IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. IV (Nov.-Dec. 2016), PP 51-58
www.iosrjournals.org

A Survey of Manet Governance Survivability on 4g Routing Techniques

Chilakalapudi Meher Babu[1], Dr. Ashish B. Sasankar[2]
[1]*Ph.D. Research Scholar, Post-Graduate Teaching Department of Electronics & Computer Science Dept, R.T.M. Nagpur University, Nagpur, India.*
[2]*professor., Head, Dept Of MCA, G.H.Raisoni Institute Of I.T, Hariganga Campus, Midc,Nagpur,India.*

Abstract: *The various research activities being done by various groups on fourth generation of the cellular system will provide single interface to all kinds of wireless networks allowing participating nodes to access to the network through cellular, wireless LAN networks, and new protocols such as successful and safe implementation of the fourth generation of the wireless technology into the mobile ad-hoc network for the next generation military environment might face tough challenges. It also can be interrupted due to significant differences between the civil and military environment. Physical and technological constraints, geographical limitations and DoS attacks are some of foreseeable challenges. By putting all possible technological advances together from the 4G and MANET, this has set an example for future battle-field. The era of the new wireless communications is very challenging on 4G and MANET communication systems has been emphasized in this paper.*

Keywords: *4G, Mobile Ad-hoc Network, Military Wireless Network, m-Governance, 4GWs.*

I. Introduction

Due to its vital services, Mobile ad hoc network have become an important part of our life. There are several types of attacks and intrusions targeting wireless networks as directly affect the performance and the survivability of MANETs. Routing is essential service for end-to-end communication in MANET, attacks on routing protocol disrupt the reliability and performance of MANET. It can be divided into two categories,

(1) First is routing disruption attack which the attacker trying to change the course of packets.
(2) Second resource consumption attack

This survey focusing on initiatives which make MANET survives against active attacks including Denial of Service (DoS). The contribution of this survey are:

1) investigation of the most valuable techniques and approaches which support MANET routing survivability;
2) Identification the requirement of routing survivability;
3) Investigation of main DoS which violate availability;
4) The classification of routing survivability in initiatives in three groups: authentication,
5) Path Selection, and attack detection.

DIMENSIONS OF MANET And 4G RESEARCHES

A large body of research has been accumulated to address these specific issues, and constraints. In this paper, we describe the ongoing research activities and the challenges in some of the main research areas within the mobile ad hoc network domain. The research activities will be grouped, according to a layered approaching to three main areas: 1.Enabling technologies;2. Networking; 3. Middleware and Applications. Also several issues (energy management, security and cooperation, quality of service, network simulation) span all areas.

SECURITY ENHANCEMENT IN MANET WITH 4G

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Authentication research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of elements of each factor are:

The general concepts of 4G can be present in the list as follows:

- improved capacity,• increased number of users in the cell,• lower transmission costs
- connection with already existing systems,• lower latency,• based on IPv6 protocol, with packet switching,• single interface for all wireless connections,• increased mobility,• support for media applications,• seamless connectivity,• improved security,• improved and guaranteed Quality-of-Service,• global roaming of networks,• standardized open interface,• self-organizing networks
- fast response

Technology/Features	**1G**	**2G/2.5G**	**3G**	**4G**
Start/ Development	1970/ 1984	1980/ 1999	1990/ 2002	2000/ 2010
Data Bandwidth	2 kbps	14.4-64kpbs	2 Mbps	2000 Mbps to1 Gbps for low mobility
Standards	AMPS	2G:TDMA, CDMS, GSM 2.5:GPRS, EDGE, 1xRTT	WCDMA, CDMA-2000	Single unified standard
Technology	Analog Cellular technology	Digital cellular technology	Broad bandwidth CDMA, IP technology	Unified IP and seamless combination of broadband, LAN/WAN/PAN and WLAN
Service	Mobile Telephony (voice)	2G: Digital voice, Short Messaging 2.5G: Higher capacity Packetized data	Integrated Higher Quality audio, video and data	Dynamic Information Access, Wearable devices
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA
Switching	Circuit	2G: Circuit 2.5G: Circuit for access network & air interface; packet for core network and data	Packet except circuit for air interface	All packet
Core Network	PSTN	PSTN	Packet network	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal and vertical

II. Manet And 4g With Governance

Governments, at various levels , have noticed the spread of the Internet and Web and interest in using the latest technologies to improve the services strategies and their implementation involving the utilization of all kinds of wireless and mobile technologies, services, applications, and devices for improving benefits to citizens, business, and all goverment units. Transparency and accountability are the key mantras of a successful government. With growing number of mobile subscriber base, mobile adhoc-Governance has become a powerful tool in the delivery of public services. It's a well known that information and communication technology (ICT) is very critical for processing, storing, organizing, and presenting data and information. The new growth driver now is the mobile phone. It has emerged as an effective tool for good governance in not only facilitating openness and transparency, but also in creating a flow of information between departments, institutions, and various layers of the government. Mobile adhoc-Governance will surely steer the government to a 'service oriented' mindset and make it more agile, responsive, accountable, and action-oriented (Singh, A., 2010).Current mobile adhoc-Governance applications do not exploit the full potential of available technology. In current stage mobile adhoc -Governance is concentrating on following service domains: mobile adhoc–Administration, mobile adhoc-Democracy, mobile adhoc–Education, mobile adhoc – Health, mobile adhoc–Transport, m–Payment. Thus, mobile devices are presently used by governments and public only for the purpose of information sharing. Different mobile adhoc governance Services are identified for pilot level implementation to deliver services through mobile phones and make it accessible to the citizens in the field, in the street, at home or other convenient locations on a 24 X 7 basis, rather than the users having to visit government offices or log on to the internet portals to access services. But, the services such as m-disaster relief/rescue operations (Flood, tsunami, earthquake)

Mobile -Education (Virtual classrooms, Conferences)

Mobile -Monitoring system (Police raids)

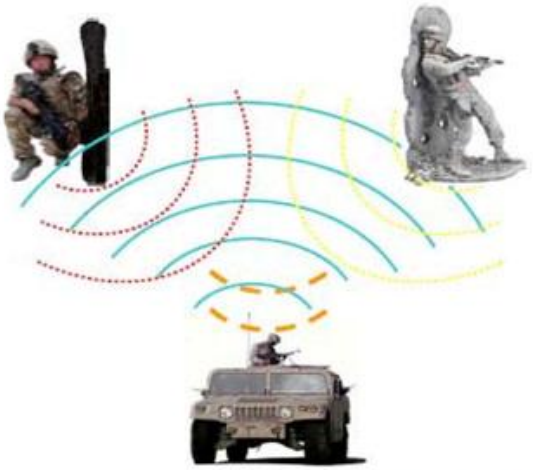
Mobile -Excavations

Mobile -Intelligent transport system

These service domains can be included in like: Military maneuvers, Mobile robotics, Disaster relief, Home networking, Conferences, and for any instant infrastructure.

MANET CAN BE EFFICIENTLY USED IN SITUATION LIKE SURGICAL STRIKE 26/11 , at TAJ HOTEL IN MUMBAI and A **SURGICAL STRIKE at UDI AT KASHMIR** is a military attack which results in surrounding structures, vehicles, buildings, or the general public infrastructure and utilities provides an extremely flexible method for establishing communications for fire/safety/rescue operations or other scenarios requiring rapidly-deployable communications with survivable, efficient dynamic networking. Rescue workers engaged in disaster relief investigate the extent of the damage around them and collaboratively work by sharing the information on their locations and findings. In a situation like 26/11, commandos inside the TAJ could communicate with the use of MANET and they could be connected with the rest of world by using satellite network. But at that time we were not aware about what was happening inside the building.

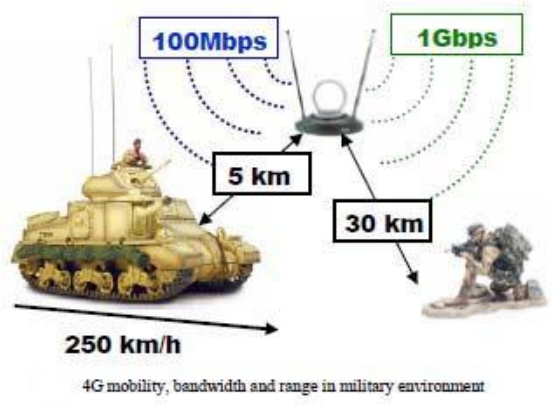
Enemy forces use jammer to interfere army's signal.



Hidden terminal problem: soldiers signal are prevented from hearing each other. The signal to the destination car is interfered.

MANETS can be used in m-Governance environment in uncertain and unorganized scenarios, the problem of constant connectivity and high transmission quality can be solved by 4G concept. This concept can be explained with help of an example of (26/11) Taj Hotel. In the earlier section, we discussed how MANET can be used in 26/11 Taj Hotel situation. The situation can be further improved if the following improvements can be implemented:

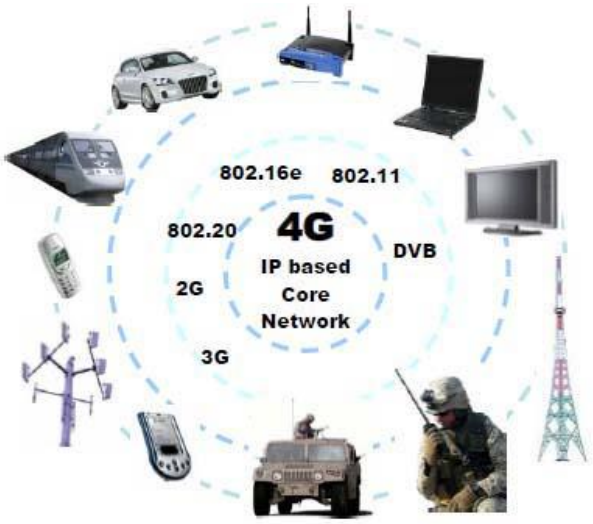
- **Situation 1**- The MANET developed in such a situation can also interact with outer world, So that cops outside the Taj Hotel can get idea of situation inside Hotel an help them in better way.



4G mobility, bandwidth and range in military environment

- **Situation 2-** As nodes can move arbitrarily, there could be a situation when an isolate network can break up in group of two or more networks. Communication between different groups is not possible if there is no connecting help between groups. The situation will become better if different groups can also connect to outer network and communicate with each other using services of external network.

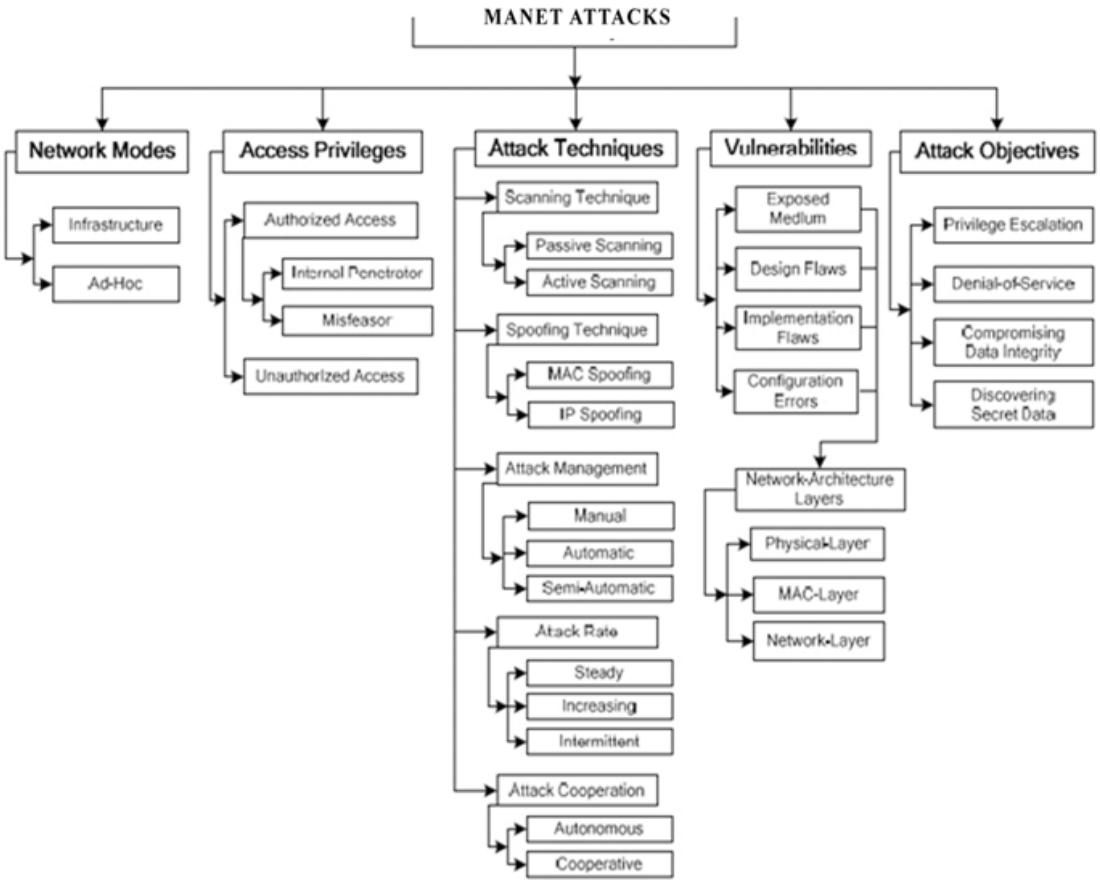
The scenarios represented in situation 1and 2 can be resolved with use of 4G concept. As 4G gives the concept of convergence, it is possible to connect MANET to outer world with 4G and also communication between different isolated MANET subgroups can be established using concept of 4G



Many faces of 4G

FACTORS INFLUENCING IMPLEMENTATION OF MANET IN COMMERCIAL ENVIRONMENT: SECURITY ATTACKS IN MANET

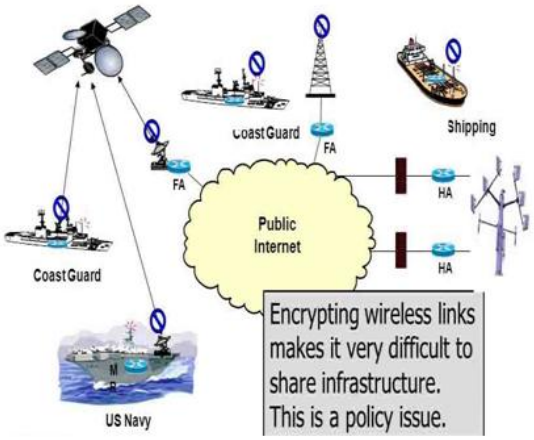
The different characteristics of attacks into two main categories [5]: Active and Passive. In passive attacks, attackers are typically camouflaged, i.e. hidden, and tap the communication lines to collect data. In active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Several papers have presented the security attacks in MOBILE ADHOC [6][7][8][9][10].

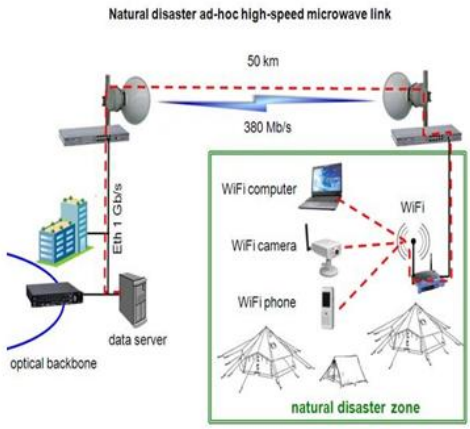


SUMMARIZE OF MANET SURVIVABILITY INITIATIVES

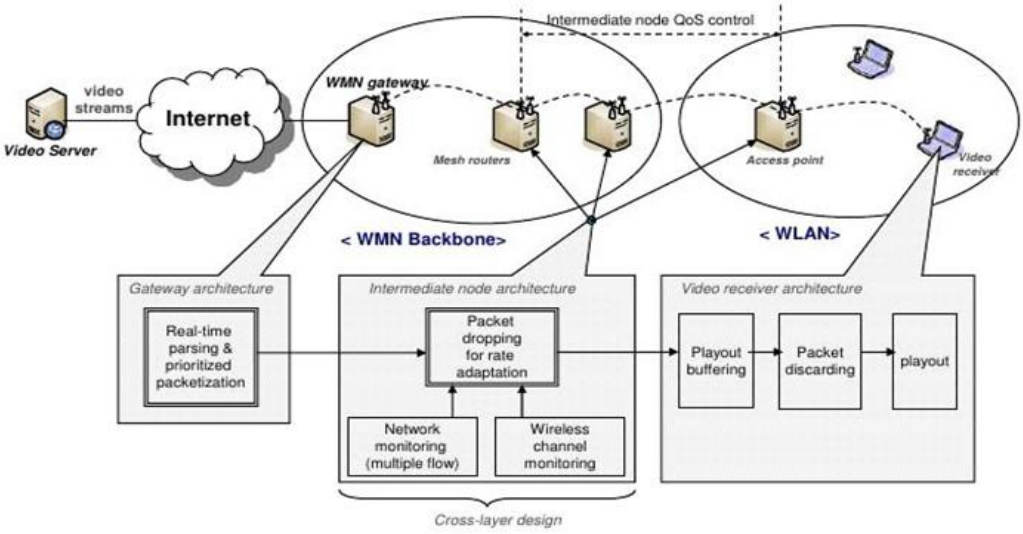
Technique	Attack	Approach	Implementation	Deficiencies	Date
Techniques for In- trusion-resistant Ad Hoc Routing Algorithms	DoS	Based on set of techniques: flow-based route access control (flow-based route access control), flow monitoring, source-initiated router switching,fast authentication, referral based resource allocation	Implemented with the existing routing protocol.	1. In the path failure a compromised node could not be identified. 2. Flow status message can cause additional traffic. 3. Implementation did not explained by author.	2003
Rushing Attack Prevention (RAP)	DoS (rushing attack)	Based on three technique: 1. Secure neighbor detection, 2. Secure route delegation 3. Randomized route request forwarding	Integrated with AODV or DSR.	1. It defends against special type of rushing attack. 2. It incurs higher overhead than other route discovery.	2003
Best effort Fault Tolerant Routing algo-rithm (BFTR)	Dropping, corruption, misrouting, tampering, delaying, fabrication and replaying	The criterion used is: end-to-end performance measured using the data packet transmission ratio and acknowledgement	Undefined	It will not perform well when misbehaving nodes are increased and when network become heavy loaded	2004
Based on Attack Detection & Location	Flooding attacks	1. Suggest a resource allocation mechanism (RAM): depends on taking advantage of existing application capability to handle intruders. 2. Uses wireless ad hoc routing and wireless GRID computing and based on managing a multi trust levels in a real time	(RAM) implemented with the wireless router through a suggested component	Undefined	2005
Mechanism by Geng	DoS	1. New routing mechanism based on common neighbor listening. 2. Each node has a trust_ value increases quickly and decreases slowly depending on its behavior. 3. Bigger trust value = higher priority to listen.	Undefined	If all the common neighbors are under the threshold_value of being trusted then there will be no trusted route to the destination.	2006
Scheme by Lima	DoS	1. Residual path lifetime. 2. Full link lifetime.	Implemented in nodes.	In low mobility environment the performance degrades significantly.	2006
Approach by Dabideen	DoS	1. Based on end-to-end verification and path diversity. 2. Uses digital signature and hash chain. 3. Detects attack by using end-to- end delay and feedback on the number of data packet.	Applied to secure routing though diversity and verification (SRDV) protocol.	Undefined	2009
Strategy by Dan-Yang	1. DoS 2. Link-discontinuing and reduce packet delay	1. Proposes mechanism survivable routing strategy (SRS). 2. Uses optimal exploring theory. 3. SRS calculate the vector angle between survivable node and destination.	Based on AODV protocol	Consumes more of CPU times.	2011
Mechanism by Al-Shahrani	DoS (Rushing attack)	Two solutions proposed: 1. A neighbor safe solution based on blacklist technique. 2. A new algorithm.	Based on SDSR protocol	Limited to solve SDSR problems.	2011

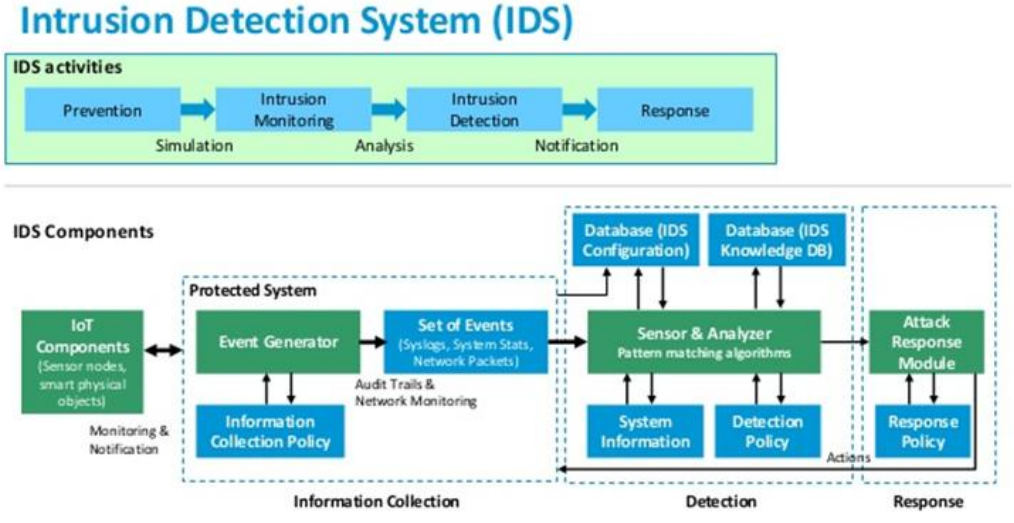
III. Conclusion





Proposed System Architecture: Preliminary Design





The MANETS provide infrastructure less architecture to mobile- Governance concept, resulting in low cost infrastructure results in MOBILE ADHOC GOVERNANCE concept. This kind of network can achieve constant connectivity and high transmission quality by implementing this concept with 4G, results in the concept of 4GMOBILE ADHOC GOVERNANCE. These kinds of networks will result in real-time information delivery revolution to serve highly mobile service user in m-Governance. The Mobile Ad-hoc Governance must face various technical challenges before its adoption; therefore factors influencing the adoption of MANET in commercial environment must be given proper attention.

References

[1]. A. K. Rai, R. R. Tewari and S. K. Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Com- munication," International Journal of Computer Science and Security, Vol. 4, No. 3, 2010, pp. 265-274.

[2]. H. L. Nguyen and U. T. Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Net- works," Networking, International Conference on Sys- tems and International Conference on Mobile Communi- cations and Learning Technologies, 23-29 April 2006, 149 p.

[3]. B. Wu, J. M. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Net- works," Wireless/Mobile Network Security, Springer, Ber- lin, 2007, pp. 103-135.

[4]. V. Gokhale, S. K. Ghosh, et al., "Classification of At- tacks on Wireless Mobile Ad Hoc Networks and Vehicu- lar Ad Hoc Networks," Security of Self-Organizing Net- works, Auerbach Publications: MANET, WSN, WMN, VANET, 2010, p. 195.

[5]. Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security & Privacy, Vol. 2, No. 3, 2004, pp. 28-39. doi:10.1109/MSP.2004.1

[6]. K. Paul, R. R. Choudhuri and S. Bandyopadhyay, "Sur- vivability Analysis of Ad Hoc Wireless Network Archi- tecture," Mobile and Wireless Communications Networks, Springer, Berlin, pp. 31-46.

[7]. M. N. Lima, A. L. dos Santos and G. Pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks," IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, 2009, pp. 66-77.

[8]. Z. Yanjun, "A Framework of Survivability Requirement Specification for Critical Information Systems," 43rd Hawaii International Conference on System Sciences, Piscataway, 2010.

[9]. M. N. Lima, H. W. da Silva, et al., "Requirements for Survivable Routing in MANETs," 3rd International Sym- posium on Wireless Pervasive Computing, 7-9 May 2008, pp. 441-445. doi:10.1109/ISWPC.2008.4556246

[10]. Y.-C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Se- cure On-Demand Routing Protocol for Ad Hoc Net- works," Wireless Networks, Vol. 11, No. 1-2, 2005, pp. 21-38. doi:10.1007/s11276-004-4744-y

[11]. A. A. Cardenas and N. Benammar, G. Papageorgiou and J. S. Baras, "Cross-Layered Security Analysis of Wireless Ad Hoc Networks," DTIC Document.

[12]. A. K. Jain and V. Tokekar, "Classification of Denial of Service Attacks in Mobile Ad Hoc Networks," Interna- tional Conference on Computational Intelligence and Communication Networks, Gwalior, 7-9 October 2011, pp. 256-261. doi:10.1109/CICN.2011.51

[13]. R. C. Linger, N. R. Mead, et al., "Requirements Defini- tion for Survivable Network Systems," Proceedings of the 3rd International Conference on Requirements Engi- neering, Washington DC, 1998, pp. 14-23.

[14]. R. Ramanujan, S. Kudige and T. Nguyen, "Techniques for Intrusion-Resistant Ad Hoc Routing Algorithms (Ti- ara)," DARPA Information Survivability Conference and Exposition IEEE Computer Society, Los Alamitos, 2003, pp. 98-100.

[15]. B. Awerbuch, R. Curtmola, et al., "On the Survivability of Routing Protocols in Ad Hoc Wireless Networks," 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, 5-9 Sep-tember 2005, pp. 327-338.

[16]. S. Dabideen, B. R. Smith and J. J. Garcia-Luna-Aceves, "An End-to-End Solution for Secure and Survivable Rout- ing in MANETs," 7*th International Workshop on Design of Reliable Communication Networks*, Washington DC, 25-28 October 2009, PP. 183-190.

[17]. R. H. Jhaveri, S. J. Patel, *et al*., "DoS Attacks in Mobile Ad Hoc Networks: A Survey," 2*nd International Con- ference on Advanced Computing & Communication Tech- nologies*, 2012.

[18]. B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *ACM Workshop on Wireless Secu- rity*, 2002.

[19]. D.-Y. Qin, L. Ma, X.-J. Sha and Y.-B. Xu, "An Effective Survivable Routing Strategy for MANET," *Tamkang Journal of Science and Engineering*, Vol. 14, No. 1, 2011, pp. 71-80.

[20]. M. N. Lima, H. W. da Silva, *et al*., "Survival Multipath Routing for MANETs," *IEEE of Network Operations and Management Symposium*, Salvador, 7-11 April 2008, pp. 425-432. doi:10.1109/NOMS.2008.4575164

[21]. E. Y. Hua and Z. J. Haas, "Path Selection Algorithms in Homogeneous Mobile Ad Hoc Networks," *Proceedings of the* 2006 *International Conference on Wireless Com- munications and Mobile Computing*, New York, 2006, pp. 275-280.

[22]. Y.-C. Hu, A. Perrig, *et al*., "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *Pro- ceedings of the* 2*nd ACM Workshop on Wireless Security*, San Diego, 2003, pp. 30-40.

[23]. A. S. Al Shahrani, "Rushing Attack in Mobile Ad Hoc Networks," 3*rd International Conference on Intelligent Networking and Collaborative Systems*, Fukuoka, 30 No- vember-2 December 2011, pp. 752-758. doi:10.1109/INCoS.2011.145

[24]. N. A. Boudriga and M. S. Obaidat, "Fault and Intrusion Tolerance in Wireless Ad Hoc Networks," *IEEE of Wire- less Communications and Networking Conference*, Vol. 4, 2005, pp. 2281-2286. doi:10.1109/WCNC.2005.1424871

[25]. P. Geng and C. Zou, "Routing Attacks and Solutions in Mobile Ad hoc Networks," *International Conference on Communication Technology*, Guilin, 27-30 November 2006, pp. 14.

[26]. Y. Xue and K. Nahrstedt, "Providing Fault-Tolerant Ad Hoc Routing Service in Adversarial Environments," *Wire- less Personal Communications*: *An International Journal*, Vol. 29, No. 3-4, 2004, pp. 367-388. doi:10.1023/B:WIRE.0000047071.75971.cd

AUTHOR PROFILE

Chilakalapudi Meher Babu did his **M.Tech in** Computer Science and Engineering from Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh (INDIA) and pursuing **Ph.D in R.T.M. Nagpur University, Nagpur(India) , Currently pursuing Ph.D in the Post-Graduate Teaching Department of Electronics & Computer Science Dept, R.T.M. Nagpur University, Nagpur, India**. He has **12 National and International** Journal Publications to his credit. His area of interest in research includes MANET, Network Intrusion Detection System on Wireless

Lan's, IP Address, Routing Algorithms etc.,

Dr. Ashish B.Sasankar did his MCA. M.Tech (CSE), M.Phil. (Computer Science) & Ph.D. in Computer Science from R.T.M. Nagpur University (India). He has a rich experience of 16 years in the field of Education. Currently, **he is the Head of the Department of MCA in the most prestigious G.H.Raisoni Institute of information Technology [GHRIIT], Nagpur [India]. He is a Ph.D Guide for Computer Science in the Faculty of Science in R.T.M. Nagpur University, Nagpur (India)** and guiding many of his research scholars doing their Ph.Ds in Computer Science in R.T.M.Nagpur University, Nagpur. **He has 40 National & International Journal Publications to his credit. He is a Member of the IEEE and CSI.**