International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Malicious Node Activity Monitoring using Cognition for Homogeneous and Heterogeneous Wireless Networks

G Sunilkumar[Ȧ*], Thriveni J[Ȧ], K R Venugopal[Ȧ] and L M Patnaik[Ḃ]

[Ȧ]Department of Computer Science and Engineering, Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001, India
[Ḃ]Indian Institute of Science, Bangalore,India

Accepted 07 January 2014, Available online 01 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

Cognitive wireless networks are the solution for the existing networks Infrastructure and security problems for all applications. Cognitive techniques adopted in this paper; monitor the transactions among the nodes in the network and detects the malicious nodes and takes preventive measures. To achieve high detection rate, single-sensing with cognition is adopted and training of network is done using artificial neural network based Supervised learning technique. The proposed concept is implemented for homogeneous and heterogeneous wireless networks and Detection probability is calculated based on the network parameters like, sensing range, transmission range, node density and broadcast reachability. As compared with the existing approaches, our proposed approach yielded efficient results.

Keywords: *Cognitive networks, Intrusion Detection, Supervised learning, Artificial intelligence, Soft-computing.*

1. Introduction

Wireless Networks can reduce the complexity of the existing networks. Mainly it reduces three-fourth of the infrastructure, even though it is not adopted for all the applications, due to security issues. There are enormous work done to solve the security issues. Malicious node detection is one of the most critical security issues in wireless networks.

Cognitive techniques can be applied to wireless networks, to detect the malicious node. Cognitive networks are the intelligent networks because, cognitive techniques involves artificial intelligence. The cognitive wireless network is based on knowledge, that achieves end to end goals of the network and increases reliability of the network, the network lifetime and reduces maintenance costs. Since cognitive networks are based on knowledge framework, network decisions are based on learning and reasoning on information shared among the nodes in the network about the observations made.

Knowledge plane (KP) in cognitive network is based on knowledge rather than tasks, so that the observations from different nodes of the network is correlated to make decisions in the presence of incomplete or conflicting information in dynamic environments .

In the proposed system, we are applying cognitive techniques on the homogeneous and heterogeneous wireless networks. In homogeneous wireless networks, all the node parameters are same, but in heterogeneous wireless networks, it is different. The parameters of the node may be sensing range, transmission range etc., these parameters should be carefully considered while constructing the network based on the applications.

Multilayered feed forward (MLFF) neural network with back propagation (BP) is used to impart intelligence to the cognitive network. MLFF-BP is used for anomaly intrusion detection, which is a supervised learning technique in artificial neural network. In supervised learning technique, the patterns of predefined behaviors of the network transactions are trained.

In wireless networks, there are two ways to detect the intruder. Namely, single-sensing detection and multiple-sensing detection. In single sensing, the intruder is identified using the sensing knowledge from one single node. Whereas in multiple-sensing, intruder is identified using co-operative knowledge of multiple node.

1.1 Motivation

The existing Intrusion Detection techniques in Homogeneous and Heterogeneous Wireless Networks using single-sensing detection and multiple-sensing detection is not efficient. Maximum researchers propose that, single-sensing detection is efficient, but it produces high false detection rate. Since Intrusion Detection System (IDS) is a major component of security infrastructure, it requires efficient detection model with minimum usage of resources.

1.2 Contribution

The Homogeneous and Heterogeneous Wireless Networks are constructed with Cognition techniques. To make

*Corresponding author: **G Sunilkumar**; **L M Patnaik** is an Honorary Professor

network intelligent, we are achieving Cognition by artificial intelligence and machine learning techniques. Because of cognitive techniques, we are covering maximum network area with minimum number of nodes. By using single-sensing detection with cognition, we are reducing false detection rate of malicious node detection.

1.3 Organization

This paper is organized into the following sections: related work is given in Section 2, Section 3 gives the problem definition, Section 4 explains the system model, Section 5 explains the implementation and Section 6 explains the result analysis, and conclusions are given in Section 7.

2. Related Work

Many researchers have proposed and presented various Intrusion and Malicious node Detection methods for wireless networks; some of the approaches are discussed in this paper.

G Sunilkumar et al., have proposed an approach called Cognition Based Self-organizing Maps for intrusion detection. It uses an unsupervised learning technique. Cognition based Gaussian and Mexican hat neighbor learning functions are evaluated to select the best learning function which exhibits high percentage of malicious node detection. The drawback of this approach is, it is computationally heavy and exhibits higher network response time.

Reznik and Von Pless have proposed the concept of using distributed intelligence into sensor networks. To impart intelligence into sensor networks, they mapped Artificial Neural Network Architecture to WSN Architecture. The advantage of this approach is reduced resource consumption. The cognition is based on reasoning; hence the influence of cognition on network goal is limited.

Youssef and Younis have proposed Gateway Relocation Algorithm, which is a neural network model used to assess safety of Gateway/Sink node at various locations in a WSN. The environment is trained by Genetic Algorithms. The advantage of this approach is, the neural network generates a risk assessment factor for future safe relocation decisions. But there is no influence of Cognition on network goals.

Boonma and Suzuki have proposed an algorithm called MONSOON. In this approach Decentralized group of software agents were inspired by a biological framework that adapt to dynamics of network by satisfying conflicting objectives under given set of constraints. Here the network exhibits Self-configuration, optimization and healing properties by software agents. Since the cognition is based on knowledge and context awareness, it exhibits good extent of network's end to end goals.

Ana Paula et al. have proposed Decentralized Intrusion Detection Algorithm. This algorithm is divided into three phases. Phase 1 is data acquisition, here messages are collected and the important information is filtered and stored for subsequent analysis. Phase 2 is rule application, here the processing and rules are applied to the stored data and if the message analysis fails then a failure is raised. Phase 3 is intrusion detection, here the number of raised failures is compared to the expected amount of occasional failures in the network and intrusion is detected.

Marti et al., have introduced the idea of watchdog for ad-hoc networks to improve the detection of malicious nodes. In this method, it uses a technique called pathrater for routing protocols to avoid malicious nodes.

Huang and Lee have proposed an IDS model for ad-hoc networks. The IDS is decentralized and intrusion is detected by clusters. Here the responsible node is elected from cluster to monitor the each cycle of transaction.
The main drawback of this approach is, it is expensive and inadequate to a WSN.

Liu et al., have proposed the intrusion detection model for mobile WSN to overcome from static WSN architecture approaches. Here each sensor is having mobility and the author have proposed optimal strategy for fast intrusion detection. Because of mobility of sensors, the quality of intrusion detection is more.

2.1 Background

Yun Wang et al., analyze the intrusion detection problem in both homogeneous and heterogeneous wireless sensor networks. Here the intrusion detection probability is characterized based on intrusion distance and network parameters. Both single sensing and multiple-sensing detection models are considered to calculate intrusion detection probability.

Here authors have considered the network connectivity and broadcast reachability in heterogeneous WSN. In this work, it provides insights for designing homogeneous and heterogeneous WSNs by selecting critical network parameters depending on the application requirements.

3. Problem Definition

Given a network with limited nodes deployed uniformly;

3.1 The objectives

(i) Realization of the cognition engine using Back-propagation algorithm.
(ii) To evaluate the Wireless Sensor Networks and Cognitive Networks with respect to Malicious Node Detection.
(iii) To improve the performance of Homogeneous and Heterogeneous Wireless Network using Cognition.
(iv) To show, single-sensing detection is efficient with respect to Intrusion Detection in Cognitive Wireless Network.
(v) To reduce the False Detection Rate in single-sensing detection with cognition.

3.2 Assumptions

(i) Uniform deployments of nodes are done to create Cognitive Wireless Network test bed.
(ii) We have taken Type-I and Type-II nodes. In which TypeI node has a larger sensing and transmission range, Type-II node has a smaller sensing and shorter transmission range.

(iii) Supervised method is used for monitoring the transactions of nodes.

4. System Model

Homogeneous and Heterogeneous Wireless Networks are characterized by the variations in parameters of nodes and their behaviors. To achieve cognition in such networks, we proposed to use Back propagation algorithm for learning and to observe the behavior of nodes.

The architecture of Cognition Engine is shown in Fig.1. The node repository maintains the node identities and the cognition engine recognizes the nodes based on these ids. Numerous predefined data transactions are carried out and these transactions need to be monitored to detect the malicious nodes. The monitored behavior is stored in observed node behavior section of the cognitive frame work.

Cognition can be achieved by using supervised learning technique. Here, to impart intelligence to the nodes, we are using back propagation algorithm to predict its peer node behavior. Relative transaction set contains peer node behavior patterns. If the monitored and relative behavior transactions match, then the node behavior is considered as normal else the variation in the behavior is calculated. If it is above the threshold, then the node is said to be malicious. If there is any unknown, normal new transaction is carried out among the nodes, then it gets trained by back propagation algorithm.

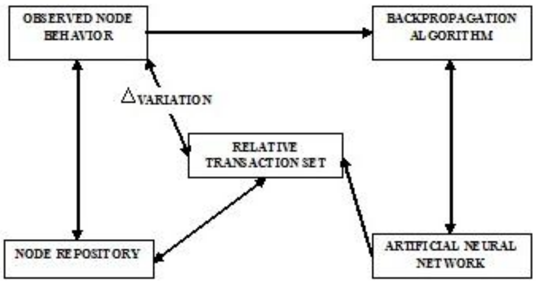

Fig.1 Cognition Engine

5. Implementation

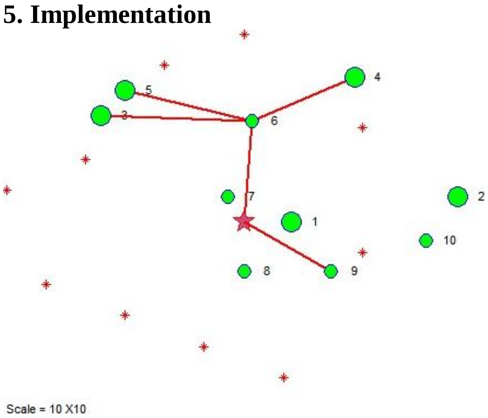

Fig. 2 Intrusion Detection in Wireless Sensor Networks

The detection of intruders in wireless sensor networks is shown in Fig.2. From the diagram, we can observe that, multiple nodes are detecting the same intruder, if it is in the transmission range of the corresponding nodes; this is called as multiple node sensing. Because of multiple nodes sensing, nodes use more bandwidth and consumes more battery power.

The detection of intruders in cognitive networks is shown in Fig.3. From this, we can observe that, multiple nodes are not detecting the same intruder. Here single node is detecting the single intruder even though the multiple nodes are in the transmission range of that intruder. This is called as single node sensing. Because of single node sensing, it uses less bandwidth and also it consumes less battery power. Table I gives the Intrusion Detection System algorithm.

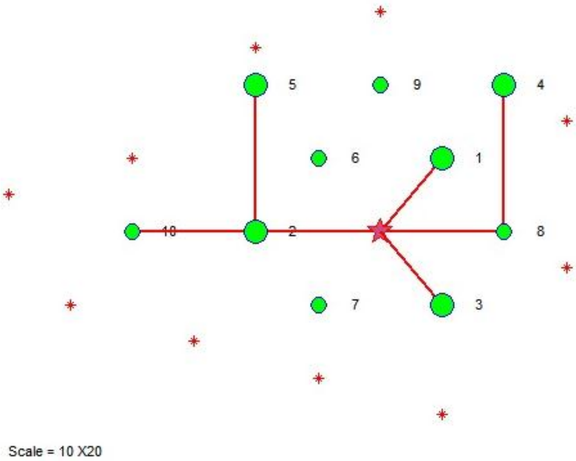

Fig. 3 Intrusion Detection in Cognitive Networks

Table I: Intrusion Detection System

Algorithm: Intrusion Detection System

// Input: Initial network N with initial weights.
// NP_{out} = Neural-network-output
// EXP_{out} = Expected output of parameter p for node N_i
for all Nodes N_i in a Network
for each parameter p in the training set T
Neural-network-output (Network, p); forward pass
Calculate difference D in output (EXP_{out} - NP_{out})
if D > threshold *then*
Consider Node N_i as intruder, report to administrator;
end if
end for
end for

The cognitive network construction is shown in Fig. 4. Based on capability of the sensing node, the nodes are deployed. So that network capability is uniformly maintained and is done by cognitive process. Based on application, we can cover larger area by using less number of sensing nodes.

In cognitive network, if there is any dead node then, the network gets reconstructed. So that it will not disturb the current application. This is called as dynamic reconstruction. Where as in wireless sensor networks, nodes are randomly deployed and there is a chance of node un-reachability. Because of random deployment, node density can be high in some area and other area it may be less. This leads to problem in application dependency. If there is any dead node in wireless sensor network, then the current application gets disturbed. Table II gives the Cognitive Network Creation.

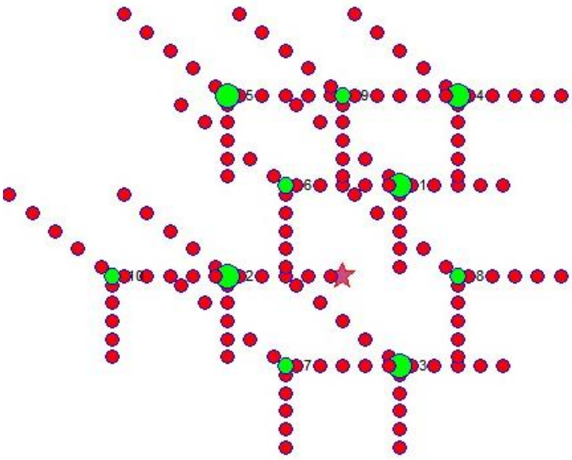

Fig. 4 Cognitive Network Construction

Table II: Cognitive Network Creation

Algorithm: Cognitive Network Creation

// Input: Initial network N with initial weights.
// Output: Balanced network N.
// N_{out} = Network output for p
// Ref_{out} = Reference output for p
for all Nodes N_i in network
for each parameter p in the training set T
do
Calculate error (Ref_{out} - N_{out})
Compute $weight_{hid}$ for all weights from hidden layer to output layer; backward pass
Compute $weight_{in}$ for all weights from input layer to hidden layer; backward pass continued
Update parameter p correctly in a training set T, so that it will satisfy the network condition
end for
end for
Return balanced network

6. Result Analysis

6.1 Verification for Homogeneous and Heterogeneous Networks

We have deployed 20 type-1 sensors uniformly in 50*50 square meters and the node density is 0.008 per square meter. The sensing range of each sensor varies from 0 to 30 meters. The simulation is done for 30 times to take average intrusion detection values to draw graph.

Fig.5. Shows the intrusion detection probability with respect to sensing range in wireless sensor networks and cognitive networks.

As the sensing range reaches to 5 meter, the intrusion detection probability increases in both wireless sensor networks and cognitive networks. But in the cognitive network the detection probability reaches to 1 and in wireless sensor network, it reaches to 0.2. As the sensing range is increased in multiples of 5 the detection probability also increases linearly in wireless sensor networks, but in cognitive network is always 1. At the sensing range 30, detection probability in wireless sensor networks also reaches to 1.

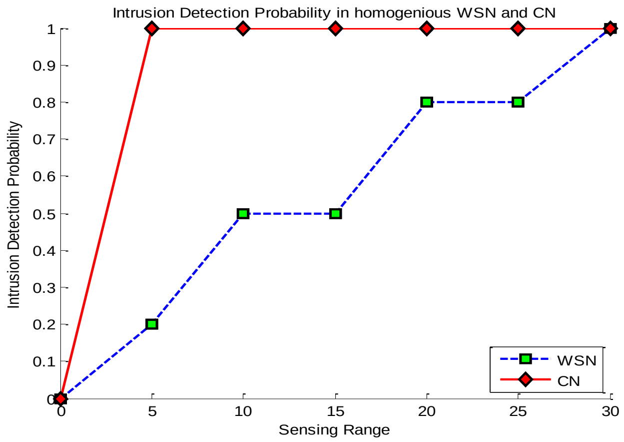

Fig. 5 Intrusion Detection Probability Vs Sensing Range in Homogeneous Networks

From this graph, we can observe that, cognitive network is not depending on sensing range of a node. Whereas wireless sensor network (WSN) is depending on sensing range of a node. The drawback of this approach is the cost of homogeneous network is more due to cost of high capacity nodes i.e., type -1 node. If it is type-II node, then it is low capability nodes and it requires more number of nodes so that cost increases.

We have deployed ten type-II nodes constant and type-I nodes is varied from 0 to 60 and the sensing range is set as 5 meters for type-II nodes and 10 meters for type – I nodes. Fig.6. shows the Intrusion detection probability under heterogeneous case.

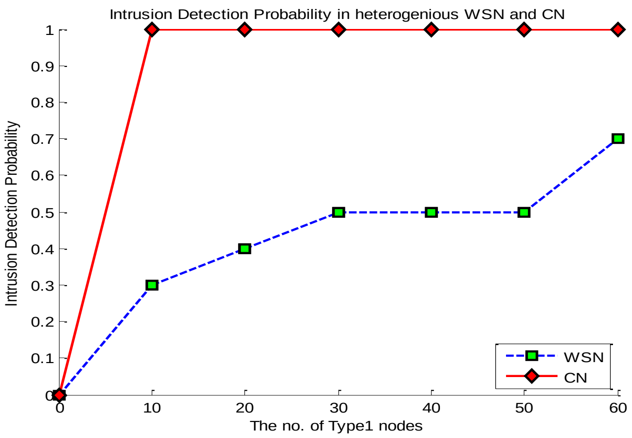

Fig. 6 Intrusion Detection Probability Vs No. of Type1 nodes in Heterogeneous Networks

As the number of type –I nodes are increased to 10, the intrusion detection probability reaches to 1 in cognitive network. But in wireless sensor network it is reached to 0.3.

The number of type – I nodes are increased in multiples of 10 till 60, and then the detection probability is 1 for cognitive network. But wireless sensor network failed to reach detection probability to 1. It is because of high chances of network unreachability in wireless sensor network, due to heterogeneous network. Only advantage is network cost due to the combinations of different capability of nodes.

6.2 Verification for Network Connectivity

6.2.1 Based on Node Density

From Fig. 7 and Fig. 8, the variation in intrusion detection probability with respect to the number of type-I and type-II node can be observed.

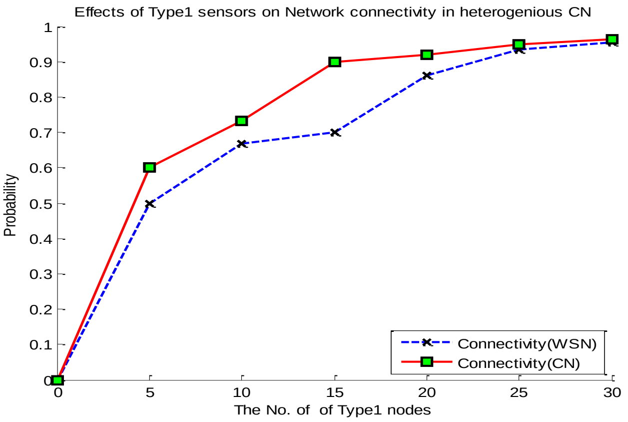

Fig. 7 Intrusion Detection Probability Vs No. of Type1 Nodes for Network Connectivity in Heterogeneous Networks.

In Fig. 6, the type-II node is kept constant and type-I node is increased, the detection probability also increased in wireless sensor network and cognitive network. But the detection probability in cognitive network is increased much faster and reached to 1 as compared to wireless sensor network.

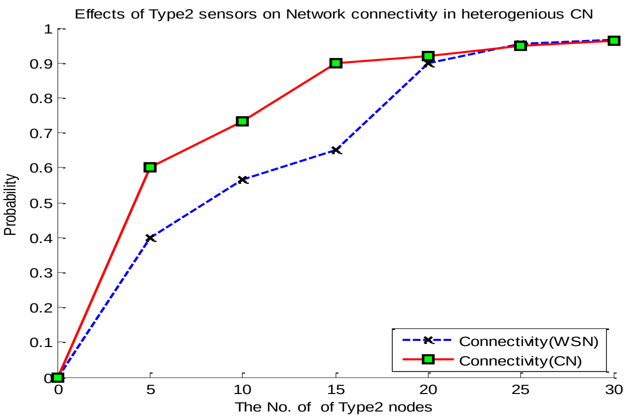

Fig. 8 Intrusion Detection Probability Vs No. of Type2 Nodes for Network Connectivity in Heterogeneous Networks

In Fig. 7, the type-I node is kept constant and type-II node is increased and we can observe the same variations as in Fig. 8. From this approach we can conclude that, connectivity depends on the node density.

6.2.2 Based on Transmission Range

From Fig. 9 and Fig. 10, we can observe the variations of detection probability with respect to increase in the transmission range of type-I and type-II node.

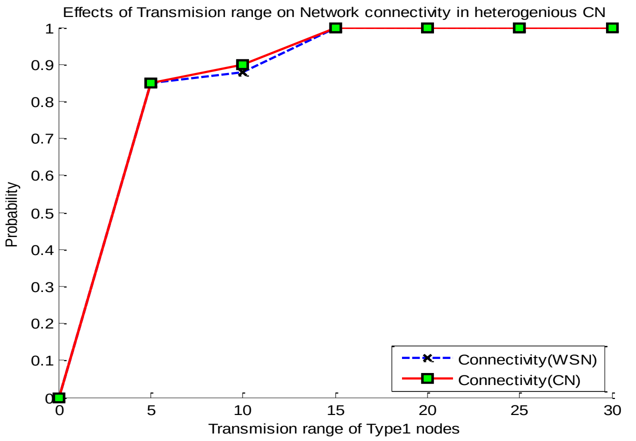

Fig. 9 Intrusion Detection Probability Vs Transmission Range of Type1 Nodes in Heterogeneous Networks

In Fig. 9, the transmission range of type-II node is kept constant and type-I node is increased from 0 to 30 meter, in Fig. 10 it is vice versa. Initially the detection probability of wireless sensor network is low compared to cognitive network, but at some threshold, both are same.

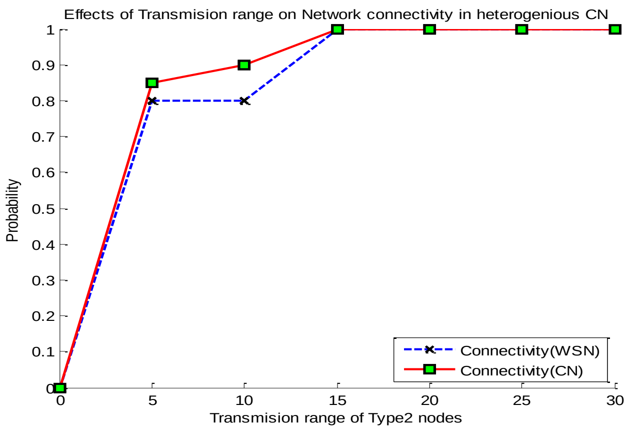

Fig. 10 Intrusion Detection Probability Vs Transmission Range of Type2 Nodes in Heterogeneous Networks

The main drawback of this approach is, the battery power consumption of a node is more. Hence the maintenance is difficult.

6.3 Verification for Broadcast Reachability

The variations in the detection probability with respect to density of nodes for broadcast reachability can be seen in Fig 11.

From the Fig 11, we can conclude that, the broadcast reachability is also depending on the density of nodes and heterogeneity.

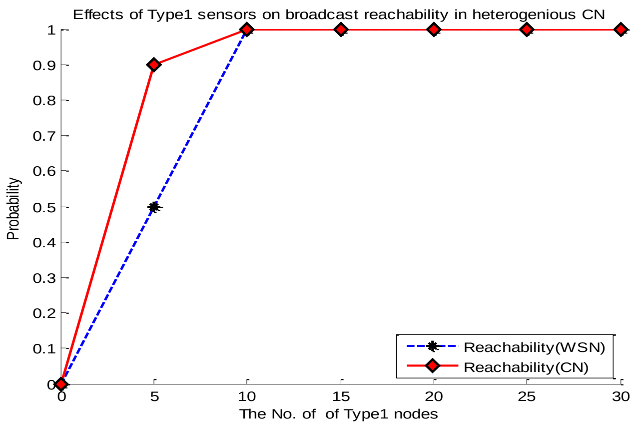

Fig. 11 Intrusion Detection Probability Vs No. of Type1 Nodes in Heterogeneous Networks for Broadcast Reachability.

7. Conclusions

Cognitive wireless networks are the solution for the existing networks Infrastructure and security problems for all applications. The transactions among the nodes in the network are monitored and detected the malicious nodes using Cognition. High detection rate is achieved by single-sensing detection with cognition. The proposed concept for homogeneous and heterogeneous wireless networks gives better results, compared with existing approaches.

References

O. B. Akan, O. Karli, O. Ergul (July-August.2009.), Cognitive Radio Sensor Networks, *IEEE Network*, vol.23, no. 4, pp. 34-40,

W. Youssef, M. Younis (2008), A Cognitive Scheme for Gateway Protection in Wireless Sensor Network, *Applied Intelligence Journal*, vol. 29, no. 3, pp. 216-227,

K. Shenai and S. Mukhopadhyay (May 2008), Cognitive Sensor Networks, in *Proc. of IEEE Twenty Sixth International Conference on Microelectronics* (MIEL), pp. 315-320,.

E. Gelenbe, P. Liu, B. K. Szymanski, C. Morrell (July 2011), Cognitive and Self-selective Routing for Sensor Networks, *Journal of Computational Management Science*, vol. 8, no. 3, pp. 237-258.

E. Bdira, M. Ibnkahla (2009), Performance Modeling of cognitive Wireless Sensor Networks Applied to Environmental Protection, in *Proc of IEEE GLOBECOM*, pp. 1-6,Honolulu

Gayathri Vijay, Elyes Bdira (2011), Mohamed Ibnkahla, Cognition in Wireless Sensor Networks:A Perspective, *IEEE Sensors Journal*, vol.11, no. 3, pp. 582-592.

D. D. Clark, C. Partrige, J. C. Ramming, J. T. Wroclawski (Aug. 2003), A Knowledge Plane for the Internet, Proc. of SIGCOMM 2003, pp. 3-10, Karlsruhe, Germany

G.Sunilkumar,ThriveniJ,K.R.Venugopal,L.M.Patnaik (March 2012),Cognitive Approach Based User Node Activity Monitoring for Intrusion Detection in Wireless Networks, *International Journal of Computer Science* Issue, vol. 9,Issue 2, no.3.

L. Reznik, G. Von Pless (June 2008), Neural Networks for Cognitive Sensor Networks, in *Proc. of IEEE International Joint Conference on Neural Networks*, pp. 1235-1241.

P. Boonma, J. Suzuki (June 2008), Exploring Self-star Properties in Cognitive Sensor Networking, in *Proc. of International Symposium on Performance Evaluation of Computer and Telecommunication Systems* (SPECTS), Edinburgh, pp. 36-43.

Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P.S.Rocha, Antonio A. F. Loureiro, Linnyer B. Ruiz and Hao Chi Wong (October, 2005), Decentrlized Intrusion Detection in Wireless Sensor Networks, in *Proc. of Q2SWinet* 2005, pp. 16-23, Montreal, Quebec, Canada.

S. Marti, T. J. Giuli, K. Lai and M. Baker (2000), Mitigating Routing Misbehavior in Mobile Ad-hoc Networks, in *Proc. of MOBICOM*, pp. 255-265.

Yi-an Huang and W. Lee (2003), A Cooperative Intrusion Detection System for Ad-hoc Networks, in *Proc. of ACM workshop on Security of Ad-hoc and Sensor Networks*, pp. 135-147.

B. Liu, P. Brass, O. Dousse, P. Nain and D. Towsley (2005), Mobility Improves Coverage of Sensor Networks, in *Proc. of MobiHoc*, pp. 300-308.

Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang and Dharma P. Agrawal (June 2008), Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks, *IEEE Transactions on Mobile Computing*, vol. 7, no. 6, pp. 698-711.

Sunilkumar G has completed Bachelor of Engineering in Electronics and Communications from Visvesavaraya Technological University,Belgaum, Master of Engineering in Information Technology from University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He is a research scholar in Bangalore University. He has 7 years of teaching experience. Currently he is an Assistant Professor in the Dept. of CSE, Alpha College of Engineering, Bangalore. His area of interest includes Cognitive Networks, Cloud Computing, and Network Security.

Thriveni J has completed Bachelor of Engineering, Masters of Engineering and Doctoral Degree in Computer Science and Engineering. She has 4 years of industrial experience and 18 years of teaching experience. Currently she is an Associate Professor in the Dept. of CSE, University Visvesvaraya College of Engineering, Bangalore. She has over 40 research papers to her credit. Currently she is guiding 7 Ph.D Students. Her research interests include Networks, Data Mining and Biometrics.

Venugopal K R is currently Special Officer, DVG Bangalore University and Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 39 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc.. During his three decades of service at UVCE he has over 400 research papers to his credit. He was a Post Doctoral Research Scholar at University of Southern California, USA. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

L M Patnaik is a Ex-Vice Chancellor, Defense Institute of Advanced Technology, Pune, India. He was a Professor since 1986 with the Department of Computer Science and Automation, Indian Institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Journals and refereed International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. Currently he is Honarary Professor, Indian Institute of Science Bangalore,India. His areas of research interest have been Parallel and Distributed Computing, Mobile Computing, CAD for VLSI circuits, Soft Computing and Computational Neuroscience