A Survey of Security Enhancement Governance in Manet with 4G

[I]Chilakalapudi MeherBabu, [II]Nuthakki Praveena
[I]Ph.D., Scholar, Post-Graduate Teaching, Dept. of Electronics & Computer Science Dept,
R.T.M. Nagpur University, Nagpur, India.
[II]Assistant Professor, Information Technology,
V.R.Siddartha Engg College. Vijayawada, Andhra Pradesh, India

Abstract

A new way to amplify the security of data transmission of mobile ad-hoc network is presented in this work. There is a gigantic increase in using mobile ad-hoc networks for both surveillance and future warfare operations. This has required the development of innovative MANET solutions to the reliability, security and scalability needs of the defense communications environment and Governance environment. Security and reliability are key aspects of mobile ad-hoc network, especially in security sensitive applications like military. Secure Communication Transmission protocol and secure the data transmission phase by end-to-end secure data forwarding protocol to the multiple paths with minimal redundancy. This work increases the through the removal of multiple paths with minimal redundancy. The fault detection delay is reduced drastically. The delay and jitter variants can also be improved if the nodes location can be predicted nodes location and reducing the unnecessary traffic with the aid of spatial and temporal work is the second phase of this work.

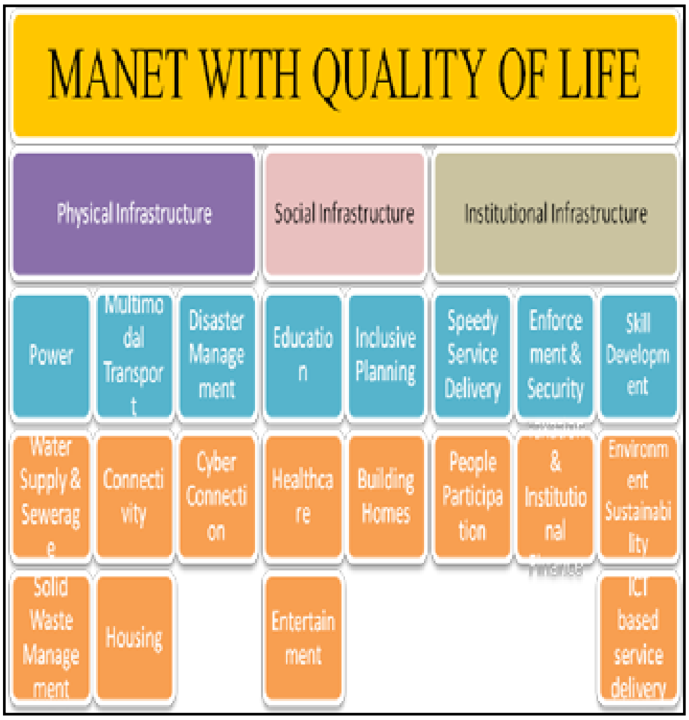
Keywords

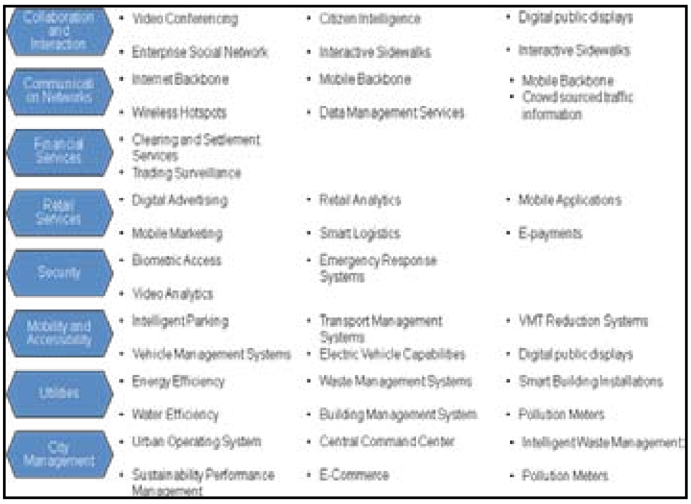
4G, Mobile Ad-hoc Network, Military Wireless Network, m-Governance, 4GWs Include at least 5 to 6 keywords

I. Introduction

Mobile ad hoc networks are need for people to communicate using mobile devices. MANET's data transmission is important to protect the privacy of the data. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies. However, most of the existing key management schemes are not feasible in adhoc networks because public key infrastructures with a centralized certification authority to deploy [16,7]. Various Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into external attacks and internal one. External attacks are carried out by nodes that do not belong to network and can be prevented by firewalls and encryption techniques. Internal attacks are from internal nodes which are actually authorized nodes and part of the network hence it is difficult to identify them. Lot of works [1, 5, 9, 10] had been done in the area of identifying and removal of adversaries in the network. Considering the benefits over the overhead involved in utilizing the multiple paths are increased security, reliability and reduced congestion [4] that is mostly needed for MANETs in military and MANET Governance in 4G. It is not able to overcome the compromised nodes attacks. The work presented in this paper has two phases. The first phase is to improve the security and reliability of data transmission in mobile ad hoc networks by providing secured routes. The faults are identified and those links will be avoided in the data transmission phase. The current topological information will be gathered based on the network behaviour such as transmission time, Probability of lost packets and correctly received acknowledged packets and a threshold is set which is used in binary search probing. Based on the global positioning system (GPS) to reduce the search space. The nodes may exchange the current velocity vectors such as speed and direction to predict the location of the nodes. The spatial and temporal mining can be used to find the relative appropriateness of the location. For example:

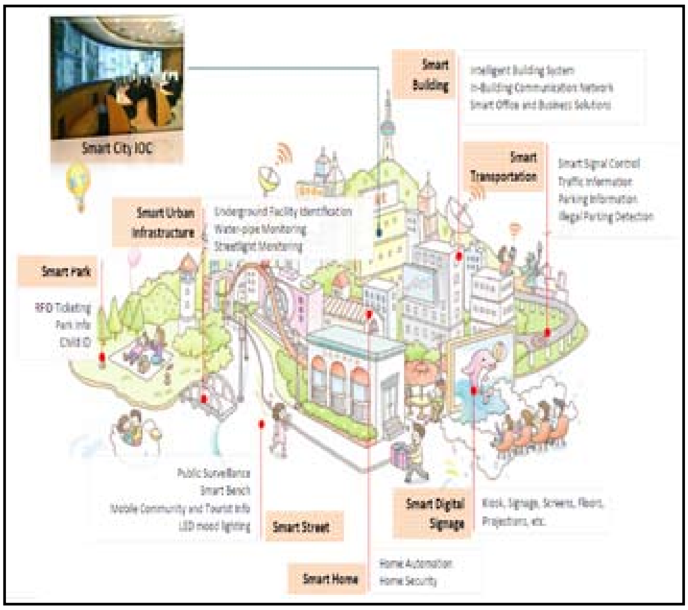
MANET CAN BE EFFICIENTLY USED IN SITUATION LIKE:
Situation 1:
Government of India has announced to develop 100 Smart Cities in the country which is appreciated as a bold step in the context of sustains the economic growth and unprecedented urban growth that is being experienced. On an analysis of the literature available on Smart Cities, it reveals that one of the reasons you need Smart Cities has been Good Governance, while analyzing the components proposed in a Smart City one of the critical component is Smart Governance. One of the challenges today which is common lack of manpower and competence to manage & regulate the urban growth. One of the key areas of concern has been urban governance. Various mandatory reforms in urban governance have been proposed under the JnNURM Scheme of Government of India of which e governance was one. The implementation of e governance has been poor and not uniform across the country. SO, if we design with MANET WITH 4G the Governance structure will be 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).



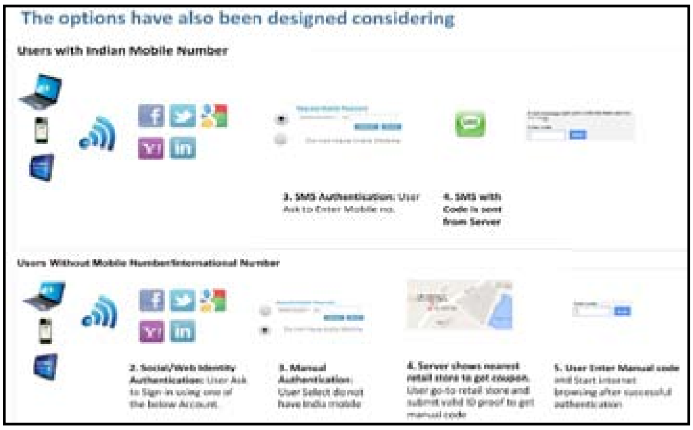


SECURED DATA COMMUNICATION with MANET:

1) MANET with Active Path Sets (APS) and Data Transmission: A set of active diverse, node disjoint multiple paths are selected by applying secured route discovery protocol. The set of paths used for current data transmission are known as Active Path. The Data is isolated based on transmitted in multiple paths by dispersing it into pieces and after encoding. Redundancy ensures successful reconstruction of data even if some loss occurs due to malicious nodes or breakage of routes. 2) MANET with Robust Feedback Mechanism: Each isolated piece is transmitted in different route and carries a Data Authentication Code and by that the integrity of the message and authenticity of the source is verified. After validation, the destination acknowledges every successful receipt. The feedback mechanism is also cryptographically protected and isolated. 3)MANET with APS Adaptation: Successful receipt of ACKS indicates operational routes while missing ACK implies that the route is either broken or compromised. The paths are rated based on short term and long term rating. The routes are selected or discarded based on their rates.



1.Public WIFI	2. Smart Parking	3. Smart Street Lighting & Grid 	4. Video Analytics & Surveillance 	5. Citizen Apps
5 MBPS High Speed Wireless Internet Connectivity	3000 Smart Parking Slots	841 Street-lights based on Solar power	Complete E & G Block covered with 90 cameras	33000 man-days saving due to ease of access of information
175 Hectare Area Covered in Public Wi-Fi in BKC	Parking Time Reduced from 20 minutes to 5 minutes	800 tonnes of Carbon Reduced Annually	Greater coordination among Security Agencies	Improves Citizen Communication
Seamless Wi-Fi Connectivity Across E& G Blocks	19000 Liters of Fuel saved annually	Energy Consumption reduced by 40%	Reduced Street furniture theft	Improved Emergency Alert and Response
50,000 man days saved per year	24 tonnes of Carbon Reduced Annually	200KW of Clean energy generated	Improved Emergency Response	6.5 lakhs Employees Covered
Public Wi-Fi as Value Added service for Business and Exhibition Use	Reduction in Unauthorized Parking	Reduced Maintenance Cost	Secured Business Environment	Increase in ease of Business in BKC



The options have also been designed considering

Users with Indian Mobile Number

3. SMS Authentication: User Ask to Enter Mobile no.

4. SMS with Code is sent from Server

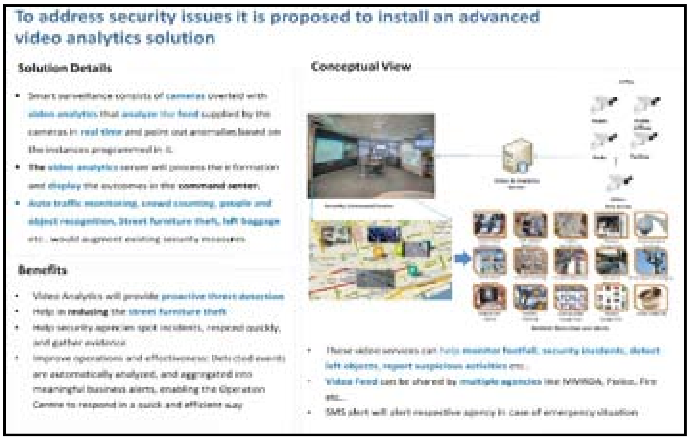
Users Without Mobile Number/International Number

2. Social/Web Identity Authentication: User Ask to Sign in using one of the below Account.

3. Manual Authentication: User Select do not have India mobile

4. Server shows nearest retail store to get coupon. User go-to retail store and submit valid ID proof to get manual code

5. User Enter Manual code and Start internet browsing after successful authentication



To address security issues it is proposed to install an advanced video analytics solution

Solution Details

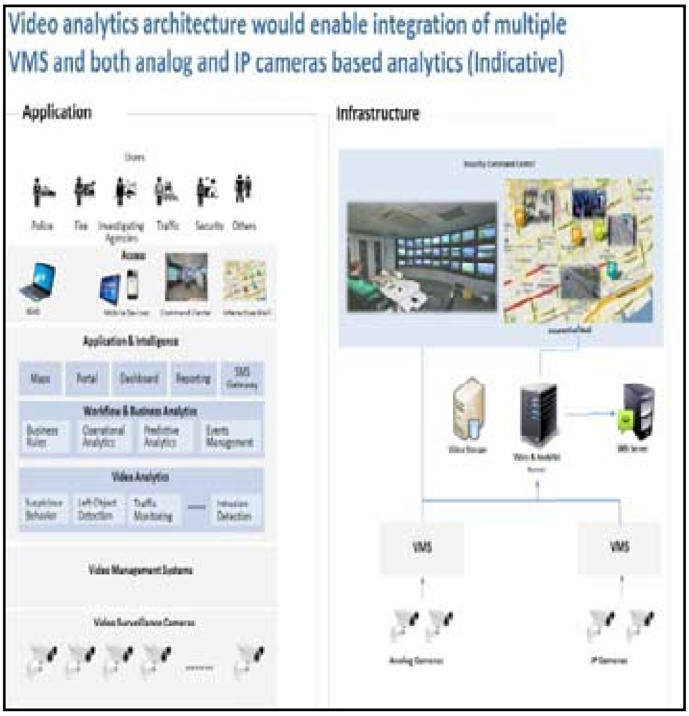
- Smart surveillance consists of cameras overlaid with video analytics that analyze the feed supplied by the cameras in real time and point out anomalies based on the instances programmed in it.
- The video analytics server will process the information and display the outcomes in the command center.
- Auto traffic monitoring, crowd counting, people and object recognition, Street furniture theft, left baggage etc., would augment existing security measures.

Benefits

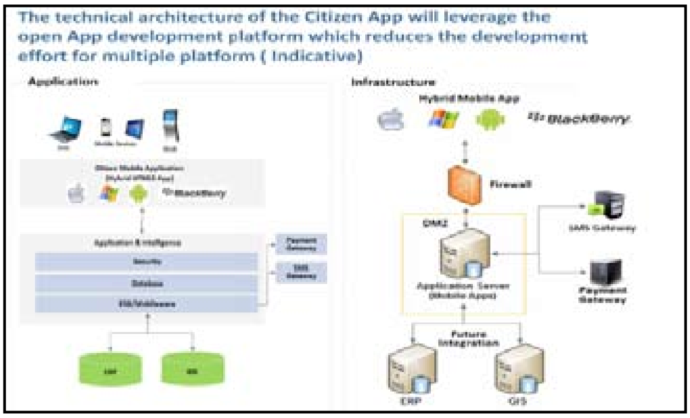
- Video Analytics will provide proactive threat detection
- Help in reducing the street furniture theft
- Help security agencies spot incidents, respond quickly, and gather evidence
- Improve operations and effectiveness: Detected events are automatically analyzed, and aggregated into meaningful business alerts, enabling the Operation Centre to respond in a quick and efficient way

Conceptual View

- These video services can help monitor footfall, security incidents, detect left objects, report suspicious activities etc.,
- Video Feed can be shared by multiple agencies like NMMDA, Police, Fire etc.,
- SMS alert will alert respective agency in case of emergency situation



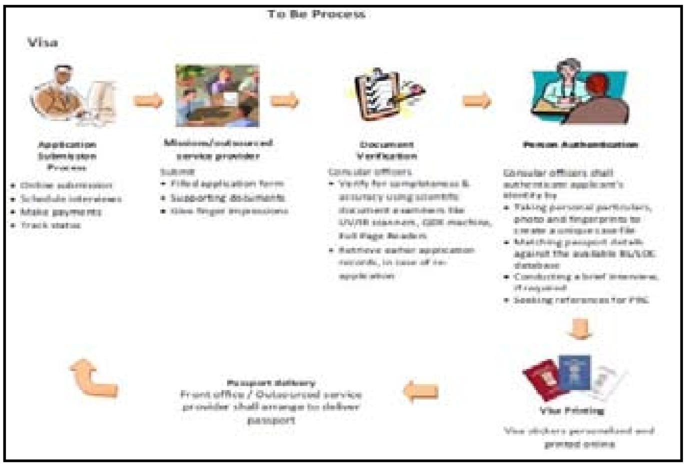
Video analytics architecture would enable integration of multiple VMS and both analog and IP cameras based analytics (Indicative)



The technical architecture of the Citizen App will leverage the open App development platform which reduces the development effort for multiple platform (Indicative)

Situation 2:

India has emerged as a key tourist destination, besides being a major business and service hub. Immigration Check Post is the first point of contact that generates public and popular perception about the country, thus necessitating a state of the art system for prompt and user-friendly services. Within the generic objective of facilitating legitimate travel without compromising security, it is necessary to develop a secure, integrated service delivery framework to enhance security and facilitation in the Visa issuance process, and the Immigration function besides fortifying the Foreigners registration processes for effective tracking of foreigners. The Passport, Visa issuance & consular matters, Immigration, Foreigners registration & tracking and Emigration are inter-related subjects involving the surveillance.



To Be Process

Visa

Application Submission Process
- Online submission
- Schedule interviews
- Make payments
- Track status

Missions/outsourced service provider
Submit
- Filled application form
- Supporting documents
- Give finger impressions

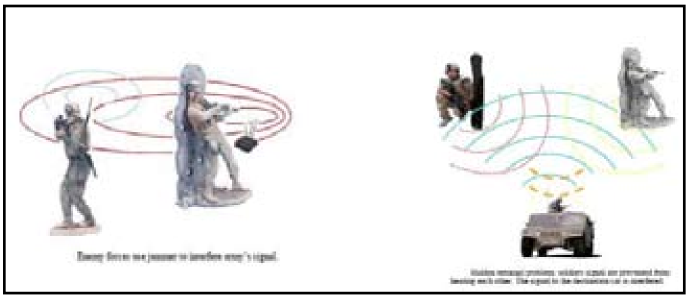
Document Verification
Consular officers
- Verify for completeness & accuracy using scientific document examiners like UV/IR scanners, QDE machine, Full Page Readers
- Retrieve earlier application records, in case of re-application

Person Authentication
Consular officers shall authenticate applicant's identity by
- Taking personal particulars, photo and fingerprints to create a unique case file
- Matching passport details against the available BL/LOC database
- Conducting a brief interview, if required
- Seeking references for PRC

Visa Printing
Visa stickers personalized and printed online

Passport delivery
Front office / Outsourced service provider shall arrange to deliver passport

MANET CAN BE EFFICIENTLY USED IN SITUATION LIKE SURGICAL STRIKE 26/11 , at TAJ HOTEL IN MUMBAI and ASURGICAL STRIKE at UDIATKASHMIR 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.



Conclusion

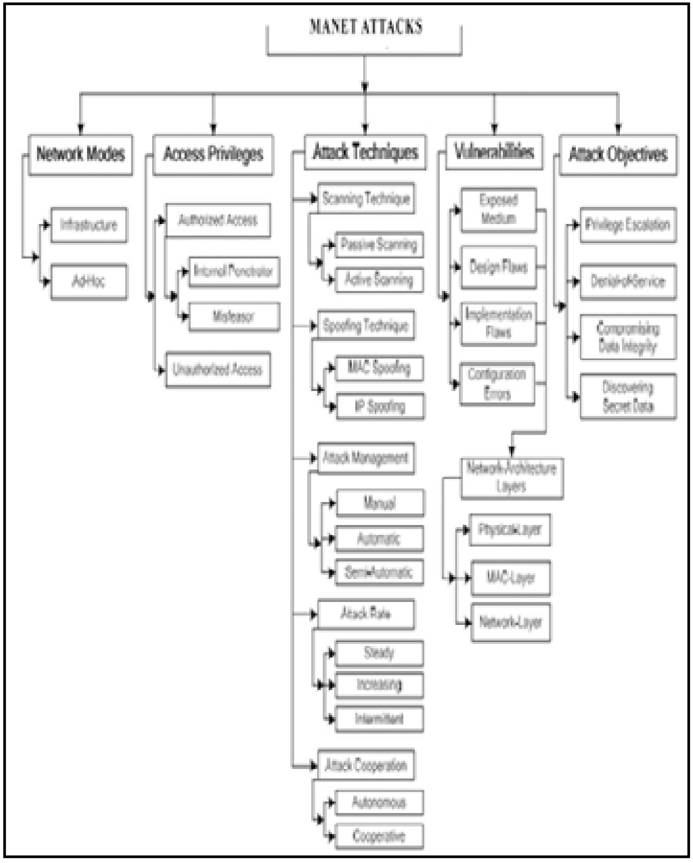
Strengths of Mobile Ad-hoc Network Intrusion Detection System:

MANIDS can perform the following functions to enhance the security.

- Measurements and analysis of typical and atypical user behavior. For example an anomaly based MANIDS is capable of detecting high volume traffic flows, flash crowds, load imbalance in the network, sudden changes in demand of a port usage, sudden surge of traffic from/to a specific host, etc.
- Detection of known worms, viruses, and exploitation of a known security hole. Signature based MANIDS can detect these events with fairly high degree of accuracy. An appropriate signature will also ensure a low false positive probability.
- Some advanced MANIDS systems also enable recognitions of patterns of system events that correspond to a known security threat.
- Enforcement of the security policies in a given network. For example a MANIDS can be configured to block all communication between certain sets of IP addresses and or ports. A MANIDS can also be used to enforce network wide access controls.
- Anomaly based MANIDS can also recognize, with a certain false positive probability, new attacks and abnormal patterns in the network traffic, whose signatures are not yet generated. This will alert the network administrator early, and potentially reduce the damage caused by the new attack.

Limitations of MANIDS

- **A mere Workaround**: A number of researchers have argued that a MANIDS is more or a less a workaround for the flaws and weak or missing security mechanisms in an operating system, an application, and/or a protocol.
- **False Positives**: MANIDS comes with a bane, i.e. false positives. A false positive is an event when a MANIDS falsely raises a security threat alarm for harmless traffic. Signatures can be tuned precisely to reduce such false positives, however fine signatures create a significant performance bottleneck, which is the next limitation of MANIDS. Current Anomaly based algorithms lead to even higher false positives.
- **Performance issues**: Current signature based MANIDS systems use to reduce false positives long signatures are required which further reduces the performance.
- **Encryption**: The ultimate threat to the very existence of the signature based MANIDS systems is the increasing use of data encryption. Everybody dreams to encrypt their data before transmission. Once the packet payloads are encrypted, the existing signatures will become completely useless in identifying the anomalous and harmful traffic.
- **New and sophisticated attacks**: Commercial MANIDS which are signature based are unable to detect new attacks whose signatures are not yet devised. Anomalies based MANIDS can detect such attacks but due to the limitations of the current anomaly detection algorithms, an intelligent attacker can always develop attacks that remain undetected.
- **Human intervention**: Almost all MANIDS systems require a constant human supervision, which slows down the detection and the associated actions. Some recent systems such as Network Intrusion Prevention Systems (NIPS) can automatically take pre-programmed actions but these are limited only to the well known attacks.



References

[1] *A. K. Rai, R. R. Tewari and S. K. Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," 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 Networks," Wireless/Mobile Network Security, Springer, Berlin, 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, "Survivability Analysis of Ad Hoc Wireless Network Architecture," 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 Symposium 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," International 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 (Tiara)," 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 September 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 Routing in MANETs," 7th 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," 2nd 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 Communications 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," Proceedings of the 2nd ACM Workshop on Wireless Security, San Diego, 2003, pp. 30-40.

[23] A. S. Al Shahrani, "Rushing Attack in Mobile Ad Hoc Networks," 3rd 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 Wireless 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 doing as Ph.D., Scholar at 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 Intursion Detection System on Wireless Lan's, IP Address, Routing Algorithms etc.,

Nutakki Praveena did her M.Tech in Information and Technology from JNTU-Vizianagaram University, Visakhapatnam. A.P. INDIA. Her area of expertise includes Computer Networks, wireless LANs, IP address, routing algorithms, Information Technology. She is working as Assistant Professor in department of information Technology at V.R.SIDDARTHA OF ENGINEERING College, Vijayawada, and Andhra Pradesh, India.