Wireless Information Security Based on Cognitive Approaches

***S.C.Lingareddy*[†] *, Dr B Stephen Charles*[††] *,* *Dr Vinaya Babu*[†††] *and* *Kashyap Dhruve*[††††]**

–

[†]Assistant Professor and Head, Dept of CSE, KNSIT ,Bangalore, India
[††]Principal Stanley Stephen College of Engineering, Kurnool, India
[†††]Professor of CSE and Director, SCDE, JNTU, Hyderabad, India
[†††]Technical Director, Planet-i Technologies, Bangalore, India

Summary

Wireless networks are becoming a key technology for ubiquitous broadband access, through city wide blanket Wi-Fi coverage or dense enterprise Wi-Fi deployments. Securing such wireless networks poses distinctive research challenges. A larger number of organizations, based on vendor literature, think that the security provided at their deployed wireless access points is adequate to prevent unauthorized access and use. Unfortunately, this is far from truth. The current security mechanisms provided at access points are vulnerable to attacks and pose huge threats to the integrity of the network. Our approach describes about securing of wireless networks by the cognitive neural network approaches in which, the users are uniquely identified using their respective Physical Architecture Description Layer (PADL) attributes.

Key Words:

Back Propagation, Cognitive Security Manager, IEEE 802.11, Neural Network approaches, Physical Architecture Description Layer, Wireless Network security

1. Introduction

The mobility of modern man is very dynamic. This vibrancy exhibited especially in his professional life raises the need for wireless communication. Wireless network standards defined IEEE 802.11 is one such solution to provide wire free network communication. The field of Wireless Networking has been experiencing an explosive growth proportional to the Internet, since the users and the service providers enjoy the flexibility and accessibility of any-time any-where network. Wireless Networks have many advantages, which come bundled along with lot of security issues. The major risk involved is that the information is transmitted through air [1].

Access Points (AP) act as a bridge between the wired and the wireless network world. To protect the internal resources from external threats, the organizations usually purchase and install firewalls. We observed that the current wireless Access Points present a larger security problem [2].

A number of institutions, corporations, based on merchant's related documents believe that the security provided by their deployed wireless access points is adequate to prevent unauthorized access and use. Several security mechanisms are provided for confidentiality, authentication, and access control [2][4][5] But it will not be an exaggeration to say that all of these are vulnerable. Network evolution towards self-aware autonomous adaptive networking attempts to overcome the inefficiency of configuring and managing networks, which leads to Performance degradation and effects Quality of Service. In order to optimize network operations, the introduction of self-awareness, self-management, and self healing into the network was proposed. This created a new paradigm in networking, known as the Fundamentals of Cognitive Networking.

Techniques for enabling cognitive properties, such as, adaptation, learning, and goal optimization processes are detailed in the text [14]. A comparison of available research proposals leads to the design of a promising cognitive network architecture capable of incorporating cognitive network techniques. Finally, a discussion on the required properties of the cross-layer design for cognitive networks and deployment issues are specified. Wireless Network security mechanism is directly proportional to the identity of the user who accesses the wireless network under consideration [9].

2. Related Work

There is a significant amount of research work done on securing wireless network based on IEEE 802.11. We discuss here some of the security threats and attacks, that may damage wireless network. There are basically two types of attacks namely Logical attacks and Physical attacks. Logical attacks are attacks on WEP, MAC Address spoofing, Denial of Service attacks, Man-in-Middle attacks, Default AP Configuration and Bad Network Design. Physical attacks are on AP. [2].

There have been some attempts to provide levels of security technologies to resolve the authentication problem for wireless network [2]. Cognitive Networks/software defined radio are areas being self adaptive and intelligent and could be a solution to the security issues related to

Manuscript received December 5, 2009
Manuscript revised December 20, 2009

IEEE802.11.Most of the attacks such as node misbehavior are on wireless networks. Authentication of the user can prevent use of the network by unauthorized user. Identification of primary user is essential to grant access. Related work was done to successfully identify and authenticate the primary user.

Security in Cognitive Networks poses many challenges [13] which are still in the implementation stage. This paper is an attempt to provide an Authorization Framework based on the PADL of the mobile nodes. The PADL is unique for each node and is used for Authentication. The Authentication is carried out by the Cognitive Security Manager (CSM) in our framework.

3. Problem Statement

The major objective of the research work is to secure the wireless network by introducing intelligent methods to wireless communications i.e. Cognitive Security Managers. The network which is studied is ad-hoc in nature. CSM will decide the authentication of each node and grant the permission to access the internet or other services offered. The authorization is achieved on the Physical Hardware Description attributes of the nodes within this network. The research is carried out on the IEEE 802.11 networks deployed at our laboratories. The security is provided for the entire system. We are making use of 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.

According to the current security features available on IEEE 802.11 wireless networks, the user nodes could be granted limited access only based on its TCP/IP Configurations or based on the Physical Hardware Address of their respective RF wireless adapters. The CSM maintains the integrity of the entire network by studying the Physical Architecture Description Layer (PADL) of all the nodes within the network.

4. Proposed Solution

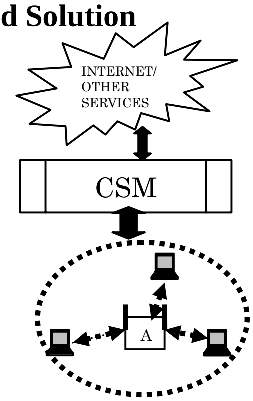

Figure 1: Cognitive Wireless Network having 3 nodes x, y and z.

The proposed Cognitive wireless network is as shown in Figure (1)

This process can be illustrated in the following steps:

Step 1: The CSM registers the wireless ad-hoc nodes based on the PADL of the nodes. The CSM maintains the Physical Description Layer data of all the nodes requesting access.

Step 2: The CSM obtains the authenticity of the nodes from its existing data grid of the nodes. The data grid maintained by the CSM is updated regularly and is maintained by the administrators.

The proposed conceptual architecture of the CSM

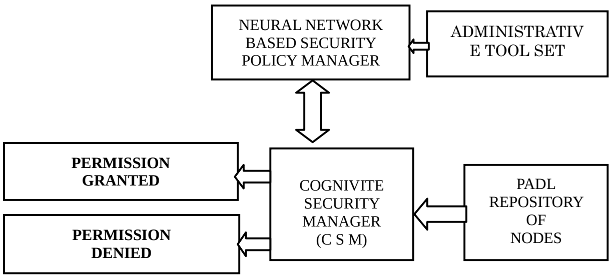

Figure 2: The conceptual Architecture

4.1 Algorithm for CSM Cognitive Analysis

Step 1: Receives the PADL of all the nodes in the network and compares it with the PADL present in the repository.

a) If the PADL is not present – New Node. Go to 4
b) If the PADL of the node is Present check
    i) Node is Authorized – Goto 2
    ii) Node is Unauthorized – Goto 3

Step 2: If a Node is authorized its behavior is monitored, then provide services access permission. Goto 5

Step 3: If a Node is unauthorized then provide the Node with service access denied. Goto 7

Step 4: If a New Node then

c) Deposit the PADL into the PADL Repository
d) Obtain its service access permission from the administrative tool set.
e) Grant service access permission under monitored conditions.

Step 5: Obtain behavior characteristics of the nodes and provide the PADL of the node to the neural network as an input. The trained neural network framework estimates the behavior pattern of the node with respect to its PADL.

Step 6: If the behavior of the node is similar to the neural network based estimated behavior then the node observes uninterrupted service access permission.

Step 7: If the behavior of the node does not match with the estimated behavior then the service access permissions are withdrawn. Then the PADL of the node is moved to the unauthorized section.

The algorithm given above gives the clear operational and functional description of the CSM. The PADL registration process enables the wireless network under consideration to prevent complete access to the network services offered thus ensuring security and data integrity. If further a registered node within the wireless network performs any unauthorized activity, then the Neural Network based CSM Policy Manager would detect a difference in that node behavior. Based on this detection the node would be moved to the unauthorized node section of the PADL repository securing the network.

4.2 CSM - Neural Network based Security Policy Manager

The neural network security manager is responsible for detection unmatched or unauthorized access of the wireless network resources and services. For this purpose node behavior monitoring and analysis, we have used the Back Propagation Algorithm in our cognitive approach.

In our approach we have considered a Multi Layer Network of Neurons and the Back Prorogation Algorithm with pattern wise learning approach. The trained Neural Networks estimate the deviation of a node behavior from the trained pattern.

Our proposed Neural Network consists of 3 layers , the input layer , hidden layer and the output layer as shown in Figure 3.

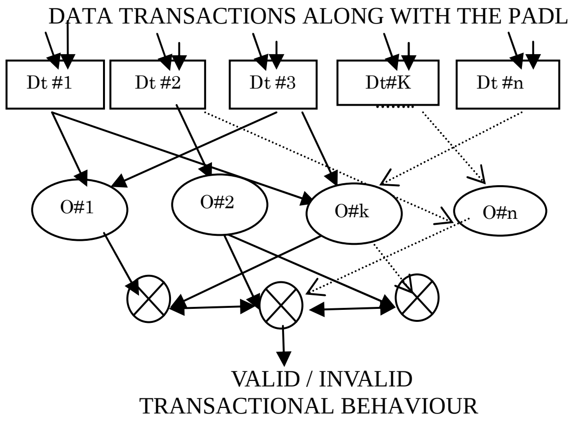

Figure 3: Back propagation based Neural Network

Under operations all the data transactions of the nodes (Registered) are monitored and studied, acting as an input to the neural network. A common operation pattern could be generated over a period of time which would be used as the trained layer of the neural network. If the pattern of data transaction of a node is found to be homogenous, a security policy is created which then provides permission to utilize the internet/other services for the node. The advantage of using neural networks is that if the user of the node performs malicious activities over PADL registered nodes, the differences could easily be identified due to the difference in operational patterns producing a denied permission and resulting the node to move from the registered section of the PADL repository to the unregistered section of the repository. When the node is provided with a denied permission it basically means that the node has no access to the services provided within the network.

Figure 4 provides a pictorial understanding of the CSM functionality

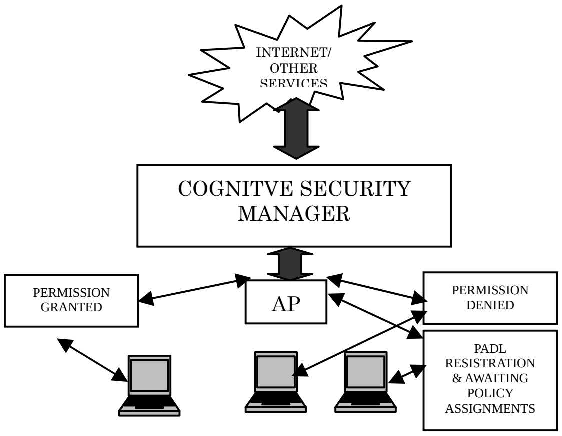

Figure 4: A overview of the Cognitive Wireless Network.

5. Experimental Study

In this section, we present the experimental setup to evaluate the functionality of the CSM. The performance of the CSM can be evaluated by studying the behavior and response of the neural network, which is the proposed network to be used.

We have created a setup to extract the PADL from each of the nodes which is eventually stored in the PADL Repository. The PADL extracted consist of a comprehensive description of all the peripherals used by the nodes. The PADL extracted consists of various parameters of the Hardware Description Layer of the nodes under consideration. A sample PADL extracted from one of the nodes under consideration is as shown below.

<u>Sample Extracted PADL</u>

```
Operating System
            --- Operating System: Microsoft Windows XP Professional
            --- Version: 5.1.2600
            --- Manufacturer: Microsoft Corporation
            --- Computer Name: ADARSH
```

```
                  --- Windows Directory: C: |WINDOWS
                  --- Serial Number: 55274-640-1048366-23351
Computer System
                  --- Computer Manufacturer Name: Dell Inc.
                  --- Computer Model: Latitude E5400
                  --- System Type: X86-based PC
                 --- Total Physical Memory: 2,051,168 KB
                  --- Domain: WORKGROUP
                  --- User Name: ADARSH |Administrator
System Processor              --- Manufacturer: Genuine Intel
                  --- Computer Processor: x86 Family 6 Model 15 Stepping
                  13
                  --- CPU Speed: 1.995G Hz
                  --- L2 Cache Size: 2 KB
System Bios
                  ---BIOS: Phoenix ROM BIOS PLUS Version 1.10
                  --- BIOS Version: DELL      - 27d9080b
Logical Memory Configuration
                  --- Total Page File Space: 3,984,416 KB
                  --- TOTAL Virtual Memory: 1,841,280 KB
                  --- TOTAL Virtual Memory: 2,051,168 KB
Network Adapter
                  --- Name: RAS Async Adapter
                  --- Name: WAN Miniport (L2TP)
                  --- Name: WAN Miniport (PPTP)
                  --- Name: Direct Parallel
                  --- Name: WAN Miniport (IP)
                  --- Name: Packet Scheduler Miniport
Video Controller
                  --- Name: Mobile Intel(R) 4 Series Express Chipset Family
                  --- Processor: Mobile Intel(R) 4 Series Express

Chipset Family
                  --- Mode: 1280 x 800 x 4294967296 colors
                  --- Video Ram: 1,048,576 KB
                  --- Status: OK
                  --- Name: Mobile Intel(R) 4 Series Express Chipset
                       Family
                  --- Processor: Mobile Intel(R) 4 Series Express
                      Chipset Family
```

Once a node enters the test wireless network the PADL is extracted and is passed on to the CSM. The PADL extraction is an over head to the node. Table 1 shows the average PADL extraction time across various nodes.

System configuration	**Average PADL Extraction Time in µs**
AMD Processor- Desktop	3.182613564
Intel P4 – Desktop	1.886062055
Intel Quad Core – Server	5.410941421
Dell Laptop – Centrino	3.005826439
Acer Laptop - Dual Core	3.440759567
Sony Vaio Laptop - Core 2 Duo	3.340289059

Table 1: Average PADL Extraction Time

From Table 1 it is clear that the over head experienced by the wireless Nodes is minimal or even negligible.

To analyze the response time of the CSM we setup a wireless test bed. The wireless teat bed consist of 50 Dell Desk Tops , 50 HCL Desktops , 3 Quad Core Servers , 15 Sony Vaio Laptops , 15 Dell Latitude Laptops , 15 Acer and 10 Zenith Laptops. All these were wirelessly connected using a number of access points. The CSM authentication system was run on the Intel Quad Core Server with 4 GB RAM.

Table 2 shows the average response time of the CSM when a PADL of a node is presented to it. The CSM classifies the PADL of the node into the following categories

1) Authorized Node
2) Un- Authorized Node
3) New Node

The PADL classifies the node into any one of the category based on the PADL Repository it houses. The PADL repository consists of PADL's of authorized and un-authorized nodes. For the purpose of testing, we had equally categorized PADL's of the nodes into authorized and un-authorized sets (i.e. for 40 nodes: 20 Authorized Nodes and 20 unauthorized nodes).If the PADL of the node presented to the CSM does not exist in the PADL repository it classifies it to a new node category.

No of PADL in repository	Response Times for Authorized Nodes	Response Times for Un-Authorized Nodes	Response Times for New Nodes
60	0.076374316	0.129842454	0.199215822
80	0.154722313	0.148269403	0.223068777
100	0.179139962	0.160555819	0.236031022
120	0.216326344	0.22035352	0.255628965
140	0.262311486	0.233723434	0.318858376

Table 2: Average Response Time of CSM – Node Classification

Figure 5 shows the graphical view of the response time of the CSM.

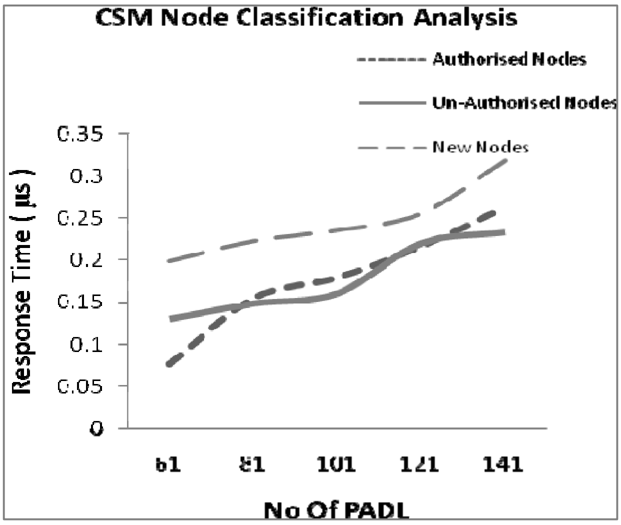

Figure 5: CSM Node Classification Analysis

From Figure 5 and Table 4 it is clear that as the size of the wireless network increases the response time of the CSM to classify the node too increases. The response time increases but is very acceptable as seen because it is in micro seconds. It is also apparent that the CSM behaves rather cautiously when a new node arrives; that's why the CSM response time is the greater for a new node when compared to authorized and un-authorized Nodes.

After studying the CSM node classification behavior it is now necessary to study the response of the CSM in analyzing the behavioral patterns of the nodes. The CSM uses a neural network based on the Back Prorogation Algorithm. We provide to the CSM two behavioral patterns. One of the patterns is homogenous in nature of a registered node and the other pattern offered is a heterogeneous. The results obtained are tabulated in Table 3.

Training Set	Valid Transaction Detection Time	Invalid transaction Detection Time
140	0.002644496	0.00211335
120	0.002148578	0.002265153
70	0.00224086	0.002085436
60	0.002228775	0.002134465
50	0.002214627	0.001994983
40	0.002212206	0.002094416
30	0.002498876	0.002035161

Table 3: CSM – Transaction Pattern Detection Analysis

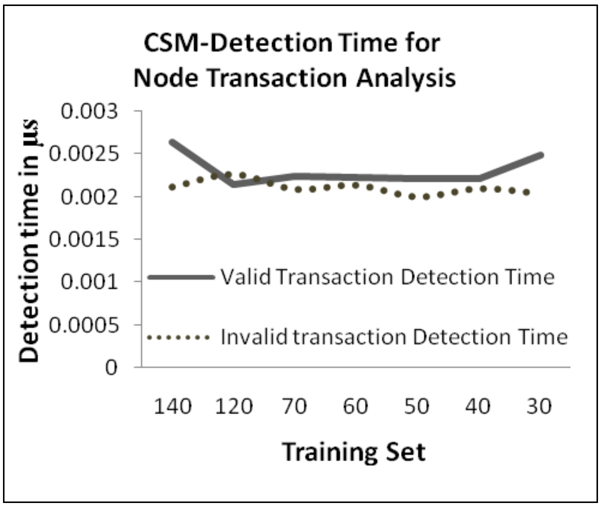

Figure 6. CSM – transaction Pattern Detection Analysis

The results obtained in Table 3 are graphically represented in figure 6. It can be seen that the Neural Network based CSM security manager identifies valid data transactions patterns and invalid data transaction patterns highly efficiently and accurately.

6. Conclusion

This paper discusses the Security threats and attacks and related work done in the research field of securing wireless network IEEE 802.11. Finally, this paper proposes a framework for Securing the wireless network using PADL and finding solution for identifying the Authentication and Authorization of the node by using cognitive approaches.

The experimental result shows that the CSM is capable of effectively securing a wireless networks with highly acceptable response times. The CSM can achieve very high authenticability of the user nodes and also detect valid and invalid behavioral patterns of the user node transaction.

A lot more research still needs to be done on software implementation and realization of this approach across various applications.

Acknowledgment

The authors would like to express their cordial thanks to Mr Ashutosh Kumar – Director Planet-i Technologies for his valuable advice.

References

[1] Mobile Agent based Authentication for Wireless Network Security, Olatunde O. Abiona ,Yu Cheng © 2008 IEEE
[2] IEEE 802.11 Wireless LAN Security Overview, Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006
[3] Your 802.11 Wireless Network has No Clothes: William A. Arbaugh,Narendar Shankar,Y.C. Justin Wan, March 30, 2001.
[4] Dependability in Wireless Networks, Can We Rely on Wi-Fi?,PUBLISHED BY THE IEEE COMPUTER SOCIETY © 2007 IEEE ■ IEEE SECURITY & PRIVACY
[5] Guide to Securing Legacy IEEE 802.11 Wireless Networks, NIST ,Karen Scarfone Derrick Dicoi Matthew Sexton Cyrus Tibbs, july 2008
[6] Securing a Wireless World ,HAO YANG , FABIO RICCIATO , SONGWU LU, AND LIXIA ZHANG, Proceedings of the IEEE, VOL. 94, NO. 2, FEBRUARY 2006
[7] Wireless Security Is Different : William A. Arbaugh, University of Maryland at College Park, IEEE August 2003
[8] Practical attacks against WEP and WPA,Martin Beck, TU-Dresden, Germany, November 8, 2008
[9] Hacking Techniques in Wireless Networks, PrabhakerMateti, The Handbook of Information Security", Hossein Bidgoli (Editor-in-Chief), John Wiley & Sons, Inc., 2005.
[10] Performance Analysis of an Authentication Scheme for Personalized Mobile Multimedia applications: A Cognitive Agents based Approach by B. Sathish Babu and Pallapa

Venkataram, International Journal of Security and its Applications Vol. 2, No. 4, October, 2008
[11] Intelligent Cognitive Radio: Research on Learning and Evaluation of CR Based on Neural Network , Zhenyu Zhang, Xiaoyao Xie, Member, IEEE,@2007,IEEE
[12] Security in Cognitive Radio Networks:Threats and Mitigation T.Charles Clancy, Nathan Goergen
[13] Secure Cognitive Networks, Neeli Rashmi Prasad, Proceedings of the 1st European Wireless Technology, Conference, October 2008, Amsterdam, The Netherlands.
[14] Learning and Adaptation in Cognitive Radios using Neural Networks, Nicola Baldo, Michele Zorzi, Publication in the IEEE CCNC 2008 proceedings.
[15] Cooperation and cognitive radio ,O. Simeone, J. Gambini, Y. Bar-Ness, U. Spagnolini,2006
[16] Cognitive Wireless Networks:Your Network Just Became a Teenager,Petri M¨ah¨onen, Marina Petrova, Janne Riihij¨arvi, Matthias Wellens,Department of Wireless Networks, RWTH Aachen University.
[17] Cognitive radio for net-generation wireless networks: An approach to opportunistic channel selection IEEE 802.11-based Wireless Mesh, DUSIT NIYATO, NANYANG TECHNOLOGICAL UNIVERSITY, KRAM HOSSAIN, IEEE Wireless Communications • February 2009
[18] COGNET: A Cognitive Complete Knowledge Network System, IEEE Wireless Communications • December 2008 B. S. MANOJ AND RAMESH R. RAO

Mr. S.C.Lingareddy is a PhD Student in Computer Science at Jawaharlal Nehru Technological University Hyderabad. Currently he is working as Assistant Professor and Head of the Department of Computer Science and Engg. KNS Institute of Technology, Bangalore. He received the B.E(CSE). degree from Karnataka University Dharwad and M.Tech.(CSE) degrees from Visvesvaraya Technological University Belgaum. in 1994 and 2004, respectively. He is a member of IEEE, ISTE. CSI, His research interests are Network Security, Information Security, Wireless sensor Network, Cognitive Radio Network.

Dr. B Stephen Charles received ME degree from Bharathiar University, Coimbatore and PhD from Jawaharlal Nehru Technological University Hyderabad. He published 18 International journal Papers and 2 National Journal papers,35 International conference papers.

He has 23 years of experience in Teaching, His area of interests are digital signal processing, Network Security ,Information Security, Wireless network.. He is working as a Principal in Stanley Stephen College of Engineering, Kurnool, His research

Dr. Vinaya Babu received ME from Osmania University Hyderbad in the year 1986, M.Tech,(CSE) ,PhD degree in Electronics and Communication from Jawaharlal Nehru Technological University, Hyderabad in the year 1992 and 2000 respectively. . He has a total of 30 publications in National and International Journals. He is a member of many Professional bodies like IEEE, IETE, ISTE, CSI and was the President and vice-President of Teachers Association, Has a total of 23 years of experience in Teaching. Dr.Vinaya Babu is currently serving as the Director of Admission And Professor of CSE., His area of interests are Algorithm ,Information Retrieval and Data mining, Computational Models,Computer Networks,Image Processing & Computer Architecture.

Mr. Kashyap Dhruve received his Bachelor of Engineering Degree in Electronics and Communication Engineering from Visvesvaraya Technological University Belgaum. He is currently working as a technical director in Planet-i Technologies. His areas of research interests are Information Security, Image Processing, Analog Design of Sensor Interface Circuts , Data Compression, Wireless Networks , Wireless Sensor Networks , Cognitive Networks.