical sensor networks. The trust is computed based on the rate of transmission and leaving time of the medical sensor nodes. Based on the trust computation malicious nodes are identified. The model is compared with $TrE$ [15] trust model.Performance improvement in terms of packet delivery and malicious node detection is proved using simulation and experimental test beds. The drawback of the system is that it is applicable to centralized systems supporting only unicast transmissions.

Tao Jun et al [9] developed an intrusion detection algorithm based on user behavior. Utilizing the statistics variance method based on the user nodes behavior in transmission rates the intrusions are detected. The paper also discusses the preventive measures incorporated in the case of Address Resolution Protocol [16] attacks. The algorithm proposed in this paper achieves a detection rate of about 0.9975 when compared to the system described in [17] which achieves a detection rate of about 0.9929. The authors have evaluated the proposed algorithm on the KDDCUP 1999 datasets [18] which has limited network user node features and is inconclusive.

S C Lingareddy et al [11] presented a paper that describes a mechanism for securing of wireless networks by the cognitive neural network approaches where the participating users are uniquely identified by implementing their respective Physical Architecture Description Layer (PADL) attributes. In this work they employ the certain data from Physical Layer and the Radio Layer in order to create the Physical Architecture

Description Layer (PADL), which is used to authenticate the system that tries to access the wireless network. Here the cognitive security manager (CSM) maintains the integrity of the entire network by analyzing the Physical Architecture Description Layer (PADL) of all the nodes within the network.

Zhang Wenzhu and Yi Bohai [19] have introduced a multi domain cognition system. The authors have proposed two cognition models namely a Local Single-Domain Cognitive approach and a Local Multi-Domain Cognition approach. A multidimensional edge detection theory [20] is adopted to achieve cognition in the Local Single-Domain Cognitive approach and similar concepts have been extended to achieve cognition in the Local Multi-Domain Cognition approach. Multi domain systems considered in this paper is defined in [21]. The concept of Local Multi-Domain Cognition approach is still very naive and can be further improved upon.

G Sunilkumar et al [22] presented a research work that not only Monitors activity of user node but also performs an effective function of taking preventive measures if user node transactions are found to be malicious. In this research work the intelligence in cognitive engine has been realized using self-organizing maps (CSOMs). In order to realize the CSOMs Gaussian and Mexican Hat neighbor learning functions have been evaluated. The research simulation made in this work proves the efficiency of Gaussian Learning function that is found to be better for cognition engine. The cognition engine being considered in this research work is evaluated for malicious node detection in dynamic networks. In this work the implemented concept results in higher Intrusion detection rate as compared to other similar approaches.

## III. Background

The authors in [11] have proposed a secure Cognitive Framework Architecture for 802.11 networks based on the OODA Loop. The core of the architecture i.e. the Cognitive Security Manager incorporates the cognition process using robust access control mechanisms based on the PADL. The authors of this paper adopt a similar access control mechanism to identify the nodes within the network. Intelligence to achieve cognition is realized using a multilayer feed forward neural network trained based on the back propagation algorithm. User behavior monitored and analyzed to achieve the Cognition Process. Access control mechanisms coupled with cognition processes is introduced. The use of Multilayer Feed Forward neural networks cannot effectively handle the network dynamics in heterogeneous environments and exhibits reduced malicious node detection. To achieve better malicious node detection rates the proposed model considers the use of discrete time dynamic neural networks to achieve cognition.

## IV. Proposed System Model

### *a) Cognitive Network Modelling*

Let's consider a network on which cognition is to be realized represented as $C_G^N$ . The cognitive network can be represented as a graph defined as

$$C_G^N = (C_E^N, C_L^N) \quad (1)$$

Where $C_L^N$ represents the set of network connections or links that exists between the network elements represented by $C_E^N$. The cognitive network element set consists of a set of cognitive servers represented as $C_S^N$, router elements set represented as $C_R^N$ and client nodes set represented as $C_C^N$. The network clients set constitute of wireless and wired type to realize a heterogeneous network. The network elements set can thus be defined as

$$C_E^N = \{C_S^N \cup C_R^N \cup C_C^N\} \quad (2)$$

All the links that constitute towards the link set $C_L^N$ are assumed to be bi-directional in nature and can of wired or wireless nature. A sample network graph is as shown in Figure 1.

The router set $C_R^N$ are assumed to be secure and are trusted network elements. The client nodes or the leafs of the network graph shown above and are assumed to constitute of trusted or normal users set represented as $C_n^N$ and malicious or untrusted users set represented as $C_m^N$. Hence the client node set can be defined as

$$C_C^N = \{C_n^N \cup C_m^N\} \quad (3)$$

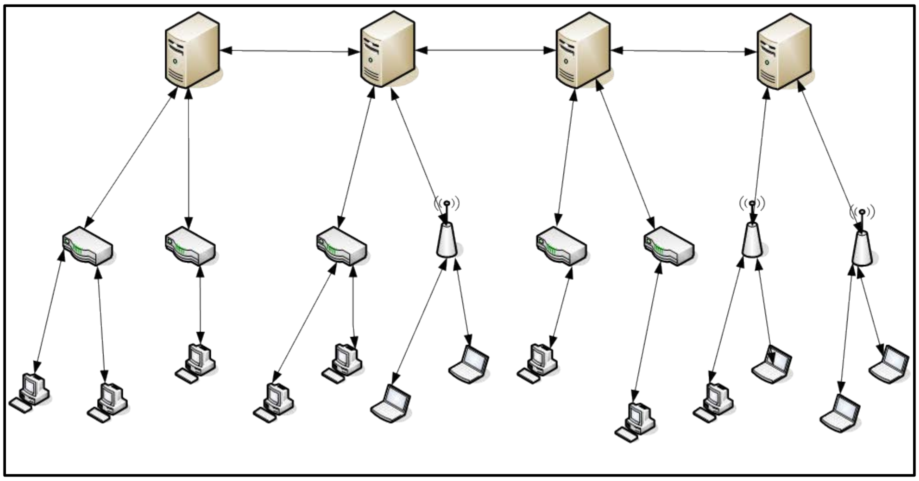

*Figure 1 :* Cognitive Network Model Graph

The objective of the cognitive network discussed here is to identify the number of malicious users $C^N_m$ in the cognitive network $C^N_G$. The cognitive server is assumed to host a set of services $S$ for the users to access.In the cognitive network model the routers set only forward the data received from the client nodes to the cognitive servers. Cognition is achieved by incorporation the Cognition Loop also known as the OODA Loop. The cognition process is carried out on the cognitive servers which intercommunicate to facilitate higher malicious user detection rates. A packet level communication model is considered in this system wherein the user nodes request for services using a packet based transmission system. The PADL based user identification approach is adopted for accurate identification of user nodes. User node behavior is observed based on the transmitted data and the transmission rate. Transmission rate is defined as

$$C^N_{ca\,x} = \frac{C^N_{Pk_x}}{t} \tag{4}$$

Where $C^N_{Pk_x}$ represents the transmitted packet set of user $x$ and $t$ is time interval.

The transmission rate of the data sent by $C^N_n$ to the cognitive server $C^N_S$ is assumed to vary between $0\,mbps$ and $C^N_{ca\,n}\,mbps$ . The malicious client nodes $C^N_m$ that are randomly deployed in the network are assumed to maintain a varying transmission rate of up to $C^N_{ca\,m}\,mbps$. The transmission rate of a user node is proportional to the quantum of service packets transmitted to the server per unit time. The bandwidth available with the cognitive server $C^N_S$ or the supported transmission rate is represented as $C^N_{S_{maxld}}$ .Normal nodes request for services $S$ offered by the $C^N_S$ at a rate $C^N_{ca\,n}$ and it can be stated that $C^N_{ca\,n} \ll C^N_{S_{maxld}}$ . Malicious activity is induced by introduction of additional packets into the network where by the transmission rate of the malicious node $C^N_{ca\,m} > C^N_{ca\,n}$. Malicious users in the ideal scenario try to compromise or attain control of a greater number of service hosts in order to perform untrusted activities. Such untrustworthy behavior is modeled by inducing additional service request packets and which can be observed by the incremental transmission rate. Identification of malicious users where in there is no increased injection of service packets is also considered.

User node activity in the cognitive network $C^N_G$ is observed by monitoring the service packet request rate measured in terms of the transmission rates of the service packets. Let the service transmission rate of a client node $x$ be represented as $C^N_{ca\,x}$ i.e. the observed service request rate of the cognitive server $C^N_S$ is also $\approx C^N_{ca\,x}$ assuming lower network losses. The cognitive process adopted relies on dynamic neural network based intelligence for analysis of the service request packets. A discrete time dynamic neural network is adopted for orientation of the cognitive process incorporated. The decision phase of the cognition cycle relies on the service request packet analysis results obtained from the output of the dynamic neural networks. The action or the control strategies phase of the cognition cycle is achieved based on the decisions and is implemented on the cognitive servers $C^N_S$ . The algorithm adopted to implement the action is discussed in the latter section of this paper. The cognition cycle is represented in Figure 2.

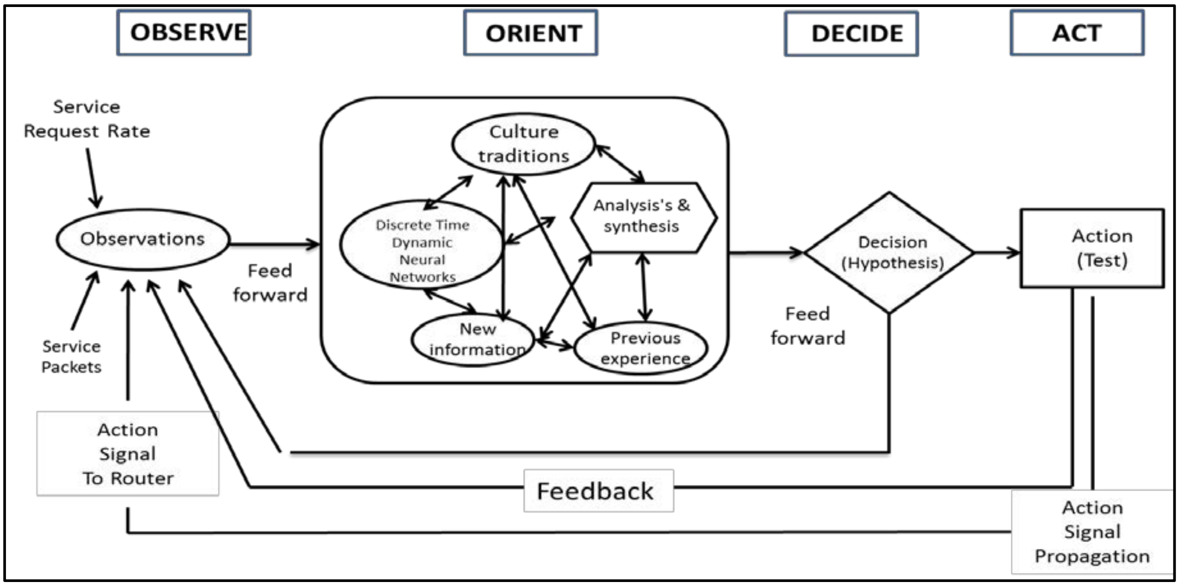

*Figure 2 :* Cognition Cycle

*b) Discrete Time Dynamic Neural Network*

Dynamic Neural networks [23] are adopted to impart intelligence similar to that of the biological neuron. The cognition process discussed in this paper adopts a discrete time dynamic neural network model for the purpose of understanding and learning about the user node behavior in terms of the service request packets received by the cognitive server $C_S^N$ . The back propagation algorithm is adopted for the training of the dynamic neural network. The network dynamics of the client nodes to be observed can be represented as a first order differential equation defined as

$$\frac{\Delta x}{\Delta t}\Big|_{t=kt} = \frac{x\big((k+1)T\big)-x(x(kT))}{T} \tag{5}$$

Where the sampling period is represented by $T$ and $k$ Represents the instance of sampling and $x(y)$ is the input service requests to be observed by the cognitive server $C_S^N$ at the $y^{th}$ time instance.

The client node behavior to be observed can also be defined as

$$\frac{\Delta x}{\Delta t} = x(k+1) - x(k) \tag{6}$$

When $T = 1$

The discrete time dynamic neural network unit can be graphically represented as shown in Figure 3 given below.

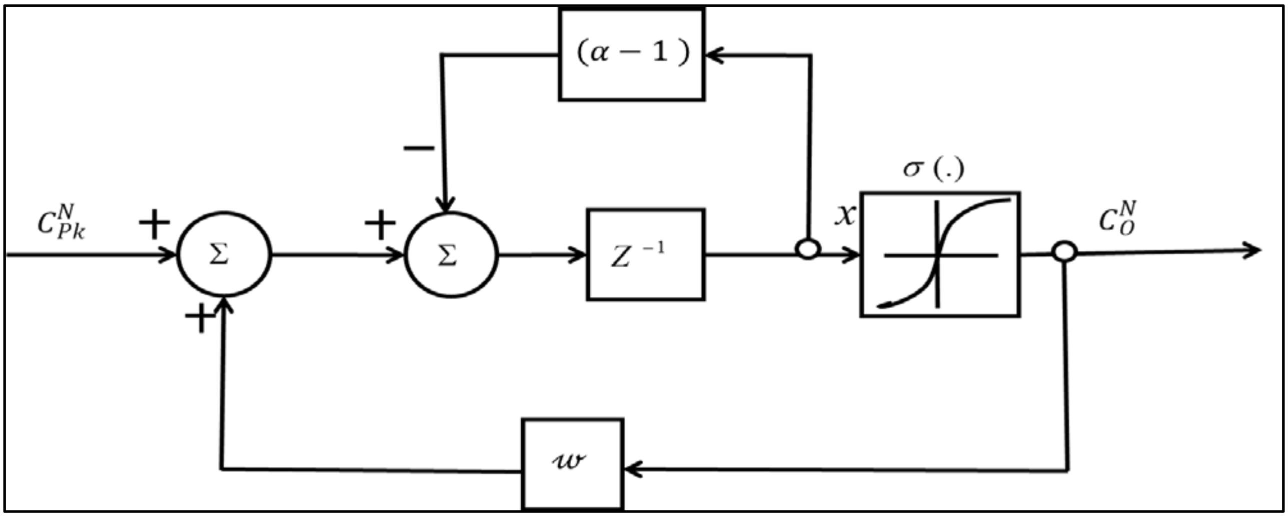

*Figure 3 :* A neuron structure of the Discrete Time Dynamic Neural Network

From Figure 3 the equivalent model of the discrete time dynamic neural network can be represented as

$$x(k+1) = \Big(\big(C_{Pk}^N\big) + \,(w \times C_O^N(k)) - \big((\alpha-1)(x(k))\big)\Big) \tag{7}$$

The output of the dynamic neural networks is the learning or the cognitive observations represented as $C_O^N(k)$ is defined as

$$C_O^N(k) = \sigma \times (x(k)) \tag{8}$$

Considering a set of service packets transmitted from the user nodes in the topology represented as$x_d(k)$. Where $k = 1,2,3,4, \ldots \ldots P$. The learning algorithm of the dynamic neural network can be defined as

$$x(k+1) = \left( (C_{Pk}^N) + f(x(k), w) - \left( (\alpha - 1)(x(k)) \right) \right) \tag{9}$$

Where,

$$f(x(k), w) = \sum_{i=1}^{p} \alpha_i \sigma(b_i x + c_i) = \alpha^T \sigma(bx + c) \tag{10}$$

The learning error of the neural network model is defined as

$$E(k) = \frac{1}{2}(x_d(P) - x(P))^2 + \frac{1}{2}\sum_{k=0}^{P-1}[x_d(k) - x(k)]^2 \tag{11}$$

Considering

$$e(k) = x_d(k) - x(k) \text{ and}$$

$$e(P) = x_d(P) - x(P)$$

The learning error can be defined as

$$E(k) = \frac{1}{2}e^2(P) + \frac{1}{2}\sum_{K=0}^{P-1} e^2(k) \tag{12}$$

Based on the parameters $\alpha$ the partial derivatives of the error index is defined as

$$\frac{\partial E}{\partial \alpha} = -(\sum_{k=0}^{P-1} z(k+1)x(k)) \tag{13}$$

Where $z(k+1)$is the Lagrange multiplier.

Based on the weight parameter $w$ the partial derivatives of the error index is defined as

$$\frac{\partial E}{\partial w} = \sum_{k=0}^{P-1} z(k+1) f_w(x(k), w) \tag{14}$$

Where $z(k+1)$is the Lagrange multiplier.

The dynamic neural networks increments the parameters $\alpha$ and the weight $w$ to minimize the learning error. The rate at which $\alpha$ is incremented represented as $\Delta\alpha(k)$ is defined as

$$\Delta\alpha(k) = -\left(\eta_\alpha \frac{\partial E}{\partial \alpha}\right) \tag{15}$$

$$\Delta\alpha(k) = \eta_\alpha \sum_{k=0}^{P-1} z(k+1)x(x) \tag{16}$$

The weight update rate is represented as $\Delta w(k)$ is defined as

$$\Delta w(k) = -\left(\eta_w \frac{\partial E}{\partial w}\right) \tag{17}$$

$$\Delta w(k) = -\eta_w \sum_{k=0}^{P-1} z(k+1) f_w(x(k), w) \tag{18}$$

The dynamic neural networks update the parameters$\alpha$ and $w$ of the forward layers based on the following definitions

$$\alpha(k+1) = \alpha(k) + \eta_\alpha \sum_{k=0}^{P-1} z(k+1)x(k) \tag{19}$$

$$w(k+1) = w(k) + \eta_w \sum_{k=0}^{P-1} z(k+1) f_w(x(k), w) \tag{20}$$

The back propagation learning for the discrete time dynamic neural network model enables to observe the service packet transmission rates of the cognitive server $C_S^N$ by adopting a multi iterative process. The observations of the neural network are utilized for decision making and action planning at the cognitive servers $C_S^N$.

### c) *Cognitive Decision Making and Action Planning*

In this section we propose an action control adopted to limit the service request rates to the cognitive server $C_S^N$. Let $p_{dat}$ represent a fraction of the service request packet set from the users to the server through the routers i.e. $0 \leq p_{dat} \leq 1$. By dropping or limiting the service requests received from the $C_m^N$ cognition could be achieved. Let the packet dropping factor which is multiplicative in nature be represented as $\mu$. The packet dropping factor is adapted based on the presence of malicious users identified in the network topology. Let us define a constant $r$ that is additive in nature and is introduced to increase the acceptance of service request packets when the number of normal users are greater i.e. $C_n^N > C_m^N$. The action control strategy is realized by the cognitive server set $C_S^N$ and is executed when the service requests rates observed exceed the limit of the maximum transmission limit $C_{S_{maxld}}^N$ or when the current service request limit drops beyond the minimum supported transmission bandwidth $C_{S_{minld}}^N$. The service requests received by the server are monitored every $u$ second. Here $u$ is the monitoring time interval is considered to smaller than the round trip time between the server $C_S^N$and the user nodes $C_C^N$. The action control mechanism is not just as it tends to drop or limit the user service request immaterial of the kind of user $C_n^N$or $C_m^N$ based on the observations $C_O^N$. To eliminate such unjust actions let us consider the service request rate of the cognitive server $C_S^N$ received to be represented as $C_{ca\,C_S^N}^N$ and it is defined as

$$C_{ca\,C_S^N}^N = \frac{\left(C_{S_{minld}}^N + C_{S_{maxld}}^N\right)}{p_{dat}(h)} \tag{21}$$

Where $p_{dat}(h)$ represents a constant and is a fraction of the service request packets sent from $C_C^N$to $C_S^N$.

If the service request load $C_{ca\,C_{ca}^N}^N$ is below the predetermined threshold $C_{S_{minld}}^N$ then the service request acceptance is increased by a small volume represented as $\delta$. The cognitive servers monitor and accept the client service requests through the controlled router represented as $C_R^N(h)$. This action control strategy is invoked every $u$ second wherein the server load $C_{ca\,C_S^N}^N$ is adjusted to be within the limits set by $C_{S_{minld}}^N$ and $C_{S_{maxld}}^N$

based on the observation $C_O^N$. From the discussion presented here it is clear that the action control strategy adopted in the cognition cycle is designed to balance and service the user request for services $S$ offered by the server $C_S^N$ limiting the service requests from malicious users $C_m^N$ and not effecting the normal user $C_n^N$ service requests by a great extent. It is observed that the action control strategy in the cognitive process is a feedback based strategy. The observed service rates $C_O^N$ of the client nodes $C_C^N$ by the dynamic neural networks enables effective decision making and control strategies to be adopted to achieve cognition. The cognition process discussed is capable of handling service rate controls between the predefined limits, heterogeneous client nodes, heterogeneous service traffic rates and server bandwidth control limits established by $C_{S_{maxld}}^N$ , $C_{S_{minld}}^N$ .

The integrity and security provisioning of cognitive server $C_S^N$ and the services $S$ it offers is considered as the objective of the research work presented here. Let the clients $C_C^N$ induce service requests i.e. the traffic load be represented as $D_r(t)$ through router $r$ has for $C_S^N$ at the time $t$ . The action strategy signal represented as $C_{sig}^N(t)$ is considered as the response to the observed traffic $C_O^N$ by the server $C_S^N$, the instantaneous response traffic rate is represented by $D_r'\ \ (t)$. The rate $D_r'\ \ (t)$is considered as a function of the controlled traffic rate $C_{ca_r}^N(t)$ and the offered traffic rate $D_r(t)$ in accordance to the action control strategy. The total traffic rate observed by the cognitive server $C_S^N$ is defined as

$$\sum_{r=1}^{C_C^N} D_r'\ \ (t) \tag{22}$$

Where $D_r'\ \ (t)$is the traffic rate through each deployment router $C_R^N(h)$

Based on the total traffic observed and the discrete time dynamic neural network analysis the $C_S^N$ orients itself and the orientation results is defined as

$$C_O^N = \sigma\left(\sum_{r=1}^{C_C^N} D_r'\ \ (t)\right) \tag{23}$$

The $C_O^N$ is utilized for decision making and the action strategies signal $C_{sig}^N(t)$ is derived for all the routers in $C_R^N(h)$ in the heterogeneous network environment. Based on the position and the link type the action signal is received at varied time instances due to inherit network delays. Let $\rho_r\ \geq 0$ represent the network delay from the $C_S^N$ to the routers $C_R^N$. The action signal $C_{sig}^N(t)$, the controlled traffic rate $C_{ca_r}^N(t)$ and the traffic rates $D_r'\ \ (t)$ change with respect to the time $t$ and be considered as a coupled system. Coupled Differential equations can be used to represent such models.

The cognitive server needs to maintain the traffic rate within the limits established by $C_{S_{minld}}^N$ , $C_{S_{maxld}}^N$ and yet generate action signals $C_{sig}^N(t)$ defined as

$$C_{sig}^N(t) = \begin{Bmatrix} -1 & \text{if } \sum_{r=1}^N D\ \ '_r(t) \geq C_{S_{maxld}}^N \\ 0 & \text{if } \sum_{r=1}^N D\ \ '_r(t) \leq C_{S_{minld}}^N \\ 1 & \text{otherwise} \end{Bmatrix} \tag{24}$$

Let the action signal $C_{sig}^N(t)$ of the cognitive server $C_S^N$ based on the service request rate $C_{ca_S}^N(t)$ such that $C_{S_{minld}}^N < C_{ca_S}^N(t) < C_{S_{maxld}}^N$ , the additive step $\delta > 0$. The changes in the action signal can be defined as

$$\frac{\Delta C_{ca}^N(t)}{\Delta t} = \left(\delta 1_{\left(C_{sig}^N(t-\rho_r)==1\right)}\right) - \left(\frac{C_{ca}^N(t)}{2} 1_{\left(C_{sig}^N(t-\rho_r)==-1\right)}\right) \tag{25}$$

To maintain quality and service provisioning to normal user clients $C_n^N$ in the presence of malicious users $C_m^N$ the cognitive server $C_S^N$ increases the instantaneous service request rate $C_{ca}^N(t)$ by a factor $\delta > 0$ when the cumulative service request rate is less than $C_{S_{minld}}^N$ or it reduces the rate by half if the instantaneous service request rate is greater than $C_{S_{maxld}}^N$ . The dynamic changes in the transmission rates $D\ \ _r(t)$ can be defined as

$$\frac{\Delta D\ \ '_r(t)}{\Delta t} = min\left\{C_{ca}^N(t-\rho_r)\,,\ D\ \ _r(t) - D\ \ '_r(t)\right\} \tag{26}$$

Where $D\ \ '_r(0) = 0$

From the above definition it is clear that request rate $D\ \ '_r(t)$ is a function of the offered request rate $D_r(t)$ and the altered rate $C_{ca}^N(t-\rho_r)$ achieved based on cognition.

At a time instance $\rho_0$, the cognitive server $C_S^N$ observes the received traffic is greater than $C_{S_{maxld}}^N$ it is said to be over-loaded. The request rate observed is defined as

$$C_{ca_S}^N(t) = \Theta_1 e^{-\frac{t}{2}} \tag{27}$$

Where $t \geq \rho_0$

$\Theta_1 = e^{(1/2)\rho_0} C_{ca_S}^N(\rho_0)$ is a constant

$C_{ca_S}^N(\rho_0)$Is the request rate at time instance $\rho_0$

Then the rate at which the over-loaded cognitive server receives request rates id defined as

$$D_r{'}(t) \approx e^{-t}\left[e^{\rho_0} D_r{'}(\rho_0) - \frac{2\mu\Theta_r}{D_r\ \ (t)}\sqrt{\Theta_r^2 D_r^2(t) e^{\rho_0}} + \frac{2\mu\Theta_r}{D_r\ \ (t)}\sqrt{\Theta_r^2 D_r^2(t) e^{t}}\right] \tag{28}$$

At a time instance $\rho_0$, the cognitive server $C_S^N$ observes the received traffic is less than $C_{S_{minld}}^{N}$ it is said to be under-loaded. The request rate observed is defined as

$$C_{ca\,S}^{N}(t) = \delta t + \Theta_2 \qquad (29)$$

Where $t \geq \rho_0$

$\Theta_2 = -\delta\rho_0$ is a constant

Then the rate at which the under-loaded cognitive server receives request rates id defined as

$$D_r^{'}\ (t) \approx \left(\left[D_r^{'}(\rho_0)e^{\rho_0} - \mu D_r\ (t)e^{\rho_0} + \mu D_r\ (t) \times \frac{e\left[1-\delta/D_r(t)\right]\rho 0\, e^{-(\Theta_r/D_r(t))}}{\left(1-\frac{\delta}{D_r(t)}\right)}\right] e^{-t}\right) + \left(\mu D_r\ (t)\left[1 - \frac{-e^{-(\delta t+\Theta_r)/D_r(t)}}{\left(1-\frac{\delta}{D_r(t)}\right)}\right]\right) \qquad (30)$$

The cognition is achieved based on the OODA loop. The service requests received from the malicious users $C_m^N$ are limited and dropped to achieve cognition and maintain the heterogeneous network integrity. The cognition process discussed derives its learning intelligence by using the discrete time dynamic neural networks trained using the back propagation algorithm. The experimental study conducted to prove the discussed cognition process is explained in the next section.

## V. Performance Evaluation

This section of the paper discusses the experimental study conducted to evaluate the cognition process based on the OODA Loop. The experimental environment for the heterogeneous environment $C_E$ test bed was developed using C# on the Visual Studio Platform. The heterogeneous environment constitutes of cognitive servers $C_S$ routers $C_R$ and client nodes $C_C$. Cognitive decision making is incorporated within the cognitive servers. We have evaluated the proposed discrete time dynamic neural network cognitive engine (DNN-DT) against the MFNN cognitive engine. The $C_C$ considered of wired and wireless type. We have considered two mobility models namely, Random Directional Mobility and Random Waypoint Mobility for the user nodes $C_C$. The user nodes $C_n^N$ introduce regular service rates over the simulation test bed within the limits set by $C_{S_{minld}}^{N}$ and $C_{S_{maxld}}^{N}$ and request the cognitive servers for a set of services through the routers deployed. A packet level structure is adopted to model such transactions. A random number of nodes i.e. malicious nodes $C_m^N$ are introduced intro the network whose transactional service rates are irregular by nature i.e. $C_{ca\,m}^{N} > C_{ca\,n}^{N}$. The aim of the experimental study can be defined as identifying malicious transactions due to which irregular service rates are observed and negate the malicious client nodes $C_m^N$ introducing such service rates by denying them service provisioning.

The ability of the simulation environment is to handle variations in the number of $C_S$, $C_R$ , $C_C$ along with the mobility options and channel noise considerations led to an extensive experimental scenarios summarized in Table 1. A total of twenty four scenarios are presented in this paper. The error in identifying the malicious nodes identified by the vibrational service rates is represented in Figure 4. The average detection error for the MFNN Cognitive Engine was found to be around $16.266\%$ when compared to a detection error of about $4.411\%$ of the DNN-DT Cognitive Engine. Network transactional errors are inherit to any networks. Network transactional errors are generally due to packet loss and channel noise. The network transactional errors observed for the simulation scenarios are shown in Figure 5. From the graph it is clear that the network transactional errors are uniform for the MFNN Cognitive Engine and DNN-DT Cognitive Engine scenarios reiterating the fairness of the results are presented in this paper. Network Transactional errors result in misclassification of client nodes increasing the False Positive Rate (FPR). The occurrence of such scenarios is controlled during test bed deployments for all the scenarios presented here.

*Table 1 :* Considered Simulation Scenarios

| No. | Cognition Engine | No. Servers $(C_S)$ | No. Routers $(C_R)$ | Mobility Model | Channel Noise | No. Nodes $(C_C)$ | No. Malicious Nodes( $C_m^N$) |
|---|---|---|---|---|---|---|---|
| 1 | MFNN COGNITIVE ENGINE | 3 | 30 | RANDOM DIRECTIONAL | PRESENT | 200 | 13 |
| 2 | MFNN COGNITIVE ENGINE | 3 | 30 | RANDOM DIRECTIONAL | ABSENT | 200 | 9 |
| 3 | MFNN COGNITIVE ENGINE | 3 | 30 | RANDOM WAYPOINT | PRESENT | 200 | 5 |
| 4 | MFNN COGNITIVE ENGINE | 3 | 30 | RANDOM WAYPOINT | ABSENT | 200 | 5 |
| 5 | MFNN COGNITIVE ENGINE | 5 | 50 | RANDOM DIRECTIONAL | PRESENT | 200 | 11 |
| 6 | MFNN COGNITIVE ENGINE | 5 | 50 | RANDOM DIRECTIONAL | ABSENT | 200 | 14 |
| 7 | MFNN COGNITIVE ENGINE | 5 | 50 | RANDOM WAYPOINT | PRESENT | 200 | 10 |
| 8 | MFNN COGNITIVE ENGINE | 5 | 50 | RANDOM WAYPOINT | ABSENT | 200 | 13 |
| 9 | MFNN COGNITIVE ENGINE | 7 | 70 | RANDOM DIRECTIONAL | PRESENT | 200 | 23 |
| 10 | MFNN COGNITIVE ENGINE | 7 | 70 | RANDOM DIRECTIONAL | ABSENT | 200 | 5 |
| 11 | MFNN COGNITIVE ENGINE | 7 | 70 | RANDOM WAYPOINT | PRESENT | 200 | 14 |
| 12 | MFNN COGNITIVE ENGINE | 7 | 70 | RANDOM WAYPOINT | ABSENT | 200 | 7 |
| 13 | DNN-DT COGNITIVE ENGINE | 3 | 30 | RANDOM DIRECTIONAL | PRESENT | 200 | 11 |
| 14 | DNN-DT COGNITIVE ENGINE | 3 | 30 | RANDOM DIRECTIONAL | ABSENT | 200 | 7 |
| 15 | DNN-DT COGNITIVE ENGINE | 3 | 30 | RANDOM WAYPOINT | PRESENT | 200 | 8 |
| 16 | DNN-DT COGNITIVE ENGINE | 3 | 30 | RANDOM WAYPOINT | ABSENT | 200 | 6 |
| 17 | DNN-DT COGNITIVE ENGINE | 5 | 50 | RANDOM DIRECTIONAL | PRESENT | 200 | 9 |
| 18 | DNN-DT COGNITIVE ENGINE | 5 | 50 | RANDOM DIRECTIONAL | ABSENT | 200 | 8 |
| 19 | DNN-DT COGNITIVE ENGINE | 5 | 50 | RANDOM WAYPOINT | PRESENT | 200 | 8 |
| 20 | DNN-DT COGNITIVE ENGINE | 5 | 50 | RANDOM WAYPOINT | ABSENT | 200 | 7 |
| 21 | DNN-DT COGNITIVE ENGINE | 7 | 70 | RANDOM DIRECTIONAL | PRESENT | 200 | 15 |
| 22 | DNN-DT COGNITIVE ENGINE | 7 | 70 | RANDOM DIRECTIONAL | ABSENT | 200 | 5 |
| 23 | DNN-DT COGNITIVE ENGINE | 7 | 70 | RANDOM WAYPOINT | PRESENT | 200 | 11 |
| 24 | DNN-DT COGNITIVE ENGINE | 7 | 70 | RANDOM WAYPOINT | ABSENT | 200 | 7 |

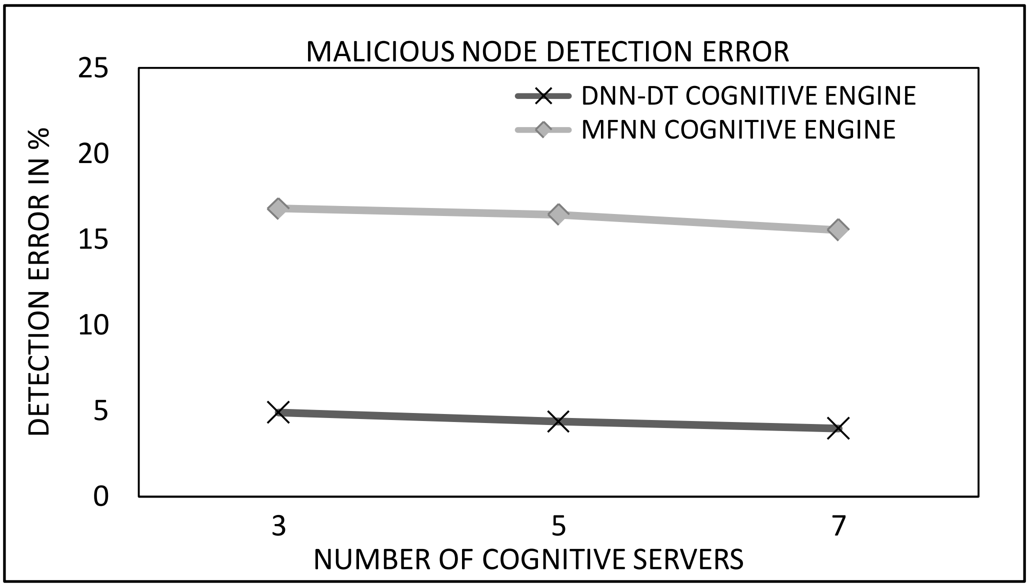

*Figure 4 :* Malicious Node Detection Error vs. Number of Cognitive Servers

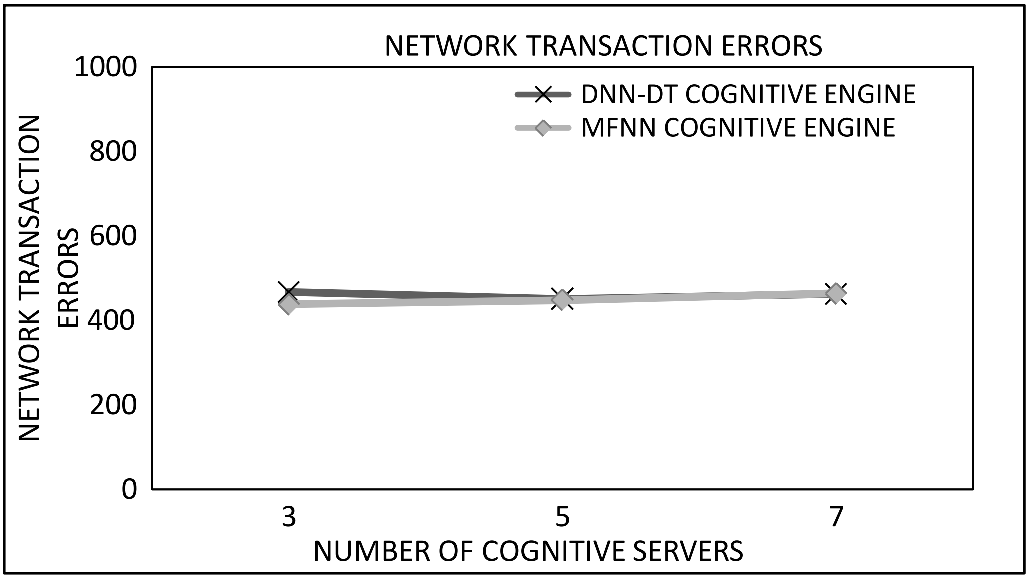

*Figure 5 :* Network Transaction Errors vs. Number of Cognitive Servers

It is observed that the DNN-DT cognitive engine reduces the malicious node detection error by about 25% when compared to the MFNN cognitive engine. The discrete time dynamic neural networks adapt quickly to the dynamic environments presented here. This ability of the discrete time dynamic neural network results in reduced network overheads in action planning and decision making phase of the OODA Loop. The network overheads observed are shown in Figure 6 and Figure 7 given below. The network overheads are measured in terms of the additional query transactions induced by the cognitive servers for accurate decision making. It was observed that about 12064, 19686 and 28865 transactional packets were reduced when considering the discrete time dynamic neural network to achieve cognition for the 3, 5 and 7 server scenarios. From Figure 7 it can be observed that the average reduction of about 2% was achieved considering an average of all the network transactions considered for the varied scenarios discussed in this section. Though the reduction in the average network overhead appears marginal, its significance increases for larger network scenarios.

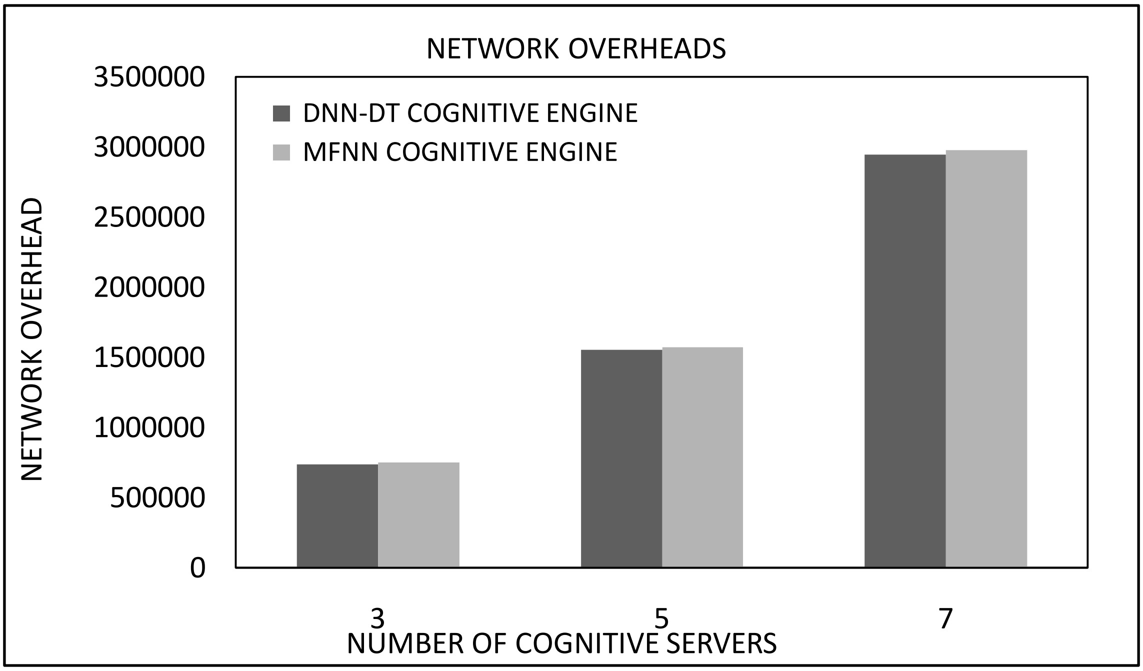

*Figure 6 :* Network Overheads vs. Number of Cognitive Servers

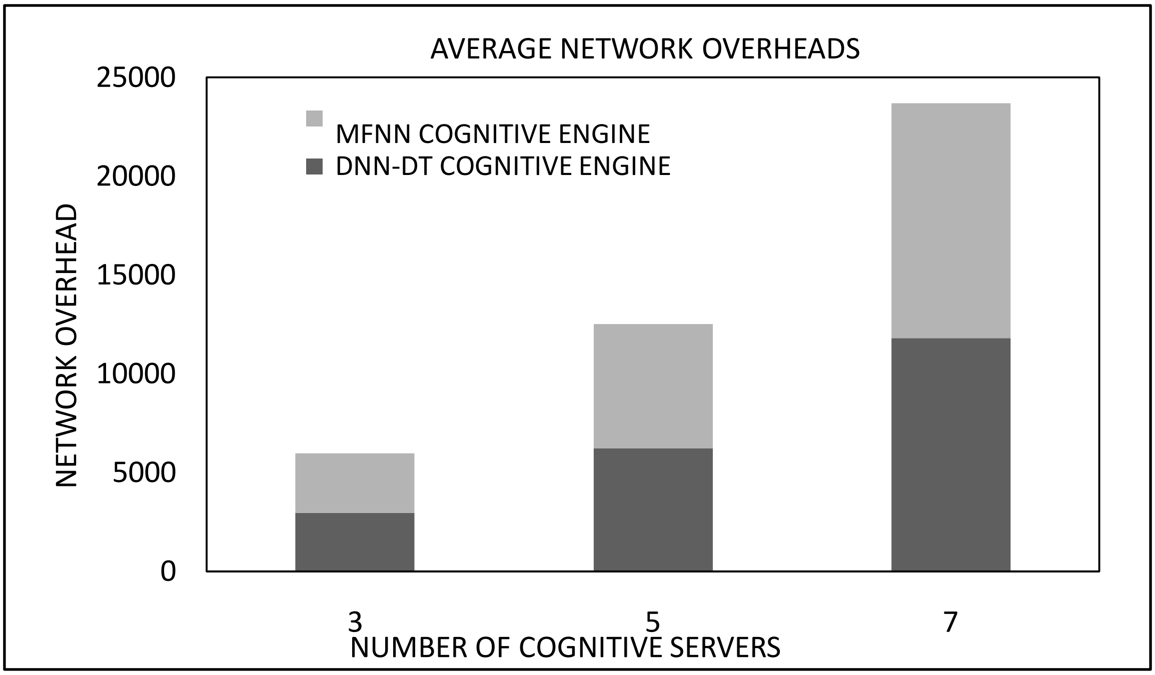

*Figure 7 :* Average Network Overheads vs. Number of Cognitive Servers

The receiver operating characteristic curve for 3, 5 and 7 server's scenarios have been studied and the efficiency of malicious node detection of the MFNN cognitive engine and the DNN-DT cognitive engine is shown in Figure 8. From the figure the average malicious node detection efficiency of the MFNN cognitive engine is about 0.83 when compared to 0.95 malicious node detection efficiency of the DNN-DT cognitive engine. It can also be observed that, as the number of cognitive servers increases, the detection efficiency of the cognition engine also increases.

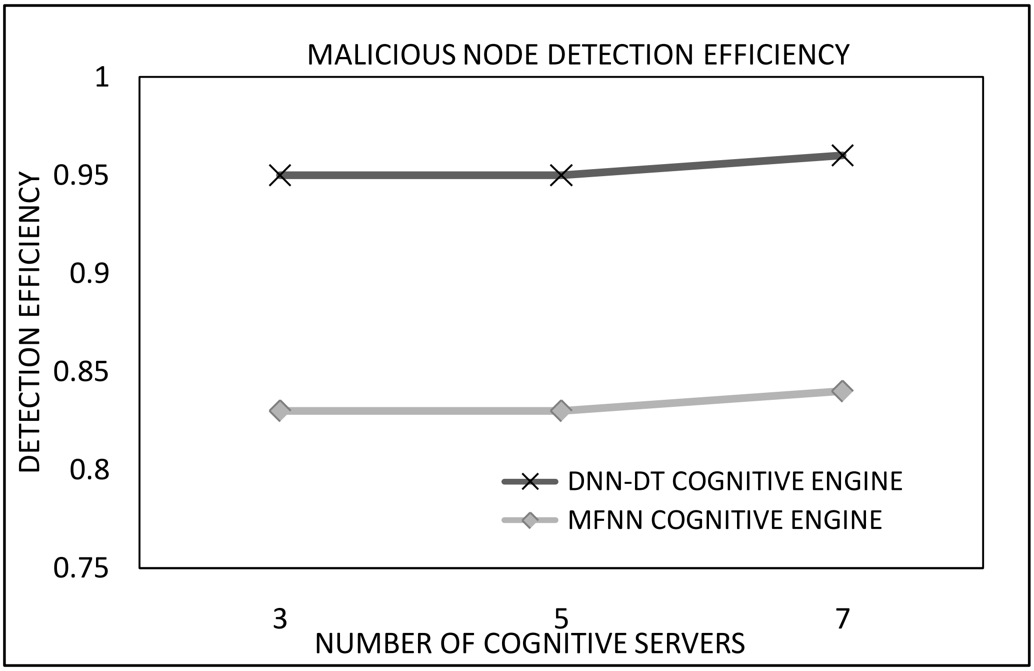

*Figure 8 :* Malicious Node Detection Efficiency vs. Number of Cognitive Servers

The variations in service rates $C_{ca}^{N}{}_{C_S^N}$ observed at the cognitive server $C_S^N$ based on the network transactions enables to identify the malicious nodes $C_m^N \in C_C$ . The classification accuracy of network transaction is critical to achieve higher malicious node identification. The malicious transaction classification accuracy based on the receiver operating characteristic is shown in Figure10 given below. From the figure it is clear that the malicious transaction classification accuracy of the discrete time dynamic neural networks is 12% better than MFNN cognitive engine.

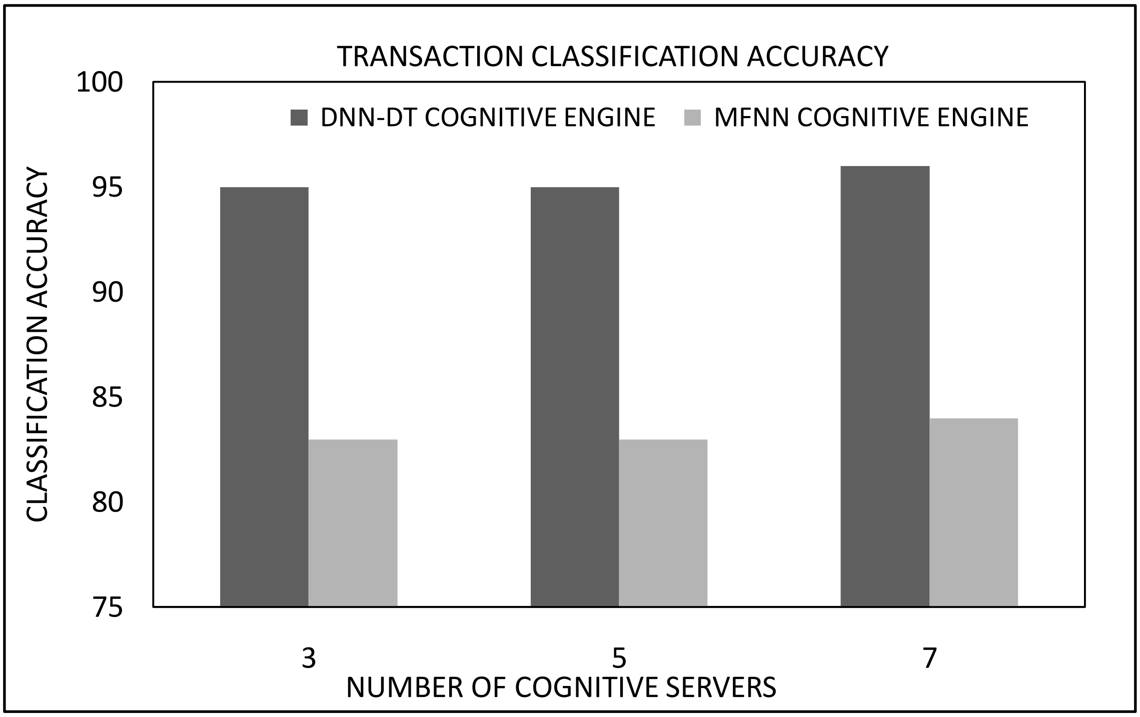

*Figure 8 :* Transaction Classification Accuracy vs. Number of Cognitive Servers

To study the effect of user node mobility let us consider a cognitive network constituting of seven cognitive servers. The experimental study conducted for this scenario can be summarized from the data tabulated and represented in Table 2. The effect of user mobility and channel noise on malicious user node detection accuracy for $C_S^7$ is shown in Figure 10. From the figure it is clear that the channel noise inclusion reduces the malicious node detection accuracy. The DNN-DT cognitive engine achieves an average detection accuracy of about 96.02% when compared to 84.45% detection accuracy achieved by the MFNN Cognitive engine. The accuracy of malicious node detection for random directional mobility is observed to be less than that of the random waypoint mobility model by about 0.297% and 0.375% for MFNN cognitive engine and DNN-DT cognitive engine.

*Table 2 :* Simulation Scenarios Considering Seven Cognitive Servers ($C_S^7$).

| Cognition Engine | No. Of Nodes | Mobility Model | Channel Noise | No. Of Malicious Nodes | Detection Error (%) |
|---|---|---|---|---|---|
| MFNN COGNITIVE ENGINE | 200 | RANDOM DIRECTIONAL | PRESENT | 23 | 15.85388007 |
| MFNN COGNITIVE ENGINE | 200 | RANDOM DIRECTIONAL | ABSENT | 5 | 15.54081344 |
| MFNN COGNITIVE ENGINE | 200 | RANDOM WAYPOINT | PRESENT | 14 | 15.55681133 |
| MFNN COGNITIVE ENGINE | 200 | RANDOM WAYPOINT | ABSENT | 7 | 15.2442622 |
| DNN-DT COGNITIVE ENGINE | 200 | RANDOM DIRECTIONAL | PRESENT | 15 | 4.276987201 |
| DNN-DT COGNITIVE ENGINE | 200 | RANDOM DIRECTIONAL | ABSENT | 5 | 4.042841339 |
| DNN-DT COGNITIVE ENGINE | 200 | RANDOM WAYPOINT | PRESENT | 11 | 3.93334491 |
| DNN-DT COGNITIVE ENGINE | 200 | RANDOM WAYPOINT | ABSENT | 7 | 3.636929 |

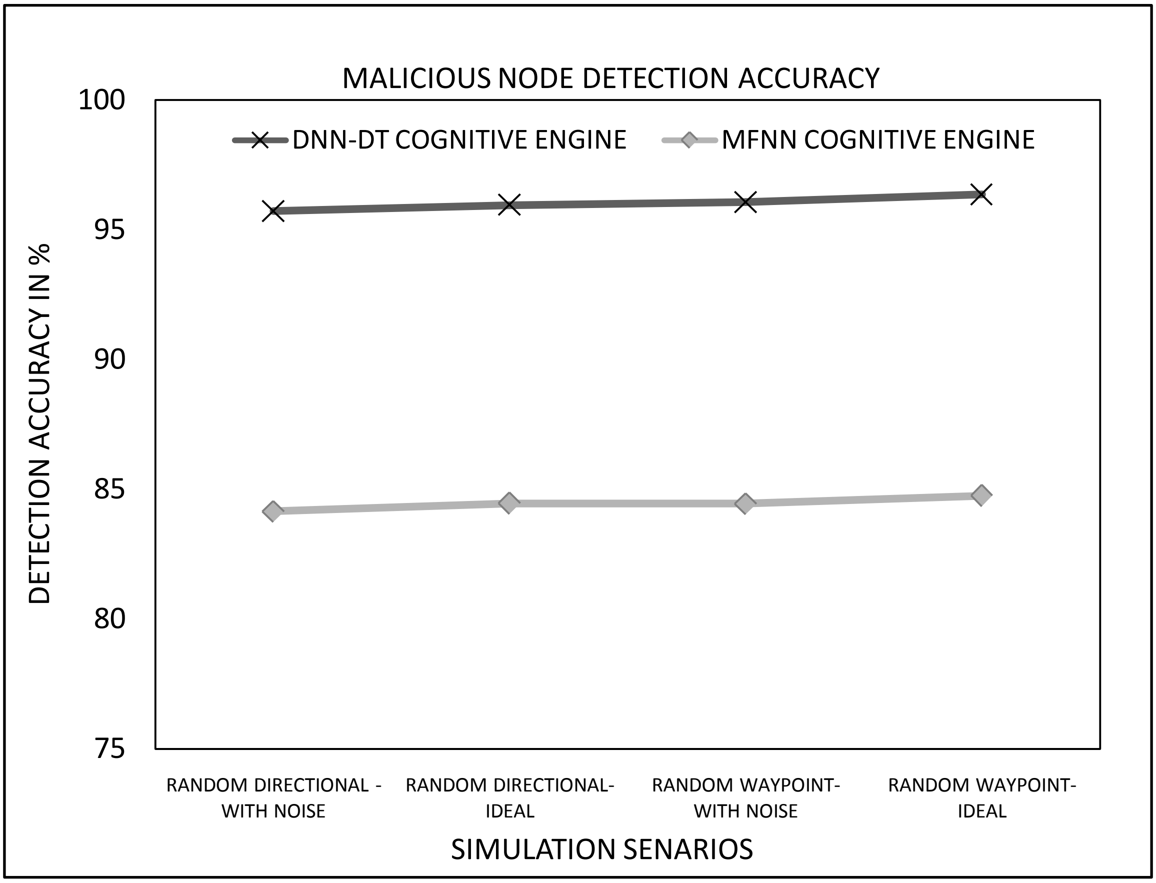

*Figure 10 :* Malicious Node Detection Accuracy for $C_S^7$

Mobility inclusion in network simulations induces an additional overhead in the network maintenance transactions. The effects of mobility on the network transactions are shown in Figure 11. The random waypoint mobility model was found to induce additional transactional overheads owing to the random node mobility it exhibits. The random directional mobility model considers the mobility of all the nodes as per a particular mobility rate and are less complicated when compared to random waypoint mobility models where in the mobility of random nodes is induced. The receiver operating characteristics curve for $C_S^7$ discussed here is shown in Figure 12. The area covered by the DNN-DT curve was found to be 0.9408 when compared to 0.7728 covered by the MFNN curve. The error of the curve for DNN-DT was about 2.5% against the error of about 4.7% exhibited by the MFNN curve.

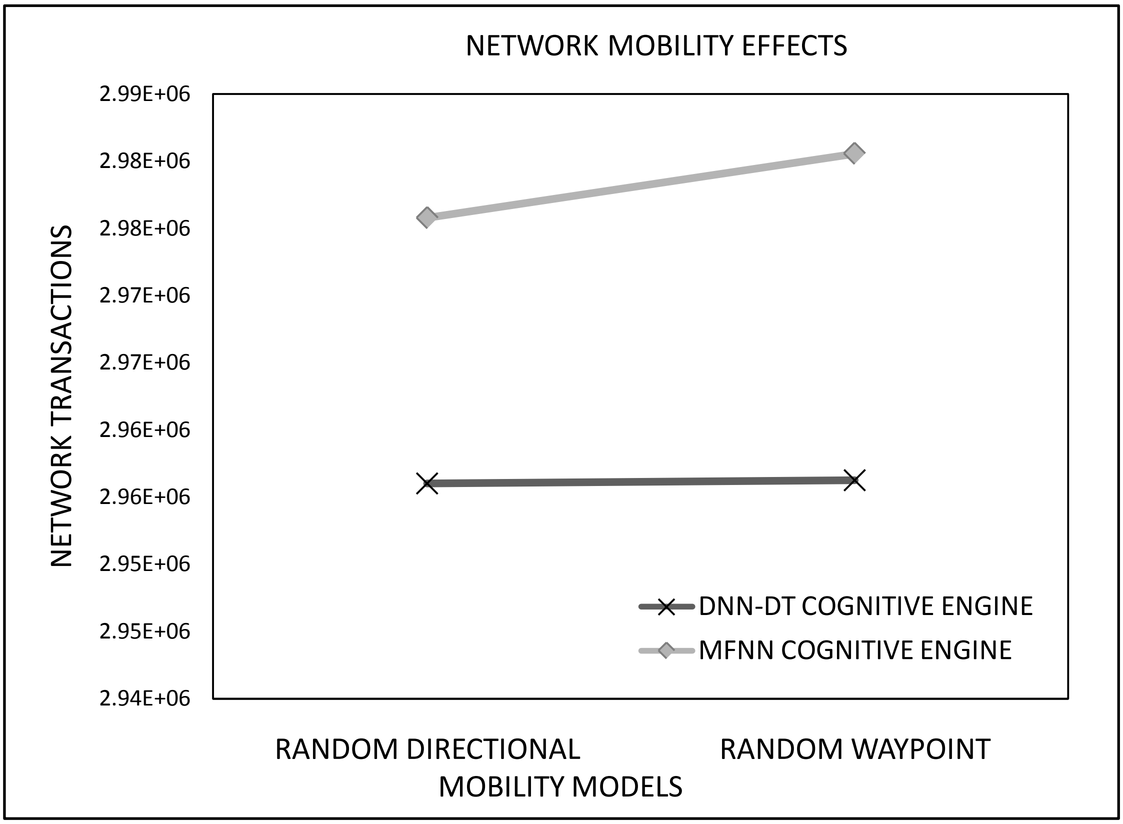

*Figure 11 :* Network Mobility Effects in Terms of Network Transactions Monitored

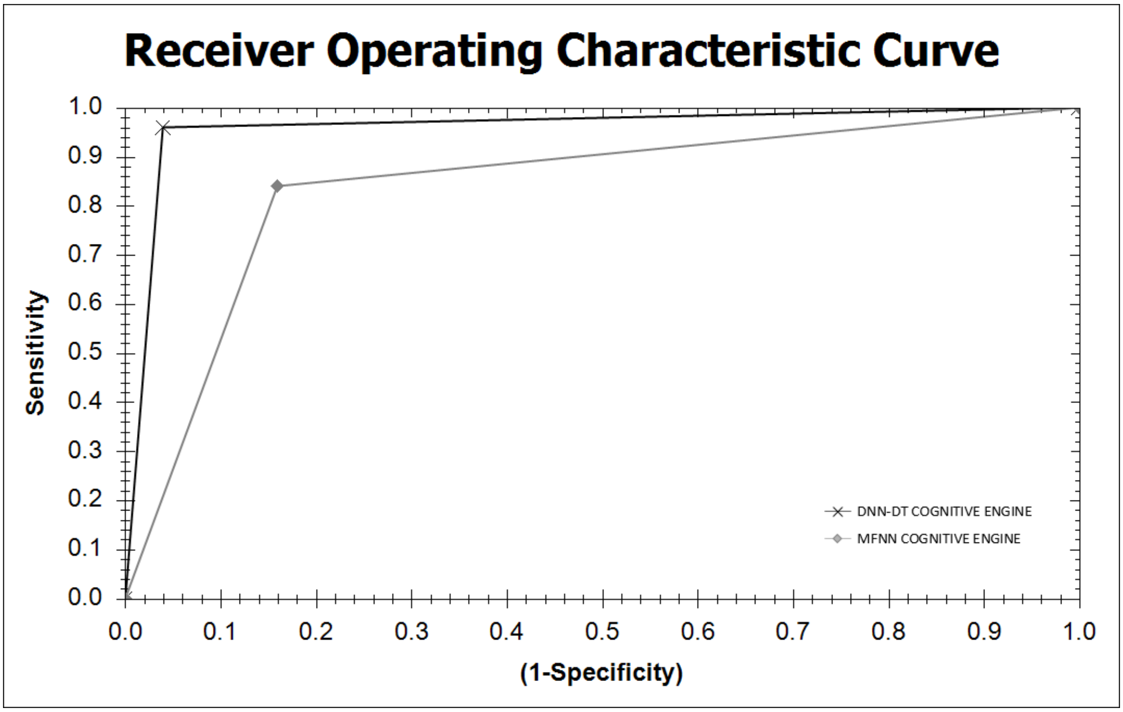

*Figure 12 :* Receiver Operating Characteristic Curve for $C_S^7$

Based on the experimental study and the analysis, it can be concluded that the proposed discrete time dynamic neural network cognition model achieves a higher accuracy of about 25% when compared to the MFNN based cognition engine.

## VI. Conclusions

The issues in security provisioning to networks can be addressed by cognitive networks. This paper proposes an OODA Loop based cognitive network. The use of discrete time dynamic neural networks to incorporate intelligence in the cognition loop is considered. The purpose of the cognitive network is to identify malicious user nodes in heterogeneous network environments. The malicious node identification is achieved by monitoring the service rates of the client nodes. Service provisioning of the services hosted by the cognitive servers to the malicious nodes is disabled hence improving performance and maintaining network integrity. The proposed system exhibits 25% higher malicious node detection efficiency and 12% higher malicious transaction classification accuracy when compared to the MFNN based cognition engine. The discrete time dynamic neural network based cognitive network proposed in this paper is an effective mechanism to identity malicious nodes and negates their presence in the considered heterogeneous network.

## References Références Referencias

1. Mitola III J, "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio", PhD thesis, Royal Institute of Technology, Sweden, 2000.
2. D H Friend, "Cognitive Networks: Foundation to Applications", Ph.D. Dissertation, Electrical and Computer Engineering, Virginia Polytechnic and State Univ., Blacksburg, March 6, 2009.
3. R W Thomas, L A DaSilva, A B MacKenzie, "Cognitive networks ", Proceedings of the First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, Baltimore, USA, November 8-11, 2005.
4. Qusay Mahmoud, "Cognitive Networks: Towards Self-Aware Networks", Wiley Inter science, 2007.
5. Xuan Han, Wen Fang Xie, Zhijun Fu, and Weidong Luo, "Nonlinear Systems Identification and Control via Dynamic Multi time Scales Neural Networks", IEEE Transactions Neural Networks and Learning Systems, no.99, 2013.
6. Xuan Han, Wen Fang Xie, Zhijun Fu, and Weidong Luo, "Nonlinear systems identification using dynamic multi-time scale neural networks", Proce-e dings of the Neuro computation, October17, 2011.
7. Komali R S, Thomas R W, DaSilva L A, MacKenzie A B, "The price of ignorance: distributed topology control in cognitive networks", IEEE Transactions on Wireless Communications, vol.9, no.4, pp.1434-1445, April 2010.
8. Daojing He, Chun Chen, Chan S, Jiajun Bu, Vasilakos A V, "A Distributed Trust Evaluation Model and Its Application Scenarios for Medical Sensor Networks", IEEE Transactions on Information Technology in Biomedicine, vol.16, no.6, pp.1164-1175, Nov. 2012.
9. Tao Jun, Lin Hui, Liu Chunlin, "IDSV: Intrusion Detection Algorithm Based on Statistics Variance

Method in User Transmission Behavior", Proceedings of International Conference on Computational and Information Sciences, pp.1182-1185, Dec.17-19, 2010.

10. Thottan M, Chuanyi Ji, "Anomaly detection in IP networks", IEEE Transactions on Signal Processing, vol.51, no.8, pp.2191-2204, Aug. 2003.
11. S C Lingareddy, B Stephen Charles, Vinayababu, Kashyap Dhruve, "Wireless Information Security Based on Cognitive Approaches", IJCSNS International Journal of Computer Science and Network Security, vol. 9 no. 12 pp. 49-54, 2009.
12. Kerry Wood and Luiz A DaSilva, "Optimal max-min lifetime routing of multicasts in ad-hoc networks with directional antennas", Proceedings of International Conference on Broadband Networks (BROADNETS 05), October 2005.
13. M Kubale, "Graph Colorings", Contemporary Mathematics, American Mathematical Society, Providence, Rhode Island, 2004.
14. R S Komali, A B MacKenzie and R P Gilles, "Effect of selfish node behavior on efficient topology design," IEEE Transactions on Mobile Computing, vol. 7, no.9, pp. 1057-1070, 2008.
15. A Boukerche and Y Ren, "A secure mobile healthcare system using trust based multicast scheme," IEEE Journal on Selected Areas of Communications, vol. 27, no. 4, pp. 387–399, May 2009.
16. David C Plummer, " An Ethernet address resolution protocol or converting network protocol addresses to 48 bit Ethernet address for transmission on Ethernet hardware", Internet Request For Comments RFC 826, November 1982.
17. Zhao Xiao feng, Ye Zhen,"Research on weighted multi-random decision tree and its application to intrusion detection", Journal of Computer Engineering and Applications, Hefei University of Technology, China.
18. Salvatore J Stolfo, Wei Fan, Wenke Lee, Andreas Prodromidis, and Philip K. Chan," Cost-based Modeling and Evaluation for Data Mining With Application to Fraud and Intrusion Detection", in Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, May 1999.
19. Zhang Wenzhu, Yi Bohai, "Approach for local multi-domain cognition in cognitive network", IEEE Transactions on Communications, vol.10, no.1, pp.146-156, China, January 2013.
20. Klein D G, Kupper L L, Nizam A, "Applied Regression Analysis and Other Multivariable Methods", Fourth Edition, Thomson Press, Belmont, USA, 2008.
21. Ding Guoru, Wang Jinlong, Wu Qihui, "System Info of Multi-Domain Cognition in Cognitive Radio Networks", Proceedings of IEEE International Conference on Wireless Communications and Signal Processing, China, October 21-23, 2010.
22. G Sunilkumar, Thriveni J, K R Venugopal, L M Patnaik , "Cognitive Approach Based User Node Activity Monitoring for Intrusion Detection in Wireless Networks", International Journal of Computer Science Issues, vol. 9, Issue 2, no.3, March 2012.
23. Madan M Gupta, Liang Jin, Noriyasu Homma, "Static and Dynamic Neural Networks: From Fundamentals to Advanced Theory", John Wiley & Sons, April 5, 2004.