IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 6, Ver. I (Nov - Dec .2015), PP 77-83
www.iosrjournals.org

An overview of contemporary security problems in wireless mesh networks

M. Sudhakar[1], Vandana Khare[2]

Professor, Department of ECE, CMR College of Engineering & Technology, India[1]
Associate Professor, Department of ECE, CMR College of Engineering & Technology, India[2]

Abstract: *Wireless mesh network (WMN) is a new wireless networking concept. Unlike traditional wireless networks, Wireless Mesh Networks do not rely on any fixed communications. As an alternative, hosts rely on each other to keep the network connected. Wireless Internet service providers are choosing WMNs to offer Internet connectivity, as it allows a fast, simple and inexpensive network use. One major challenge in design of these networks is their vulnerability to security attacks. In this paper, principal contemporary security issues for wireless mesh networks have been investigated. Identification of the threats a Wireless mesh network faces and the security goals to be realized are described. The new challenges and opportunities posed by this new networking environment are dealt with and explored approaches to secure its communication.*

Key Words: *WLAN, WMN, MANET, WPA, MAC Layer.*

I. Introduction

Wireless communication is without a doubt a very desirable service as emphasized by the tremendous growthin both cellular and Wireless Local Area Networks (WLANs) on the other hand, these 2 radically different technologies address only a narrow range of connectivity wants, & there are numerous other applications that can benefit from wireless connectivity. The cellular networks offer wide area exposure, but the service is relatively expensive and offers low data rates: even the third generation of cellular networks (3G) offers (at best) low data rates (_2Mbps) compared to WLANs (>50Mbps for IEEE 802.11a and 802.11g and _100Mbps for proprietary solutions at the time of this writing). On the other hand, the WLANs have rather limited coverage. In order to increase the coverage of Wireless Local Area Networks, a wired backbone connecting multiple access points is required. Wireless mesh networks (WMNs) have the potential toeliminate many of these disadvantages by offeringlow cost, wireless broadband Internet access both for fixed and mobile users.

In its most general form a wireless mesh network (WMN) interconnects stationary and/or mobileclients and optionally provides access to the Internet. The important characteristic of a wireless mesh network is that the nodes at the core of the network are forwarding the data to and from the clients in a multi hop fashion, thus forming a (mobile) ad hoc network (MANET). Beyond the multi hop constraint; there are no other restrictions on the design of a wireless mesh network, resulting in considerable flexibility and versatility. This versatility allowed many players to enter the mesh networking arena with different products and applications.

The wireless links used to connect the mobile clients can be of the same type as the intra-mesh wireless links[2] or can be a completely different technology [1]. (They can also be missing altogether.) Many implementations allow mobile nodes to connect to the WMN while in its range; their packets are forwarded in the same multi hop manner as the ones of the stationary nodes (and in their turn, although not always preferable, the mobile nodes can forward packets on behalf of other nodes). Not all nodes have to support client nodes; the service provider can employ several relay nodes to increase the coverage of the network (or to improve its performance, as the relays can allow some clients to reach their destinations in fewer hops).

As WMNs become increasingly popular wireless networking technology for establishing the last-mile connectivity for home networking, neighbourhood networking and community, it is imperative to design efficient and secure communication protocols for these networks. On the other hand, the broadcast nature of transmissions in the wireless medium and the dependency on the intermediate nodes for multi-hop communications in such networks lead to several security susceptibilities. These security loopholes can be exploited by potential external and internal attackers causing a detrimental effect on the network performance and disturbance of services. The outer attacks are launched by unauthorized users who intrude into the network for eavesdropping on the network packets and replay those packets at a later point of time to gain access to the network resources [3]. On the contrary, the internal attacks are strategized by some legitimate members in the network processing the authenticated credentials for accessing the network services. Identifying and defending against these attacks in Wireless Mesh Networks, it is a critical requirement in order to provide sustained network services satisfying the quality of services of the user applications [4].

The chapter is planned as follows, Section II to VII presents various possible attacks on different layers on the communication protocol stack of the WMNs. Section VIII discusses briefly on protection mechanism of threats on various layers. Section IX highlights some future research trends on security and privacy issues in WMNs.

II. Security Susceptibilities in WMNs

Different protocols for various layers of WMN communication stack have several susceptibilities. These susceptibilities can be exploited by potential attackers to degrade or disrupt the networkservices. Since many of the protocols assume a pre-existing cooperative relation among the nodes, for successful working of these protocols, the contributing nodes need to be honest and well-behaving with no malicious or dishonest purposes. In practice, some nodes may behave in amalicious or selfish manner or may be compromised by some other malicious users. The assumption of pre existing trust relationships among the nodes and the absence of a central administrator make the protocols at the link, network and transport layers vulnerable to various types of attacks.

Furthermore, the application layer protocols can be attacked by worms, viruses, malwares etc. Variouspossible attacks may also be launched on the protocols used for authentication, key management, and user privacy security. In this section we present a comprehensive discussion on various types of attacks in different layers of WMN protocol stack.

III. Security susceptibilities in the physical layer

The physical layer is responsible for carrier frequency generation, frequency selection, and modulation, signal, detection, and data encryption. As with any radio based medium and the possibility of a jamming attack in WMNs is high since this attack can be launched without much effort and sophistication. Jamming is a type of attack which interferes with the radio frequencies that the nodesuse in a WMN for communication [5]. A jamming source may be powerful enough to disrupt communication in the complete network. Still with less powerful jamming sources, an adversary canpotentially disrupt communication in the entire network by strategically distributing the jamming sources. An intermittent jamming source may also prove detrimental as some communications in WMNs may be time sensitive. Congestion attacks can be more complex to detect if the attackingdevices do not obey the MAC layer protocols [6].

IV. Security susceptibilities in the link layer

Different types of attacks square measure attainable within the link layer of a Wireless Mesh Networks. A number of the key attacks at this layer are: passive eavesdropping, waterproof address spoofing, congestion, unfairness in allocation, replay, partial matching and pre computation etc. These attacks square measure concisely delineated during this sub section.

A. Passive eavesdropping: the printed nature of transmission of the wireless networks makes these networks at risk of passive eavesdropping by the external attackers inside the transmission vary of the conversing nodes. Multi-hop wireless networks like Wireless Mesh Networks are at risk of internal eavesdropping by the midway hops, anyplace in a very malicious intermediate node might keep the copy of all the information that it forwards while not the data of the other nodes within the network. Though a passive eaves dropping doesn’t have an effect on the network, practicality directly, it ends up in the compromise in knowledge confidentiality and knowledge integrity. Cryptography is usually used with victimisation sturdy encryption keys to guard the confidentiality and integrity of knowledge.

B. Link layer ECM attack: link layers attacks square measure additional complicated compared to blind physical layer jamming attacks. Instead of transmission random bits perpetually, the offender might transmit regular waterproof frame headers (with no payload) on the channel that conforms to the MAC protocol being employed within the victim network [7]. Consequently, the legitimate nodes continually notice the channel busy and back down for a random amount of your time before sensing the channel once more. This ends up in the denial-of-service for the legitimate nodes and additionally allows the ECM node to conserve its energy. Intelligent ECM isn't a strictly transmit activity. Refined sensors square measure deployed, that observe and establish victim network activity, with a selected specialise in the linguistics of higher-layer protocols (e.g., AODV and TCP). Supported by the observations of the sensors, the attackers will exploit the sure temporal order behaviour exhibited by higher-layer protocols and use offline analysis of packet sequences to maximise the potential gain for the transmitter. These attacks are often effective although cryptography techniques like wired equivalent privacy (WEP) and local area network protocol access (WPA) are used. As a result of the sensing element that assists the transmitter can still monitor the packet size, timing, and sequence to guide the transmitter. As a result of these attacks square measure supported fastidiously exploiting protocol patterns and consistencies across size, temporal order and sequence, preventing them would force modifications to the protocol linguistics so these consistencies square measure removed where attainable.

C. Intentional collision of frames: a collision happens once 2 nodes conceive to transmit on constant frequency at the same time [9]. Once frames collide, they're discarded and wish to be retransmitted. A mortal might strategically cause collisions in specific packets such as acknowledgment (ACK) management messages. An attainable results of such collision is that the pricey exponential back-off. The mortal might merely violate the communication protocol and unceasingly transmit messages in an effort to get collisions. Recurrent collisions also can be employed by AN offender to cause resource exhaustion. As an example, a naïve water proof layer implementation might unceasingly conceive to channel the corrupted packets. Unless these retransmissions square measure detected early, the energy levels of the nodes would be exhausted quickly. An offender might cause unfairness by intermittently victimisation the waterproof layer attacks. During this case, the mortal cause's degradation of period applications running on different nodes by intermittently disrupts their frame transmissions.

D. Water proof spoofing attack: waterproof addresses have long been used because the singularly distinctive layer-2 network identifiers in each wired and wireless LANs. Waterproof addresses that square measure globally distinctive have typically been used as an authentication issue or as a singular symbol for granting variable levels of network privileges to a user. This can be notably common in 802.11 local area network networks. However, the waterproof protocol in 802.11 customary and also the network interface cards don't offer any safeguards against a possible offender from modifying the supply waterproof address in its transmitted frames. Modifying the waterproof addresses in transmitted frames is referred to as waterproof spoofing, and it is often employed by attackers in a different ways. Waterproof spoofing allows the offender to evade intrusion detection systems (IDSs) within the networks. Further, the network administrators typically use waterproof addresses in access management lists.

E. Replay attack: the replay attack typically referred to as the man-in-the-middle attack [10], can be launched by external moreover as internal nodes. As an example, an external malicious node (M) can listen in on the printed communication between 2 nodes A and B. It will then replay the (eaves dropped) messages later to realize access to the network resources. Generally, the authentication information is replayed wherever the offender M deceives a node (node B) to believe that the attacker could be a legitimate node (node). On an identical note, the malicious node M, that is an intermediate hop between 2 nodes A and B, will keep a duplicate of all relayed knowledge. It will then retransmit this knowledge later to realize an unauthorized access to the network resources.

F. Pre-computation and partial matching attack: in contrast to the preceding attacks, where MAC protocol vulnerabilities square measure exploited, these attacks exploit the vulnerabilities within the security mechanisms that square measure used to secure the water proof layer of the network. Pre-computation and partial matching attacks exploit the crypto logic primitives that square measure used at the waterproof layer for secure communication. In a very pre-computation attack or time memory trade-off attack (TMTO), the attacker computes an oversized quantity of data (key, plaintext, and individual cipher text) and stores that information before launching the attack. Once the particular transmission starts, the offender uses the pre computed information to hurry up the cryptography method. TMTO attacks square measure extremely effective against an oversized range of crypto logic solutions. On the opposite hand, in a very partial matching attack, the attacker has access to some (cipher text, plaintext) pairs, that successively decreases the cryptography key strength, and improves the possibilities of success of the brute force mechanisms. Partial matching attacks exploit the weak implementations of cryptography algorithms. as an example, within the IEEE 802.11 standard for waterproof layer security in wireless networks, the waterproof address fields within the waterproof header square measure used in the message integrity code (MIC). The waterproof header is transmitted as plaintext whereas the MIC field is transmitted within the encrypted type. Partial data of the plaintext (MAC address) and also the cipher text (MIC) makes IEEE 802.11i at risk of partial matching attacks. DoS attacks can also be launched by exploiting the protection mechanisms.

V. Security susceptibilities in the network layer

The attacks on the network layer are loosely divided into 2 types: management packets attacks and knowledge packets attacks. What is more, each of these attacks can be either active or passive in nature [11]. Management packets attacks usually target the routing practicality of the network layer. The target of the assaulter is to create routes untouchable or force the network to decide on sub-optimal routes. On the opposite hand, the information packet attacks have an effect on the packet forwarding practicality of the network. The target of the assaulter is to cause the denial of service for the legitimate user by creating user knowledge undeliverable or injecting malicious knowledge into the network. We tend to first think about the network layer management packets attacks.

A. Attacks on the management packets: dashing attacks that focus on the on-demand routing protocols (e.g., AODV), were among the primary exposed attacks known by Hu et al. [12] on the network layer of multi-hop wireless networks. Dashing attacks exploit the route discovery mechanism of on-demand routing protocols. In these protocols, the node requiring a route to the destination floods the route request (RREQ) message that is known by a sequence range. To limit the flooding, every node solely forwards the primary message that it receives and drops remaining messages with an equivalent sequence range. The protocol specify a particular quantity of delay between receiving the RREQ message by a specific node and forwarding it, to avoid collusion of those messages. The malicious node launching the dashing attack forwards the RREQ message to the target node before the other intermediate node from the supply to destination. This could simply be achieved by ignoring the required delay.

A black hole attack (or depression attack) [13] is another attack that ends up in denial of service in WMNs. It conjointly exploits the route discovery mechanism of on-demand routing protocols. In an exceedingly black hole attack, the malicious node forever replies completely to a RREQ, though it should not have a sound route to the destination. As a result, the malicious node doesn't check its routing entries; it'll forever be the primary to reply to the RREQ message. Therefore, most the traffic inside the neighbourhood of the malicious node is going to be directed towards the malicious node, which can drop all the packets, inflicting a denial of service

A gray hole attack could be a variant of the black hole attack. In an exceedingly black hole attack, the malicious node drops all the traffic that it's imagined to forward. This might result in doable detection of the malicious node. In a gray hole attack, the someone avoids the detection by dropping the packets by selection. A gray hole doesn't result in complete denial of service; however it should go undetected for an extended length of time.

A Sybil attack is that the type of attack wherever a malicious node creates multiple identities within the network, every showing as a legitimate node [14]. A Sybil attack was first exposed in distributed computing applications wherever the redundancy within the system was exploited by making multiple identities and dominant the goodish system resources. Within the networking state of affairs, variety of services like packet forwarding, routing, and cooperative security mechanisms is discontinuous by someone employing a Sybil attack.

In addition to the above-named attacks, the network layer of WMNs also are liable to various types of attacks such as: route request (RREQ) flooding attack, route reply (RREP) loop attack, route re-direction attack, false route fabrication attack, network partitioning attack, etc.,

B. Attacks on the information packets: the attacks on the information packets square measure primarily launched by selfish and malicious (i.e., compromised) nodes within the network and result in performance degradation or denial of service of the legitimate user knowledge traffic. The best of the information plane attacks is passive eavesdropping. Eavesdropping could be a raincoat layer attack. Narcissistic behaviour of the participating WMN nodes could be a major security issue as a result of the WMN nodes square measure obsessed on each other for knowledge forwarding. The intermediate-hop narcissistic nodes might not perform the packet-forwarding functionality as per the protocol. The narcissistic node could drop all the information packets, leading to completed of service, or it should drop the information packets by selection or indiscriminately. It's arduous to distinguish between such a narcissistic behaviour and therefore the link failure or network congestion. On the opposite hand, malicious intermediate-hop nodes could inject junk packets into the network. Goodish network resources (i.e., information measure and packet process time) could also be consumed to forward the junk packets, which may result in denial of service for legitimate user traffic.

C. Attacks on multicast routing protocols: multicast routing protocols deliver knowledge from a supply node to multiple destinations that square measure organized in an exceedingly multicast cluster. Since several of the applications that use multicast services in an exceedingly WMN have high-throughput needs, and hop-count will not serve as a decent metric for increasing output, some protocols [15,16] concentrate on increasing path throughput, wherever ways square measure chosen supported metrics that square measure obsessed on the wireless link qualities. In these protocols, nodes sporadically send probes to their neighbours to live the quality of the links from their neighbours. Choice of the most effective path for increasing output is finished based on collaboration of nodes. Associate in nursing aggressive strategy for the most effective path choice presumptuous a perfect collaboration among all taking part nodes provides a straightforward chance to a malicious node to manipulate the link metrics to its own advantage. In different words, Associate in nursing assaulter could fitly regulate the link metrics so it gets chosen on the most effective routing path for a source-destination combine. During this method, it draws additional traffic towards itself. However, since its intention is to disrupt network communication, it starts dropping packets will which which may might} result in a doable network partitioning or can facilitate the malicious node to hold out a traffic analysis on the network.

VI. Security vulnerabilities in the transport layer

The attacks that can be launched on the transport layer of a WMN are *SYN flooding attack* and D*e-synchronization attack.*

A. SYN flooding attacks are simple to launch on a transport layer protocol like transmission control protocol. Transmission control protocol needs state in formation to be maintained at each ends of an affiliation between 2 nodes, that makes the protocol at risk of memory exhaustion through flooding. Associate in nursing assaulter could repeatedly build new connection request till the resources needed by every affiliation are exhausted or reach a maximum limit. In either case, more legitimate requests are going to be neglected. One variant of such *DoS* attacks is the SYN flooding attack, during which Associate in Nursing assaulter creates an oversized variety of half-open transmission control protocol connections with a target node while not finishing any of those requests. Within the transmission control protocol, 2 nodes have to successfully complete a three-party shake mechanism before sessions are often established between the nodes. Within the first message, the node initiating the communication sends a SYN packet to the receiver node in conjunction with a sequence variety. The receiver node sends a SYN/ACK message containing a sequence variety Associate in nursing an acknowledgment sequence variety to the initiator node. The instigator node then completes the shake method by causing Associate in nursing ACK message containing Associate in nursing acknowledgment variety. Associate in nursing assaulter will exploit this protocol by causing a large number of SYN packets to a target node and spoofing the destination of the SYN packets.

Session hijacking attacks exploits the vulnerability of the transport protocols (e.g., TCP) that do not provide AN security check throughout an on-going session. All security mechanisms square measure applied only during the session institution time. in an exceedingly protocol session hijacking attack, AN wrongdoer spoofs the IP address of a victim node, properly determines the present sequence range that's expected to be generated at the victim node, then performs a DoS attack on the victim node.

B. De-synchronization attack refers to the disruption of associate existing affiliation [9]. Associate offender might for instance, repeatedly spoof messages to associate finish host inflicting the host to request the retransmission of incomprehensible frames. If regular properly, associate offender might degrade or perhaps stop the power of the end hosts to with success exchange knowledge inflicting them instead to waste energy making an attempt to recover from errors that ne'er extremely exist.

In this attack, associate offender injects false knowledge in associate current session between 2 nodes by launching a session hijacking attack. The false injected knowledge is received by one of the nodes within the human action try and on receipt of the information; the node sends associate ACK to the other node. Since the node at the opposite finish wasn't expecting the sequence range of this ACK packet, the node tries to re-synchronize the session with its human action peer. This cycle goes on indefinitely as the ACK packets travelling back associated forth within the network causes an ACK storm.

VII. Security vulnerabilities in the application layer

At the appliance layer, a compromise needs a full information of the human activity applications (e.g., application layer info for traffic snooping) furthermore as compromising all the lower layers. The impact of such attacks will be extraordinarily prejudicial. As an example, a flooding attack will have an effect on the availability of the victim node furthermore as an oversized portion of the network. Snooping attack at the application layer will have an effect on the integrity of the messages being communicated.

The attacks in the application layer are principally as a result of the viruses, malwares and worms or the repudiation attacks launched by business executive nodes [17]. Mobile viruses and worms contain malicious codes that unfold or replicate apace in a very network and in the hosts and launch varied styles of attacks like memory exhaustion, data escape, phishing etc.

Repudiation attacks launched within the application layer cannot be detected or prevented by deploying firewalls at the network layer or by end-to-end cryptography of traffic at the transport layer. Associate degree attacker getting associate degree access to the data in network or host by refined techniques will repudiate having conducting such an activity. Detection of such attacks desires refined intrusion detection systems at multiple layers.

VIII. Security vulnerabilities and the user privacy protection mechanisms

Protection of user privacy is a very important issue in wireless network communication. However, ensuring privacy of the users is tough to realize although the messages within the network are protected, as there are not many security solutions or mechanisms which may guarantee that knowledge isn't discovered by the authorized parties themselves [18]. Communication privacy can't be assured with message encryption since the attackers will still observe UN agency is human activity with whom likewise as the frequency and period of every communication session. Additionally, unauthorized parties will get access to the situation info regarding the positions of various MCs by observant their communication and traffic patterns. Hence, there's a desire to make sure location privacy in WMNs likewise.

Table 1 presents a summary of various types of vulnerabilities in different layers of the communication protocol stack of a WMN and their possible defence mechanisms. The details of the different defence mechanisms are just mentioned.

TABLE 1
Various Types Of Vulnarabilites And Their Defence Mechanisms

Layer	Attacks	Defence Mechanisms
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
MAC	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Spoofed routing information & selective forwarding	Egress filtering, authentication, monitoring
	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring, redundancy
	Wormhole	Authentication, probing
	Hello Flood	Authentication, packet leashes by using geographic and temporal information
	Ack. Flooding	Authentication, bi-directional link authentication verification
Transport	SYN Flooding De-synchronization	Client puzzles, SSL-TLS authentication, EAP
Application	Logic errors Buffer overflow	Application authentication Trusted computing, Antivirus
Privacy	Traffic analysis, Attack on data privacy and location privacy	Holomorphic encryption, Onion routing, schemes based on traffic entropy computation, group signature based anonymity schemes, use of pseudonyms

IX. Conclusion

WMNs became the main focus of analysis in wireless networks within the recent years because of their great promise in realizing varied next-generation wireless services. Driven by the demand for made and high-speed content access, recent analysis on WMNs has targeted on developing high performance communication protocols. Whereas, the protection and privacy problems with these protocols have received comparatively less attention. However, given the wireless and multi-hop nature of communication in WMNs, these networks square measure susceptible to a larger form of attacks the least bit layers of the communication protocol stack. Although, the researchers have created substantial contributions within the areas of security and privacy in WMNs, there square measure still several challenges that stay to be addressed.

Driven by the increasing demand for made, high-speed and information measure intensive content access, recent analysis has targeted on developing high performance communication protocols for such networks, whereas problems like security, privacy, access management, intrusion detection, secure authentication etc. have taken the rear seat. However, given the inherent vulnerabilities of the wireless medium as a result of its broadcast nature and multi-hop communications in WMNs, these networks square measure subject to a large vary of threats.

This paper has facilitated a comprehensive presentation on the assorted attacks on totally different layers of the communication protocol stack of WMNs. While highlight varied vulnerabilities within the physical, link, network, transport and application layers, this paper simply mentioned its attention on however attacks are often launched on authentication, privacy and key management protocols on WMNs. In respect of distinctive varied security threats, the paper has varied defence mechanisms for defending those attacks. Future work is going to be carried out on comprehensive survey of a number of these defence mechanisms and conjointly comparison of them with relation to their different approaches towards security and their performance efficiencies.

References

[1] "Firetide website." http://www.firetide.com.

[2] "MeshNetworks website." http://www.meshnetworks.com.

[3] J. Sen, "Secure and privacy-preserving authentication protocols for wireless mesh networks", bookchapter in: Applied Cryptography and Network Security, J. Sen (ed.), pp. 3 - 34, INTECH, Croatia,2012.

[4] J. Sen, "Secure routing in wireless mesh networks", book chapter in: Wireless Mesh Networks, N.Funabiki (ed.), pp. 237-280, INTECH, Croatia, 2011.

[5] E. Shi and A. Perrig, "Designing secure sensor networks", IEEE Wireless Communication Magazine,vol 11, no 6, pp. 38-43, 2004.

[6] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jammingattacks in wireless networks", in Proceedings of the 6th ACM International Symposium on Mobile AdHoc Networking and Computing (MobiHoc'05), Urbana-Champaign, IL, USA, pp. 46-47, May 2005,ACM Press.

[7] Y. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient linklayer jamming attacks against wireless sensor network MAC protocols", in ACM Transactions onSensor Networks (TOSN), vol 5, no 1, article no 6, February 2009.

[8] T. X. Brown, J. E. James, and A. Sethi, "Jamming and sensing of encrypted wireless ad hoc networks", in Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc'06), Florence, Italy, pp. 120-130, May 2006.

[9] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks", IEEE Computer, vol 35, no10, pp. 54-62, 2002.

[10] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1X standard", Technical Report CS-TR-4328, Computer Science Department, University of Maryland, USA, 2002.

[11] A. Naveed, S. S. Kanhere, and S. K. Jha, "Attacks and security mechanisms", book chapter in: Securityin Wireless Mesh Networks, Y. Zhang et al. (eds.), pp. 111-144, Auerbach Publications, CRC Press,USA, 2008.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc networkrouting protocols", in Proceedings of the ACM Workshop on Wireless Security (WiSe'03) inconjunction with ACM MobiCom'03, San Diego, CL, USA, pp. 30-40, September 2003, ACM Press.

[13] M. Al-Shurman, S-M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks", in Proceedings of the 42nd Annual Southeast Regional Conference(ACM-SE), Huntsville, Alabama, USA,pp. 96-97, April 2004.

[14] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis and defenses", in Proceedings of the 3rd International Symposium on Information Processing in SensorNetworks (IPSN'04), Berkeley, CA, USA, pp. 259 – 268, April 2004, ACM Press.

[15] S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-throughput multicast routing metrics in wireless mesh networks", in Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06), Lisbon, Portugal, p. 48, July 2006. IEEE Computer Society Press.

[16] A. Chen, D. Lee. G. Chandrasekaran, and P. Sinha, "HIMAC: high throughput MAC layer multicasting in wireless networks", in Proceedings of the 3rd IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS'06), Vancouver, British Columbia, Canada, pp. 41-50, October 2006.

[17] B. Wu, J. Chen, J. Wu., and M. Cardei, "A survey on attacks and countermeasures in mobile ad hoc networks", book chapter in: Wireless Network Security, Y. Xiao et al. (eds.), pp. 103-135, Springer, Signals and Communications Technology, 2006.

[18] H. Moustafa, "Providing authentication, trust, and privacy in wireless mesh networks", book chapter in: Security in Wireless Mesh Networks. Y.Zhang et al. (eds.), pp. 261-295, CRC Press, USA, 2007.

[19] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: anonymous on-demand routing in mobile ad hoc networks", IEEE Transactions on Wireless Communications, vol 5, no 9, pp. 2376–2385, September 2006.

[20] X. Lin, X. Ling, H. Zhu, P.-H. Ho, and X. S. Shen, "A novel localised authentication scheme in IEEE 802.11 based wireless mesh networks", International Journal of Security and Networks, vol 3, no 2, pp. 122-132, 2008

AUTHOR BIOGRAPHY

Dr. M. Sudhakar[1]: Graduated from JNTU College of Engineering, Hyderabad in 1979, with specialization in ECE. He completed his M.Tech from Indian Institute of Technology Madras in 1986 with the specialization in Instrumentation, Control & Guidance. Obtained doctoral degree from Annamalai University. Successfully headed R&D Project assigned by IAF on "Mathematical Modelling & Simulation of Aero Engine Control System‟ at Aeronautical Development Establishment, Bangalore and Gas Turbine Research Establishment, Bangalore. He is presently working as a Professor in the department of ECE and Vice Principal at CMR College of Engineering & Technology, Hyderabad.

Mrs. Vandana Khare[2] is pursuing PhD in Communication Engineering JNTU Hyderabad (A.P). She completed M.E (Digital techniques) in 1999 from SGSITS, INDORE (M.P) India and B.E in ECE in the year 1994 from GEC Rewa (M.P). She is Associate Professor in ECE at CMR College of Engineering & Technology. Secunderabad. She has 18 years of teaching experience and has published 13 research papers in International journals &presented 5 papers in National & International conferences. She is life member of ISTE, IETE & IEEE Technical societies. Her research Interest includes Wireless Communication, Computer Networks, Mobile Computing and Bio-Medical Imaging.