iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1040

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Survey on evaluation of network management strategies and services in Emerging Wireless Networks

Potala Chandra sekhar[1]
[1]*Gitam University Visakhapatnam, India.*

Abstract*: The wireless networks play a major role in connecting the different devices and home networks. The usage of network or wireless networks rapidly increasing in scientific and in technology. The usage and requirements in emerging networks is controlled by different models like optical networks, storage networks, multimedia networks, grid networks, ad-hoc networks and wireless networks. In order to manage these networks one has to satisfy the following constraints like scalability, security, mobility, probability, context awareness. This paper describes the emerging trends in networks or wireless networks and management of wireless network strategies and services. This surveys on different business approaches in managing the Information technology strategies and includes different architectures followed to manage the networks.
Keywords: Security, wireless network, Scalability, wireless network strategies, management of wireless networks and mobility.

I. INTRODUCTION

Heterogeneity, network services, complexity of application, stemming from the growth in size, the combination of rapidly evolving technologies, increased requirements from corporate customers and pervasiveness are the new challenges being faced by network management. The Simple Network Management Protocol (SNMP), exemplified in the OSI reference model, the prevalent network management architecture, and the Telecommunications Management Network (TMN) management framework are the classical agent-manager centralized models over the past decade. A change in management paradigms from centralized and solutions that are able to cope with multiple autonomous management domains and local to distributed strategies and possibly conflicting management policies are the changes which are forced by the increasing trend towards enterprise application integration based on loosely coupled heterogeneous IT infrastructures. Service level agreements (SLA) that depend on the qualities of the underlying IT infrastructure and with end-to-end application level quality of service requirements used to get service-oriented business application. More recently, computing models and emerging network are used to amend control and network management requirements. The emerging environments may be categorized as the service and the network of the future with a large diversity of devices, service domains and networks. It is particularly crucial to develop the new architectures and models, to manage these services and networks, also enable new management technologies , which can cope with multi federated operations, resource constraints, dependability, context awareness, mobility, scalability, probability, security etc. In this scenario, the novel business approach for Information Technology (IT) management services also has a huge demand. The network evolution and their trends like the strategies of evolution of network management the challenges of emerging networks, service management and solutions in network management are surveyed in this paper.

II. ADVANCES IN NETWORKS

In recent times, the network evolution brings novel characteristics respect to today's networks and future networks, like:
Allowing access to mobile services and broadband nomadic, used for efficient and flexible radio access;
New forms of ad-hoc communications are managed with time-varying network topology and intermittent connectivity requirements;
The sub-networks are integrate at the edge, such as sensor and personal networks, and are possibly integrated to Internet for the benefit of humans;
It will enable intelligent distribution of services across different access technologies with distributed control or centralized by eliminating the barriers to broadband access;
Enable service composition and business domains and seamless end to end network and operation across multiple operators;
Support critical infrastructure and support high-quality media services, (e.g., for transport and energy), the existing networks will be gradually replaced or even significantly enhanced.

©IJRASET (UGC Approved Journal): All Rights are Reserved

The need to explore disruptive architectures to build future mobile and striking a balance between backward compatibility requirements to address the evolution from today's large legacy infrastructures to new infrastructures, broadband networks and associated service infrastructures are required in this version. The application and technical trends of networks could be:

A. Nomadic computing (Mobility)

Mobility in future network designs should consider both the services and terminals. The number of nomadic users and mobile networked devices will increase dramatically. Subsequently they have direct dynamic communication link and more devices and users are connected.

B. Wireless high speed networks

The network applications are being complemented with really low-cost wireless access and high-capacity alternatives for largest coverage for high speed access to networks and finest possible access granularity. Next generation Mobile WiMAX network can transmit data at a speed which is up to one gigabit per second while stationary, and 100 megabits per second in a moving vehicle are the examples.

C. Scalability

The new challenges to scalability are brought by increasing number of networks. Few examples are: the extension of modelling, network physical topologies, verification of business processes composed on SOA and validation; reliable management of composed services; execution of business processes and flexible evolution; service mediation and data, process and brokering, aggregation and data management.

D. Security (Trust

Security in modern network services are becoming one of the most important footstones. The trusted environments are created for the new service which the world will require: In order to detect and assess security risk, one has to participate in complex networks to monitor, analyze and display the information flows between different nodes. It provides safeguards, guarantees and rules to ensure trust, confidence and services created by end users, which leads to bring changes in the perception.

E. Interoperability

In different levels the Network interoperability is applied. The service interoperability has ability to integrate the largely stand-alone system services and with other services from business domain. The quality of service and understanding of the information is exchanged is done by semantic interoperability.

F. Context-awareness

It is used to design innovative user interfaces, and is often used as a part of ubiquitous and wearable computing. It is used to customize the intuitive communications services for mobile lifestyle and for users of the mobile and it provides intelligent services in an invisible manner to the users.

G. Autonomic Computing

It is used to gain a significant importance from autonomous machine to machine data communication besides human to human or human to machine communication. Now-a-days without human intervention, the business transactions are taking place in the network.

H. Integration

The network or wireless network data communication can be done by integrated with devices like television sets, phones, portable digital assistants, home appliances and few hardware devices. The users can access the information from all the devices by using this network from anywhere in the world.

I. Expanded Services

It comprises of different components like variety of players which are running over decentralized hosting infrastructure and which includes end user devices like Servers, PC, networking and storage devices. This leads to way for integration of service and network

©IJRASET (UGC Approved Journal): All Rights are Reserved

framework for network convergence among the players in new business models. The openness, do it yourself innovative services and knowledge management will allow the people to access the true center of information society.

III. EMERGING CHALLENGES FOR NETWORK MANAGEMENT AND SERVICES

The network management is required in emerging networks to meet the following requirements like the increasing pervasiveness of mobility and wireless technologies. In order to access the data, one has to increase the processing speed and the memory to support different devices in the network. Now-a-days, due to digitization, there is a lot of increase in digitized media, which leads to increase in the content, data search and data handling is difficult in an organization. In order to access the data one has to find the location of the end user for security purposes. The users of network services have to reveal his identities for security reasons and these services are maintained by network management. The International Organization for Standardization (ISO) suggested important areas in the network management and these areas are useful in organizing and managing the networks and wireless networks. The following are:

A. Fault Management

It is used to find isolation, correction and detection operations in the Open Systems Interconnection (OSI) environment. To manage the complex network, one has to identify the essential components of the whole system and check the working condition of each component in the whole network. If the fault occurs in the network then immediately one has to separate the component from the whole network. By separating this component one can isolate the rest of the network from failure and it will not effect the functionality of the whole system. Reconfigure or modify the network in such a way as to minimize the impact of operation without the failed component or components. Repair or replace the failed components to restore the network to its initial state. Central to the definition of fault management is the fundamental concept of a fault. Faults are to be distinguished from errors. A fault is an abnormal condition that requires management attention (or action) to repair .A fault is usually indicated by failure to operate correctly or by excessive errors. For example, if a communications line is physically cut, no signals can get through. Or a crimp in the cable may cause wild distortions so that there is a persistently high bit error rate. Certain errors (e.g., a single bit error on a communication line) may occur occasionally and are not normally considered to be faults. It is usually possible to compensate for errors using the error control mechanisms of the various protocols.

The Users of the network are expecting fast and reliable problem resolution and the most of the end users will tolerate occasional outages. When these infrequent outages do occur in the network then the user expects to receive immediate notification, solution and expects that the problem will be corrected almost immediately. In order to provide immediate resolution one requires very rapid and reliable fault detection and diagnostic management functions. By using the redundant components, one can minimize the impact and duration of faults and by using the alternate communication routes to give the network a degree of fault tolerance. The fault management capability itself should be redundant to increase network reliability. Users expect to be kept informed of the network status, including both scheduled and unscheduled disruptive maintenance. Users expect reassurance of correct network operation through mechanisms that use confidence tests or analyze dumps, logs, alerts, or statistics. After correcting a fault and restoring a system to its full operational state, the fault management service must ensure that the problem is truly resolved and that no new problems are introduced. This requirement is called problem tracking and control. As with other areas of network management, fault management should have minimal effect on network performance.

B. Accounting Management

The financial charges of networks are also plays important role in managing the networks and one has identify the cost of those managed objects. In large enterprise networks, cost centers (individual divisions or even individual project accounts) are charged for the use of network services. These are internal accounting procedures rather than actual cash transfers, but they are important to the participating users nevertheless. Furthermore, even if no such internal charging is employed, the network manager needs to be able to track the use of network resources by user or user class for a number of reasons, including the following:

1) a user or group of users may be abusing their access privileges and burdening the network at the expense of other users.
2) Users may be making inefficient use of the network, and the network manager can assist in changing procedures to improve performance.
3) The network manager is in a better position to plan for network growth if user activity is known in sufficient detail.

The network manager needs to be able to specify the kinds of accounting information to be recorded at various nodes, the desired interval between successive sending's of the recorded information to higher-level management nodes, and the algorithms to be used in calculating the charging. Accounting reports should be generated under network manager control. To limit access to accounting

©IJRASET (UGC Approved Journal): All Rights are Reserved

information, the accounting facility must provide the capability to verify users' authorization to access and manipulate that information.

C. Configuration Management

This management is used to collect the data, identify and provide data to the objects in order to assisting in providing for continuous operation of interconnection services. The latest data communication networks are composed of logical subsystems and individual components (e.g., the device driver in an operating system) that can be configured to perform many different applications. For example, the same device can be configured to act either as a router or as an end system node or both. Once the device is selected for configuration then the configuration manager can choose the particular software and set of attributes and values (e.g., a transport layer retransmission timer) for that device. The initialization of a network and gracefully shutting down part or all of the network is done by the Configuration management. It is also concerned with adding, maintaining and updating the relationships among components and the status of components themselves during network operation.

It is often desirable for these operations on certain components to be performed unattended (e.g., starting up or shutting down a network interface unit). The network manager needs the capability to identify initially the components that comprise the network and to define the desired connectivity of these components. Those who regularly configure a network with the same or a similar set of resource attributes need ways to define and modify default attributes and to load these predefined sets of attributes into the specified network components. Basing on the needs of user, the network manager needs the capability to change the connectivity of network components. Reconfiguration of a network is often desired in response to performance evaluation or in support of fault recovery, network upgrade, or security checks. Users often need to, or want to, be informed of the status of network resources and components. Therefore, the users have to get notifications, whenever the changes occur in configuration management. The reports of the Configuration can be generated either on some routine periodic basis or in response to a request of the user for specific a report. The users often want to inquire about the upcoming status of resources and their attributes before reconfiguration. Network managers generally prefer authorized users or operators to control and manage network operation which includes software update and distribution.

D. Performance Management

This management is used to evaluate the behavior of components and objects and used to calculate the effectiveness of communication activities. In recent network system, is used to share data resources and to communicate data between various components. The effectiveness of an application that the communication over the network be within certain performance limits. The two broad functional categories monitoring and controlling are used to test the performance management of a computer network. In the performance management, the monitoring function is used to track the activities on the network and the controlling function makes some adjustments to improve network performance in the the performance management. The following are the performance issues related to network manage are:

What is the level of capacity utilization? 2) Is there excessive traffic? 3) Has throughput been reduced to unacceptable levels? 4) Are there bottlenecks? 5) Is response time increasing?

In order to deal above issues, the network manager has to concentrate on initial resources and these are monitored to calculate the performance levels. The different levels of performance are depending on the appropriate metrics and values with relevant network resources. Performance management must monitor many resources to provide information in determining network operating level. The information is gathered and it is used to analyze and by using the resultant analysis as feedback to the prescribed set of values. The network manager can become more and more adept at recognizing situations indicative of present or impending performance degradation. In order to implement particular application in the network, one has to know the worst case and average response and reliability of the network services. On must have clear cut idea on performances then one can respond to the user queries. The End users of the network services always managed to produce their applications consistently good response time. The performance statistics in the network management are used to manage, planning and maintain large networks. These Performance statistics are used to find the bottle necks before creating the problems to end users in the network. In order to solve the above, one has to take appropriate action and it is in the form changing the routing tables or redistribute traffic load on the network during the peak use times or fault is identified in rapidly growing load in one location. This can solved by expanding the lines in that area.

E. Security Management

It always related with distributing, generating and storing encryption keys. The authorization or access control information and passwords must be maintained properly to safe guard the information. It is concerned with controlling access and monitoring access

©IJRASET (UGC Approved Journal): All Rights are Reserved

to computer networks and access to all parts information of the network management can be obtained from the network nodes. Security management always involved with storage, collection, examination audit records and logs of the security tool. These are enabled and disabled of logging facilities makes the system more secured in the network management. This provides facilities for user information protection of network resources. The authorized users should be provided with Network security facilities and every user should know the proper security policies that are in force and effective.

F. Network Inventory Management

It is the process of keeping all records of IT or network assets that make up the network. It enables network administrators to have a physical record of all Information Technology and network equipment within the organization. It can implemented through IT asset tracking software which is used to scans records the data and compiles the data of each node/device in the entire network. It may include:

1) Number of routers, their make, type, serial number and place of installation.
2) IP addresses of all nodes/ devices, IP addressing scheme used.
3) Number and type of software along with expiry dates and license keys.

This data helps businesses with:

4) Network capacity planning, Network size estimation.
5) Network ROI/ cost estimation.
6) Physical network administration (to deal with device/equipment loss and theft)

The four ways in inventory management system will help protect any company's largest asset in entire computer network and they are as follows:

a) *Information theft :* A network inventory management system not only keeps track of software and hardware. It also finds those who are having an access to that software. A regular check of your system's inventory will let you know who has downloaded and once the used software they may not be authorized to use.
b) *Equipment theft :* A network management system will track and detect every piece of software and equipment connected to the system. And it will also help us to know which components are not working properly, which components have mysteriously disappeared and which components need to be replaced. This is used to eliminate theft in workplace by running a regularly scheduled inventory check
c) *Licensing agreements:* An inventory of licensing and software agreements will let us know if you've got the necessary licensing agreements for all software's in network. Insufficient licensing can cost fines, usage fees and duplicating software that you already have is an unnecessary expense.
d) *System Upgrades:* Outdated software and equipment can cost company money, time and resources. slow response times and Downtime are two of the biggest time killers of the business. Set filters on the network inventory management system to alert, when it's time to replace hardware or upgrade software with upcoming technology to keep the system running efficiently and smoothly.

IV. CONCLUSION

The Emerging networks and wireless network has following features to enhance the speed and access the data from the network and they are diffusion of heterogeneous nodes and devices, mobility, mass digitization, multi-federated operations, dependability, scalability, security, context awareness, new models of services and improved with security and privacy. These features produce the networking architectures, new technologies and exhibits different challenges to provide different services, security and management. The new management standards and technologies should be implemented to satisfy the current requirements and to manage emerging networks. The potential candidates are identified in the network management based on the artificial intelligence techniques, bio-inspired approaches and policy-based management strategies. In order to keep control complex network systems, It is always necessary for Information Technology industry to move to context-aware management, autonomic management and self-management systems the technology itself will manage the all the business transactions in the network similar to the humans in different technology.

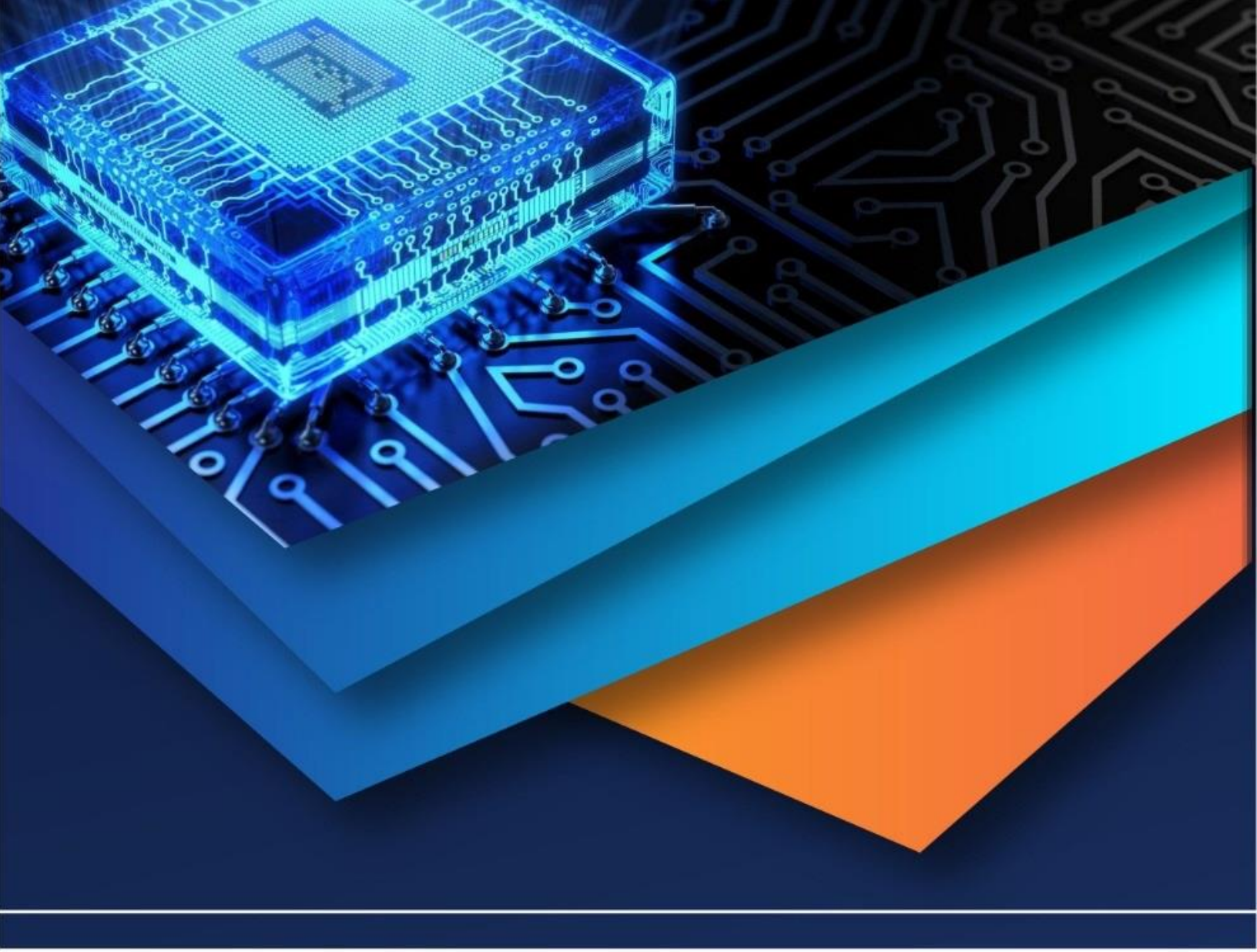
REFERENCES

[1] M. H. Ali. Phenomenon-aware sensor database systems. In Proc. of the EDBT Ph.D. Workshop, March 2006.
[2] M. H. Ali,W. G. Aref, R. Bose, A. K. Elmagarmid, A. Helal, Kamel, and M. F. Mokbel. Nile-pdt: A phenomena detection and tracking framework for data stream managementsystems. In VLDB, Sept. 2005.

©IJRASET (UGC Approved Journal): All Rights are Reserved

[3] KS Rao, P Chandra Sekhar, PS Rao, "Image Segmentation for Animal Images using Finite Mixture of Pearson type VI Distribution" Global Journal of Computer Science and Technology 14 (3), 2014.
[4] KS Rao, P Chandra Sekhar, MS Sayee "Text Independent Speaker Identification Model using Pearsonian System of Models and K-Means Algorithm" Journal of Innovation in Computer Science and Engineering 3 (2), 2014.
[5] P Chandra Sekhar, KS Rao, PS Rao, "Image Segmentation Algorithm for Images having Asymmetrically Distributed Image Regions" International Journal of Computer Applications 96 (21), 2014.
[6] M.H. Ali, W.G. Aref, I. Kamel. Scalability Management in Sensor Network Phenomena Bases. Proc. of the 18th International Conference on Scientific and Statistical Database Management, pages 91-100, 2006.
[7] I.F. Akyildiz, J. McNair, J.S.M. Ho, H. Uzunalioglu, Wenye Wang. Mobility management in next-generation wireless systems.
[8] PROCEEDINGS OF THE IEEE, VOL. 87, NO. 8, pages 1347-1384, 1999.
[9] EIA/TIA, “Cellular radio-telecommunications intersystem operations, ”EIA/TIA, Tech. Rep. IS-41 Revision C, 1995.
[10] “Mobile station-land station compatibility specification,”EIA/TIA, Tech. Rep. 553, 1989.
[11] “Cellular system dual-mode mobile station–Base station compatibility standard,” EIA/TIA, Tech. Rep. IS-54, 1992.
[12] Manish Anand, Edmund B. Nightingale and Jason Flinn. Self-tuning wireless network power management. Proc. of the 9th annual international conference on Mobile computing and networking, pages: 176 - 189, 2003.
[13] Box, D., Ehnebuske, D., Kakivaya, G., Layman,A., Mendelsohn, N., Nielsen, H. F., Thatte, S.,and Winer, D. Simple Object Access Protocol(SOAP) 1.1. Tech. rep., W3C Note, May 2000.
[14] Chandra, S. Wireless network interface energyconsumption implications of popular streaming formats. In Proceedings of Multimedia Computing andNetworking (San Jose, CA, 2002), pp. 85{99.
[15] Cisco Systems, Inc. Cisco Aironet wireless LAN client adapters installation and con_guration guide for Linux.
[16] Traian Avram, Seungchan Oh, Salim Hariri. Analyzing Attacks in Wireless
[17] Ad Hoc Network with Self-Organizing Maps. Proc. of the FifthAnnual Conference on Communication Networks and Services Research, pp.166-175, 2007.
[18] D. Djenouri, L. Khelladi, and A. N. Badache, "A surveyof security issues in mobile ad hoc and sensornetworks," IEEE Communications Surveys & Tutorials,vol. 7, pp. 2-28, 2005.
[19] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," 1999.
[20] B. SUN, "INTRUSION DETECTION IN MOBILE AD HOC NETWORKS," Texas A&M University, 2004.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)