A Review on MANET using Soft Computing and Dempster-Shafer Theory

Naveen Pathak, Anand Bisen

Abstract: Mobile ad hoc networks (MANETs) is an substructure-less, dynamic network include of a sets of wirelessly mobility nodes which communicate with all different without the exploit of any centralized authority. Because of its fundamental characteristics, like as wireless medium, dynamic topology, distributed cooperation. In this paper we study MANET and its characteristics, application, security goals and different types security attacks, soft computing approach and dempster-shafer theory of evidence .

Keywords: MANET; soft computing appproch; dempster-shafer theory of evidence;

I. INTRODUCTION

Wireless networks are growing frequently because of their physical benefits over traditional wired communication networks. In this, network devices are linked with a wireless medium for communicating each other. Broadly, wireless communication can be categorized in two parts with infrastructure and infrastructure less. WANET (wireless ad hoc network) is defined by its own characteristics; it is self-organizing, mobile communication manner where topologies are dynamically created. On account of ad hoc nature of the network framework and mobility it is still a territory of new innovative work. Due to wireless communication mobility two major issues are found in such kind of network i.e. performance and security [1].

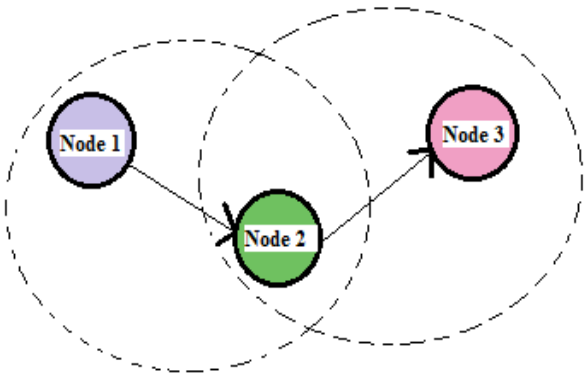

Fig. 1 Example of MANET

II. MANETS CHARACTERISTICS

A. Distributed Operation

There isn't background network for central control of n/w operations; manager of network is dispensed among devices.

B. Multi hop Routing

When a node tries to ship information to other nodes which is out of its verbal exchange variety, the packet will have to be forwarded via one or more intermediate nodes.

C. Self-Sufficient Terminal

In MANET, every mobile node is an impartial node, which would perform as both a host and a router [2].

D. Dynamic Topology

Nodes are free to the move arbitrarily with specific speeds; as a consequence, the network topology could alternate randomly and at unpredictable time.

E. Light-Weight Terminals

In maximum circumstances, the nodes at MANET are mobile with much less CPU potential, low power storage and small memory measurement.

F. Shared Physical Medium

Wireless correspondence medium is out there to any element with plentiful resources and appropriate hardware. For that reason, access to the channel can't be confined

III. ADVANTAGES OF MANET

The advantages of an Ad-Hoc network incorporate the next:

- They provide access to knowledge and services regardless of geographic function.
- Scalable contains the addition of extra nodes.
- Expanded Flexibility.
- Strong due to decentralize administration.
- The network can be also set up at any time and situation.

Revised Version Manuscript Received on February 14, 2017.

Naveen Pathak Department of Computer Science, Vikrant Institute of Technology & Management (VITM), Gwalior (M.P)-474006, India. Email: nvnpathak9@gmail.com

Anand Bisen, Department of Computer Science, Vikrant Institute of Technology & Management (VITM), Gwalior (M.P)-474006, India. Email: bisenanand82@gmail.com

IV. DISADVANTAGES OF MANETS

- Physical security and Limited resources.
- Inherent shared trust prone to attacks.
- Lack of approval administrations.
- Volatile network topology makes this difficult to watch malicious devices.
- Security protocols for wired networks cannot work for ad hoc networks [3].

V. SECURITY GOALS

Security concludes an investments collection that is adequately funded. Every networking services equivalent to routing in addition packet forwarding are carried out via devices themselves in self-organizing method in MANET. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if MANET is secure or not are as follows:

A. Availability

Availability approach the belongings are accessible to the authorized parties at proper times. Availability applies both to data and to services. This ensures survivability of network service regardless of Dos attack.

B. Confidentiality

Confidentiality ensures that pc-associated assets are accessed simplest by means of authorized parties. That is, simplest those who need to have access to something will genuinely get that get right of entry to. To preserve confidentiality of some confidential understanding, we have got to hold them secret from all entities that shouldn't have privilege to access them. Confidentiality is repeatedly called privacy or secrecy.

C. Integrity

Integrity signifies that belongings may also be modified most effective with the aid of authorized parties or only in authorized way. Modification entails writing, altering repute, deleting and creating. Integrity assures that a message being transferred is by no means corrupted.

D. Authentication

Authentication enables a nodal to make sure the individuality of peer nodal it's communicate with. Authentication is almost assurance which participants in communication are authenticated also not impersonators. Authenticity is ensured since only legit sender can create information with a purpose to decrypt competently with the shared key.

E. Anonymity

Anonymity manner all information that can be used to determine proprietor or current person of node must default be kept private and no longer be distributed through node. itself or the system software.

F. Authorization

This property assigns different access rights to different types of users. For instance a network management will also be performed via network administrator handiest.

VI. SECURITY IN MANET

MANET is distinguishing thru the fixed substructure lack, quick topology modify and highest nodal mobility. These characteristics investigate that wireless ad hoc network is extra susceptible to malicious attacks than the usual internet. The vulnerabilities are as a rule triggered through the following motives [4] using wireless links makes the network susceptible to attacks ranging from passive eavesdropping to active interfering. It's not like what is in traditional wired networks that attackers have to physically access the wires or get through several defense lines at firewalls or gateways.

- Mobile nodes able to roam independently make them easier to be captured, compromised and hijacked. Considering that monitoring down a precise mobile node in a huge-scale ad hoc network might be difficult, attacks via a compromised node from within the network are a ways extra unsafe and much harder to detect. Creating and maintaining trust among peer nodes is also difficult and thus Byzantine failure should be prevented.
- Due to lack of centralized mechanisms in ad hoc network and various algorithms rely on cooperative participation of all devices, adversaries may take benefit of this vulnerability for brand spanking new forms of attacks designed to interrupt the cooperative algorithms.
- Most ad hoc routing algorithms are additionally cooperative in nature, which is in contrast to with a wired network, the place extra defense can also be positioned on gateways and routers. Due to these characteristics, the MANETs have tougher safety requirements than the normal, wired and static internet. One of the most severe threats to the routing in ad hoc networks is attack from compromised nodes, which could exert unpredictable and undetectable Byzantine failures.

VII. PROTOCOLS

A. Destination Sequenced Distance Vector (DSDV)

DSDV is a table-driven routing arrangement checking the Bellman-Ford algorithm and planned for ad hoc mobile networks the change made to the Bellman-Ford algorithm incorporates liberation from circles in routing tables by utilizing succession numbers. A record of the table include location identifier of a destination, briefest called separation metric to that target measured in hop checks and the location identifier of the node that is the main hop on the most limited way to the destination. A succession number is likewise connected with every route/path to the destination.

B. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for remote cross section organizes and depends on a technique known as source steering. But one distinction that every middle of the intermediate node that communicates a course asks for packet adds its uncommon location identifier to a rundown conveyed in the packet. The destination node then produces route reply information that contains the rundown of locations got in the route request and transmits it back along the same way to the source.

C. Optimized Link State Routing (OLSR)

OLSR is an optimized version of a conventional link state protocol in which potential changes in topology cause the flooding of the topological info to each obtainable hosts inside the n/w. In addition, as OLSR constantly maintains routes to all destinations in the network, the protocol is advantageous for traffic patterns where a huge nodes subset are speaking with another vast subset of nodes, and where the [source, destination] couples are changing after some time. OLSR protocol is reciprocal for the application which does not permit the long delays in the transmission of the data packets.

D. Ad hoc on demand distance vector (AODV)

AODV is essentially a combination of both DSR and DSDV. It detects the basic on- demand system of Route Maintenance and Route Discovery from DSR, and in totaling the hop-via-hop routing utilization, set numbers, and rambling guides from DSDV [16].

VIII. SOFT COMPUTING APPROACH

In this paper, are providing a comprehensive review of three soft computing approaches to improve quality of service and route optimization in MANET.

A. Neural Network

An Artificial neural network is a biological network, capable of thinking, reasoning, decision-making and a high degree of parallelism. It draws inferences from a considerable storehouse of knowledge and experience received over a time frame in fixing issues. It may go with obscure also sick-described parameters in arriving at solutions. It will probably work with imprecise and in poor health-outlined parameters in arriving at options Fuzzy Logic and GA are additional ingredients which may also create an ANN more aggressive and powerful in solving unsolvable issue thru analytical technique [5].

Truly, the most significant characteristic of NEURAL is the uniform distribution of the information around the node's vicinity centered on the current alterations in nearby. Motivated through the biological worried process, artificial Neural System (ANS) and neural networks are being applied to be taught a large kind of issues within the areas of engineering and business [6][7][8].In a ANS approach, the know-how is propagated between neurons making use of electrical stimulation alongside dendrites. Excessive stimulation signal produces an output to the other neighbor neurons and so the knowledge takes the proper strategy to the destination, where a response will arise. In this approach, [9] authors have proposed Kohonen Model [10] for Self-Organizing Systems.

The conjunction of three phases, that think algorithms usually useful in the region of NN, confer efficient and robust tools to be implement in NEURAL. Sooner or later, the efficiency of a trust mechanism is carried up in the studying module.

Illustrates in regards to the schematic structure for NEURAL. It consists of two modules:

- Preprocessing Module
- Route discovery module

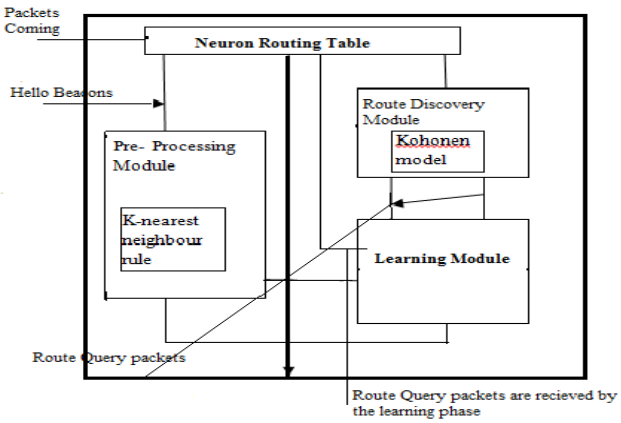

Fig. 2 Schematic Architecture for NEURAL

1) Preprocessing Module

Preprocessing module adapts the KNN rule sensing the continuously topology modify of the n/w that is depend on sending hello requests and reply packets during an interval of time.

2) Route Discovery Module

- Kohonen model, that it's exploited to elect the next route in the MANET n/w depend on a competitive learning process. Route discovery phase is divided into three steps:
- Broadcasting
- Selection of the "winner"
- Adaptation

B. WMN

WMN (Wirelessly mesh network) distinct changes of MANET make a probability to implement various novel wirelessly grids. One of them is WMN. WMN are rapidly diffuse, dynamically self-healing; self-organizing, self-balancing, self-configuring and self-aware multi hop networks. One in every of them is a WMN. WMN are quickly diffuse, dynamically self-organizing; self-cure, self-balancing, self-mindful and self-configuring multi hop networks. In these networks every node (stationary or mobility) has the ability to add and make a grid automatically via sensing nodes with a similar capability within its radio range.

C. Fuzzy Based Genetic Approach

This is also another soft computing method for route optimization in MANET. In this work authors have presented the choice of the subsequent cross over child path will be recognized depend on cyclic fuzzy logic. The entire process will optimize the routing algorithm to increase the QOS. Authors have presented genetic depend methods to construct the grid path for the route building in an optimize method. Finally mutation will be performed. In this work, the choice of the subsequent cross over child path will be recognized depend on fuzzy logic. The fuzzy logic will be carried out beneath the parameters of energy and the space specification.

IX. DEMPSTER-SHAFER THEORY OF EVIDENCE

Dempster-Shafer mathematical theory of proof is both thought of evidence as well as theory of possible reasoning. The measure of perception models the evidence, while Dempster's rule of mixture is the system to aggregate and summarize a corpus of evidences. Nevertheless, previous research efforts establish many obstacles of Dempster's rule of combination

- Associative For A non-associative combo rule is essential for a lot of cases
- None weighted DRC implies that we believe all evidences equally. However, virtually, our trust on exceptional evidences could range. In other words; it means we should consider various factors for each evidence.

Yager and Yamada and Kudo proposed rules to mix a number of evidences presented sequentially for the primary problem. Wu et al. recommended a weighted combo rule to manage the second predicament. However, the burden for extraordinary evidences in their proposed rule is ineffective and inadequate to distinguish and prioritize unique evidences in terms of safety also criticality. Our extended Dempster-Shafer theory using importance reasons may overcome each of aforementioned limitations.

1. Importance Factors and Belief Function

At the point when suggestion relates to a subset of a casing of wisdom, this infers a particular edge recognizes recommendation. In the first place, we present a proposition of essentialness.

Definition1. Importance aspect (IF) is an optimistic actual number related to the significance of evidence. If are derived from historic observations or proficient experiences.

Definition2. A proof E is a 2-tuple hm; IFi, where m describes fundamental probability challenge [11].

Definition3. Multiplied D-S evidence model with significance reasons: suppose E1=<m1, IF1> and E2 =< m2, IF2> are two independent evidences. Then, the mixture of E1 and E2 is E = <m1 Θ m2,(IF2+IF2)/2>, the place Θ is Dempster's rule of blend with importance factors.

Believe Bel1 and Bel2 are belief services over the equal frame of discernment, with common probability assignments m1 and m2 [12]. The importance causes of these evidences are IF1 and IF2. Then, function m outlined through suggested DRCIF is non-associative for a couple of evidences. Therefore, for the case in which sequential information is not available for some instances, it is necessary to make the result of combination consistent with multiple our combination algorithm supports this necessity and our algorithm complexity is O (n), where n is the evidences quantity [13]. It recommends that our multiplied Dempster-Shafer theory demands no extra computational price compare to a naıve fuzzy-founded system. The algorithm for combo of multiple evidences is built as follows:

Algorithm1. MUL-EDS-CMB

INPUT: Evidence pool Ep

OUTPUT: One evidence

1.jEpj¼ sizeof(Ep);
2. While jEpj> 1 do
3. Decide upon two evidences with the least IF in Ep, named E1 and E2;
4. Combine these two evidences, E =<m1 Θ m2, (IF1 + IF2)/2>;
5. Dispose of E1 and E2 from Ep;
6. Add E to Ep;
7. Finish
8. Return the evidence in Ep[14].

With references of base paper Using anomaly based intrusion detection system results in the false positive identification of the intrusion. Computing trust value for each node in the network leads to higher computational complexity. Combining trust value along with intrusion detection system can reduce the pitfalls of both methods. A comparative study of exploiting only anomaly depend IDS and combination of trust value along with an anomaly depend IDS is performed. The proposed anomaly detection system uses ANN and Dempster-Shafer theory to confirm the attack occurrence in the network [15].

X. LITERATURE SURVEY

In the year 2014, V.G. Muralishankar MANETs are separately self-prepared n/w without substructure aid. Devices move arbitrarily; thus network could experience fast and unpredictable topology changes in MANET. Since nodes in a MANET on the whole have constrained transmission degrees, some nodes are not able to keep up a correspondence directly with each and every different. Consequently MANET has the accountability to act as a router. This thesis is a survey of active project work on routing protocols for MANET [16].

In the year 2014, R. RagulRavi MANET is set of multi-hop wireless devices which keep up a correspondence with all other without established infrastructure or centralized manage. The wireless links in MANET are error inclined and may go down in most cases due to less infrastructure, interference and mobility of nodes. Therefore, in MANET routing is a critical task as a result of totally dynamic atmosphere [17].

In the year 2013, Alex Hinds The broaden in availability and popularity of mobile wireless devices has lead researchers to increase a large style of MANET protocols to take advantage of the detailed communication opportunities presented by means of these devices. Gadgets are equipped to be in contact directly utilizing the wireless spectrum in a peer-to-peer fashion, and route messages by way of intermediate nodes, however the character of wireless shared communication and mobile contraptions effect in lots of routing and protection challenges which need to be addressed before deploying a MANET. We examine range of MANET routing protocols available and discuss functionalities of several ranging from early protocols equivalent to DSDV to more developed such as MAODV, our protocol study centers upon works by means of Perkins in setting up and enhancing MANET routing in this thesis. Range of literature in case of field of MANET routing used to be reviewed and recognized, we additionally reviewed literature on subject of securing AODV centered MANETs as this can be probably the most trendy MANET protocol. The literature review identified a number of developments within research papers reminiscent of extraordinary use of the random waypoint mobility model, except key metrics from simulation outcomes and now not evaluating protocol performance against obtainable alternatives [18].

In the year 2013, Boaz Benmoshe MANET does now not have constant infrastructure, all single node in n/w works as each a transmitter and a receiver. Nodes directly keep up a correspondence with every other when they are each within their communiqué degrees. As MANET does not require any fixed infrastructure and it's in a position of self-configuring, these specified characteristics made MANET best to be deployed in a far off or mission central subject like military use or far off exploration. Nonetheless, the open medium and extensive distribution of nodes in MANET go away it susceptible to more than a few ways of attacks [19].

In the year 2012, author Parimal Kumar Giri has proposed the neural network based approach for MANET. He located a number of makes an attempt utilizing neural networks, namely Hopfield Neural Networks(HNNs), have been made to clear up or furnish an approximate strategy to the Shortest Path problem faster than would be viable with any algorithmic answer, counting on the Neural Networks(NNs) parallel architecture [20].

In the year 2012, Adnan Nadeem MANETs are liable to quite a lot of attacks at all layers, together with in precise the network layer, when you consider that the design of most MANET routing protocols suppose that there's no malicious intruder nodal in the n/w. In this thesis, we present a survey of the predominant types of attack at the network layer, and we then evaluation intrusion detection and safety mechanisms which have been not compulsory in literature. We categorize this machine as both element detection algorithms which deal with a sole sort of attack, or as IDSs which can deal with a range of attacks. A comparison of the proposed protection mechanisms is also included in this thesis. As a final

point, we identify areas where other research could concentration [21].

In the year 2012, Adnan Nadeem Ad hoc networking proposition won't be new one, having been around in various assortments for more than 20 years. More often than not, tactical networks had been the one communication networking utility that followed the ad hoc paradigm. Just lately, the introduction of recent applied sciences such because the Bluetooth, IEEE 802.11 and Hyperlink are serving to enable eventual business MANET deployments external the navy domain. Latest evolutions had been generating renewed as well as growing interest within progress and research of MANET.This first explains predominant position which MANET play in evolution of future wireless applied sciences. Then, it studies the modern study pursuits in these areas of MANET_s traits, capabilities and applications [22].

In the year 2010, Siddesh. G.K et al. in this work, they have got performed simulation utilizing hyper web simulator for quite a lot of present protocols like proactive routing, reactive routing, hybrid routing .Writer have completed that it appears reasonable to suppose which the essential ingredients of ANN with FL and GA go a long way in improving performance of protocol in most dramatic terms [23].

B.Praveen Kumar It offers rise to many new purposes. Up to now of few a long time, now we have noticeable the advancement in wireless networks. The emerging capabilities of mobile devices have given a brand new direction to the web, which decreases the cost and allow us to make use of infrastructure wireless networks and foundation considerably less wireless networks (i.e. MANET) with so many purposes that MANETs presents us, there are nonetheless some challenges that have got to overcome. The infrastructure less and the dynamic nature of those networks demands new set of networking tactics to be implemented with the intention to provide efficient end to end communiqué. It along with diverse application of networks in many different scenarios akin to disaster restoration and battlefield, have noticeable MANET being researched by using many extraordinary firms and institutes. MANETs rent the normal TCP/IP structure to provide end-to-end verbal exchange between nodes. In MANET, One exciting research area is routing. Routing within MANETs is challenging project also has received a colossal quantity of attention from researches. Because of lack of defined critical authority, securitizing routing method becomes challenging venture thereby leaving MANET at risk of attack, which outcome in disintegration in execution attributes and raises a genuine inquiry mark about dependability of such networks. In this thesis, we furnish the history of MANET, challenges (disorders) involve in MANET and its some purposes and a summary of a broad variety of routing protocols proposed [24].

XI. PROBLEM STATEMENT

MANET is one of the growing fields of research there are huge amount work complete regarding this field problem of existing work is that it classify true node as false node which called false detection and in existing work no security mechanism provide to send data over network. Overcome this problem we proposed a secure D-S for detect attacks and prevent network by these attacks in MANET.

XII. CONCLUSION

The evolution in the field of mobile computing is driving a new alternative way for mobile communication, in which mobile devices form a self-creating, self-organizing and self-administering wireless network, called a mobile ad hoc network. MANETs are expected to be very useful and important infrastructure for achieving future ubiquitous society. Designing MANET protocols and applications is a very complicated task since it is hardly possible to build large-scale and realistic test beds in real world for performance evaluation.

REFERENCES

1. PriyankaGoyal, VintiParmarand Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Applications”, IJCEM, Vol.11, January 2011
2. Aarti, Dr. S. S. Tyagi “ Study of MANET: Characteristics, Challenges, Application and Security Attacks” Volume 3, Issue 5, May 2013.
3. C. R. Lin and M. Gerla, “Adaptive Clustering for Mobile Wireless Networks,” IEEE JSAC, vol. 15, pp. 1265–75, Sept. 1997
4. Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003, pp. 13–6
5. HaoYang, Haiyun& Fan Ye ― Security in mobile ad-hoc networks : Challenges and solutions,‖, Pg. 38-47, Vol 11, issue 1, Feb 2004.
6. Bin Lu and Udo W. Pooch, “Cooperative Security-Enforcement Routing in Mobile Ad Hoc Networks,” in proceedings of the 4th IEEE International Conference on Mobile and Wireless Communications Network (MWCN 2002), Stockholm, Sweden, September 2002, pp.157 – 161.
7. Siddesh.G.K,K.N.Muralidhara,Manjula.N.Harihar,2011. Routing in Ad Hoc Wireless Networks using SoftComputing techniques and performanceevaluation using HypernetsimulatorInternational Journal of Soft Computing and Engineering (IJSCE)ISSN: 2231-2307, Volume-1, Issue-3, July 2011.
8. A. Skabar and I. Cloete,2001. Discovery of financial traading rules. In Proc. Artificial Intelligence and Applications (AIA2001), pages 121–125, Marbella, Spain.
9. I. Cloete and A. Skabar,2001. Feature selection for financial trading rules. In Proceedings of 13th.EuropeanSimulation Symposium:Simulation in Industry, pages 713–717, Marseille,France,
10. Parimal Kumar Giri, Member,IACSIT,2012.A Survey on Soft Computing Techniques forMulti-Constrained QoS Routing in MANETIJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 03, ISSUE 02, MANUSCRIPT CODE: 130103.

11. T. Kohonen,1982. Self-organized formation of topologically correctfeature maps. Biological Cybernetics, 43:59–69.
12. Jaspal Jindal Vishal Gupta Associate Professor in ECE Deptt. M.Tech (ECE) Student P.I.E.T College Smalkha (Panipat) ,2013. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June2013 ISSN: 2277 128X,June 2013
13. Sharad Sharma, Shakti Kumar and Brahmjit Singh,1,3Deptt. of Electronics & Communication Engineering, National Institute ofTechnology,Kurukshetra, India2Computational Intelligence (CI) Lab, IST Klawad, Yamunanagar, India2013. Routing in Wireless Mesh Networks: Two Soft Computing Based Approaches. International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.3, June 2013DOI: 10.5121/ijmnct.2013.3304 29.
14. Luis Bernardo, Rodolfo Oliveira, Sérgio Gaspar, David Paulino and Paulo Pinto A Telephony Application for Manets: Voice over a MANET-Extended JXTA Virtual Overlay Network
15. Indira N, "Establishing a secure routing in MANET using a Hybrid Intrusion Detection System", 978-1-4799-8159-5/14/$31.00©2014 IEEE.
16. V. G. Muralishankar, Dr. E. George Dharma PrakashRaj"Routing Protocols for MANET: A Literature Survey" ©2014, IJCSMA All Rights Reserved, www.ijcsma.com.
17. R.RagulRavi , V.Jayanthi "A Survey of Routing Protocol in MANET" R.RagulRavi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1984-1988.
18. Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)" International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.
19. Boaz Benmoshe, Eyal Berliner. AmitDvir "Performance Monitoring Framework for Wi-Fi MANET" 2013 IEEE Wireless Communications and Networking Conference (WCNC): SERVICES & APPLICATIONS
20. Parimal Kumar Giri, Member,IACSIT,2012.A Survey on Soft Computing Techniques forMulti-Constrained QoS Routing in MANETIJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 03, ISSUE 02, MANUSCRIPT CODE: 130103/2012.
21. Adnan Nadeem "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks"2012.
22. Adnan Nadeem "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks"2012.
23. S. A. Ade & P. A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSRRouting Protocols in Mobile Ad Hoc Networks", International Journal of Information Technology and Knowledge Management, July-Dec 2010, Volume 2, No. 2, pp. 545-548
24. B.Praveen Kumar P.ChandraSekharN.PapannaB.BharathBhushan "A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS" P Chandra Sekhar et al, Int.J.Computer Technology & Applications,Vol 4 (2),248-256.